

Cesare Gallotti

con contributi di

Massimo Cottafavi e Stefano Ramacciotti

.....
SICUREZZA
DELLE
INFORMAZIONI
.....

GESTIONE DEL RISCHIO
I SISTEMI DI GESTIONE
LA ISO/IEC 27001:2022
I CONTROLLI DELLA ISO/IEC 27002:2022



Versione Gennaio 2022

Cesare Gallotti

con contributi di

Massimo Cottafavi e Stefano Ramacciotti

.....
SICUREZZA
DELLE
INFORMAZIONI
.....

GESTIONE DEL RISCHIO
I SISTEMI DI GESTIONE
LA ISO/IEC 27001:2022
I CONTROLLI DELLA ISO/IEC 27002:2022



Versione Gennaio 2022

Cesare Gallotti

con il contributo di

Massimo Cottafavi e Stefano Ramacciotti

Sicurezza delle informazioni

Valutazione del rischio

I sistemi di gestione per la sicurezza delle informazioni

La norma ISO/IEC 27001

©2022 Cesare Gallotti

Tutti i diritti riservati

Ovviamente non è difficile copiare questo libro tutto o in parte, ma devo offrire una pizza a chi mi ha aiutato (vedere nei ringraziamenti), quindi vi prego di non farlo.

Versione Gennaio 2022

Dedicato, come nel 2014, a, in ordine di apparizione:

Roberto e Mariangela Gallotti;

Clara;

Chiara e Giulia;

Paola Aurora, Alessio e Riccardo;

Juan Andrés e Yeferson, venuti da lontano

direttamente nel nostro cuore.

Indice

Presentazione e ringraziamenti

1 Introduzione

I Le basi

2 Sicurezza delle informazioni e organizzazione

2.1 Dati e informazioni

2.2 Sicurezza delle informazioni

2.2.1 Riservatezza

2.2.2 Integrità

2.2.3 Disponibilità

2.2.4 Altre proprietà di sicurezza

2.2.5 Gli impatti sui parametri RID

2.3 Sicurezza informatica e cybersecurity

2.4 Organizzazione, processi e funzioni

2.4.1 I processi

2.4.2 Le funzioni

2.5 Processi, prodotti e persone

3 Sistema di gestione per la sicurezza delle informazioni

3.1 Sistema di gestione

3.2 Sistema di gestione per la sicurezza

3.3 Le certificazioni

II La gestione del rischio

4 Rischio e valutazione del rischio

4.1 Cos'è il rischio

4.1.1 I rischi positivi e negativi

4.1.2 Il livello di rischio

4.2 Cos'è la valutazione del rischio

4.3 I metodi per valutare il rischio

4.3.1 I programmi software per la valutazione del rischio

4.3.2 Avvertenza

4.4 Chi coinvolgere

4.4.1 I responsabili del rischio

4.4.2 I facilitatori

4.5 I documenti di gestione del rischio

5 Il contesto e l'ambito

5.1 Il contesto

5.2 L'ambito

6 Identificazione del rischio

6.1 Gli asset

6.1.1 Informazioni

6.1.2 Gli altri asset

6.1.3 Chi identifica gli asset

6.2 Le minacce

6.2.1 Gli agenti di minaccia

6.2.2 Tecniche di minaccia

6.2.3 Le minacce e il rischio privacy

6.2.4 Chi individua le minacce

6.3 Associare le minacce agli asset

6.4 Collegare le minacce alle conseguenze

6.5 Le vulnerabilità e i controlli di sicurezza

6.6 Correlare le vulnerabilità agli asset

6.7 Correlare vulnerabilità e minacce

6.7.1 Controlli alternativi, compensativi, complementari e correlati

6.7.2 Controlli di prevenzione, recupero e rilevazione

6.8 Conclusione

7 Analisi del rischio

7.1 Metodi di analisi

7.1.1 Metodi quantitativi

7.1.2 Metodi qualitativi

7.2 Il valore degli asset

7.2.1 Valutare le informazioni

7.2.2 Il rischio privacy

7.2.3 Chi assegna i valori alle informazioni

7.2.4 Valutare gli altri asset

7.2.5 Valutare gli asset IoT e industriali

7.3 Valutare la verosimiglianza delle minacce

7.3.1 Quali valori assegnare alle minacce

7.3.2 Chi assegna i valori alle minacce

7.4 Il rischio intrinseco

7.4.1 Rischio intrinseco quantitativo

7.4.2 Rischio intrinseco qualitativo

7.5 Valutare le vulnerabilità e i controlli

7.5.1 Identificare i controlli ideali

7.5.2 Quali valori assegnare ai controlli

7.5.3 Chi assegna i valori ai controlli

7.6 Il livello di rischio

7.6.1 Livello di rischio quantitativo

7.6.2 Livello di rischio qualitativo

7.6.3 Conclusioni

7.7 Ulteriori riflessioni sulle aggregazioni

8 Ponderazione del rischio

9 Trattamento del rischio

9.1 Le opzioni di trattamento del rischio

9.1.1 Evitare o eliminare il rischio

9.1.2 Aumentare il rischio

9.1.3 Modificare la probabilità della minaccia (Prevenire)

9.1.4 Modificare le conseguenze (Recuperare)

9.1.5 Condividere il rischio

9.1.6 Mantenere il rischio (Accettare)

9.2 Piano di trattamento del rischio

9.3 Scelta e attuazione delle azioni di riduzione

9.3.1 Riesaminare il piano delle azioni

9.3.2 Il piano delle azioni

9.3.3 Efficacia delle azioni

9.3.4 Tenuta sotto controllo del piano di azioni

10 Monitoraggio e riesame del rischio

10.1 Analisi del rischio operativo

10.2 L'integrazione delle analisi del rischio

III Minacce e controlli di sicurezza delle informazioni

11 Tecniche di minaccia

11.1 Intrusione nella sede o nei locali da parte di malintenzionati

11.2 Intrusione nei sistemi informatici

11.3 Social engineering e frodi

11.4 Furto d'identità

11.5 Danneggiamento di apparecchiature fisiche

11.6 Danneggiamenti dei programmi informatici

11.7 Furto di apparecchiature IT o di impianti

11.8 Furto di documenti fisici

11.9 Intercettazioni di emissioni elettromagnetiche

11.10 Interferenze da emissioni elettromagnetiche

11.11 Lettura e copia di documenti IT

11.12 Modifica di documenti informatici

11.13 Trattamento scorretto delle informazioni

11.14 Malware

11.15 Copia e uso illegale di software

11.16 Uso non autorizzato di servizi IT esterni

11.17 Uso non autorizzato di sistemi e servizi informatici offerti dall'organizzazione

11.18 Recupero di informazioni

11.19 Esaurimento o riduzione delle risorse

11.20 Intercettazione delle comunicazioni

11.21 Invio di dati a persone non autorizzate

11.22 Invio e ricezione di dati non accurati

11.23 Ripudio di invio da parte del mittente

11.24 IoT, OT, IIOT

11.25 Intelligenza artificiale

12 I controlli di sicurezza

12.1 Documenti

12.1.1 Tipi di documenti

12.1.2 Come scrivere i documenti

12.1.3 Approvazione e distribuzione

12.1.4 Archiviazione delle registrazioni

12.1.5 Tempo di conservazione

12.1.6 Verifica e manutenzione dei documenti

12.1.7 Documenti di origine esterna

12.2 Politiche di sicurezza delle informazioni

12.3 Organizzazione per la sicurezza delle informazioni

12.3.1 Organizzazione

12.3.2 Separazione dei ruoli

12.3.3 Gestione dei progetti

12.3.4 Rapporti con le autorità

12.3.5 Monitoraggio delle minacce

12.4 Gestione del personale

12.4.1 Inserimento del personale

12.4.2 Uscita del personale e cambiamenti di posizione

12.4.3 Competenze e sensibilizzazione

12.4.4 Lavoro fuori sede

12.5 Gestione degli asset

12.5.1 Informazioni

12.5.2 Identificazione, censimento e proprietà degli asset

12.6 Controllo degli accessi

12.6.1 Credenziali e identificazione

12.6.2 Autenticazione

12.6.3 Autorizzazioni

12.7 Crittografia

12.7.1 Algoritmi simmetrici e asimmetrici

12.7.2 Le funzioni hash

12.7.3 Protocolli crittografici

12.7.4 Chiavi crittografiche

12.7.5 Servizi fiduciari

12.7.6 Normativa applicabile alla crittografia

12.8 Sicurezza fisica

12.8.1 Sicurezza della sede

12.8.2 Sicurezza delle apparecchiature

12.8.3 Archivi fisici

12.9 Conduzione dei sistemi informatici

12.9.1 Documentazione

12.9.2 Configurazione dei dispositivi e dei sistemi informatici

12.9.3 Gestione dei cambiamenti

12.9.4 Malware

12.9.5 Backup

12.9.6 Logging e monitoraggio

12.9.7 Gestione della capacità

12.9.8 Dispositivi portatili e personali

12.9.9 Cancellazione dei dati

12.10 Sicurezza delle comunicazioni

12.10.1 Servizi autorizzati

12.10.2 Segmentazione della rete

12.10.3 Sicurezza della rete

12.10.4 Scambi di informazioni

12.11 Acquisizione, sviluppo e manutenzione

12.11.1 Acquisizione dei sistemi IT

12.11.2 Internet of things

12.11.3 Intelligenza artificiale

12.12 Gestione dei fornitori

12.12.1 Gli accordi e i contratti con i fornitori

12.12.2 Selezione dei fornitori

12.12.3 Monitoraggio dei fornitori

12.12.4 Cloud computing e fornitori

12.12.5 L'acquisizione di prodotti informatici e lo sviluppo affidato all'esterno

12.12.6 Le assicurazioni

12.13 Gestione degli incidenti

12.13.1 Ruoli e procedure

12.13.2 Processo di gestione degli incidenti

12.13.3 Controllo delle vulnerabilità

12.13.4 Gestione dei problemi

12.13.5 Gestione delle crisi

12.13.6 Digital forensics

12.14 Continuità operativa (Business continuity)

12.14.1 La business impact analysis (BIA)

12.14.2 Valutazione del rischio per la continuità operativa

12.14.3 Obiettivi e strategie di ripristino

12.14.4 I piani di continuità

12.14.5 Test e manutenzione

12.15 Conformità

12.15.1 Normativa vigente

12.15.2 Contratti

12.15.3 Audit

12.15.4 Vulnerability assessment

12.15.5 Il riesame del sistema di gestione

IV I requisiti di un sistema di gestione per la sicurezza delle informazioni

13 Le norme ISO e l'HLS

13.1 Specifiche e linee guida

13.2 Le norme della famiglia ISO/IEC 27000

13.3 ISO/IEC 27701

13.4 L'HLS

13.5 Storia della ISO/IEC 27001

13.6 Come funziona la normazione

14 Il miglioramento continuo e il ciclo PDCA

14.1 Il miglioramento continuo

14.2 Il ciclo PDCA

14.2.1 Pianificare

14.2.2 Fare

14.2.3 Verificare

14.2.4 Intervenire

14.2.5 La natura frattale del ciclo PDCA

15 I requisiti di sistema

15.1 Ambito di applicazione dello standard

15.2 Riferimenti normativi della ISO/IEC 27001

15.3 Termini e definizioni della ISO/IEC 27001

15.4 Contesto dell'organizzazione e ambito del SGSI

15.4.1 Il contesto dell'organizzazione

15.4.2 L'ambito del SGSI

15.4.3 Sistema di gestione per la sicurezza delle informazioni

15.5 Leadership

15.5.1 Politica per la sicurezza delle informazioni

15.5.2 Ruoli e responsabilità

15.6 Pianificazione

15.6.1 I rischi relativi all'efficacia del sistema di gestione

15.6.2 Valutazione del rischio relativo alla sicurezza delle informazioni

15.6.3 Il trattamento del rischio relativo alla sicurezza delle informazioni

15.6.4 Le azioni

15.6.5 Obiettivi

15.7 Processi di supporto

15.7.1 Risorse

15.7.2 Competenze e consapevolezza

15.7.3 Comunicazione

15.7.4 Informazioni documentate

15.8 Attività operative

15.8.1 La pianificazione e il controllo dei processi operativi

15.8.2 Valutazione e trattamento del rischio relativo alla sicurezza delle informazioni

15.9 Valutazione delle prestazioni

15.9.1 Monitoraggio, misurazione, analisi, valutazione

15.9.2 Audit interni

15.9.3 Riesami di Direzione

15.10 Miglioramento

15.10.1 Non conformità

15.10.2 Azioni correttive

15.10.3 Azioni preventive

15.10.4 Miglioramento continuo

15.11 Appendice A della ISO/IEC 27001

15.12 Bibliografia della ISO/IEC 27001

V Appendici

A Gestire gli auditor

A.1 L'auditor è un ospite

A.2 L'auditor è un partner

A.3 L'auditor è un fornitore

A.4 L'auditor è un auditor

B I primi passi per realizzare un SGSI

B.1 Individuare l'ambito

B.2 Coinvolgere i manager

B.3 Gestire i documenti

B.4 Miglioramento

B.5 Formare il personale

B.6 Gap analysis

B.7 Realizzare il sistema di gestione

C La certificazione di un sistema di gestione

C.1 Gli attori

C.2 Il percorso di certificazione

C.2.1 Il contratto

C.2.2 L'audit di certificazione

C.2.3 Raccomandazione ed emissione del certificato

C.2.4 Audit straordinario

C.2.5 Audit periodici

C.2.6 Audit di ricertificazione

C.3 I bandi di gara

C.4 Standard e certificazioni per settori specifici

C.5 Accreditamento

C.5.1 Accreditamento per la certificazione dei sistemi di gestione

C.5.2 Certificazione e accreditamento dei laboratori

C.5.3 Certificazione dei prodotti, servizi e processi

C.5.4 Certificazione della sicurezza informatica, Common Criteria e Cybersecurity Act

C.5.5 Certificazione e perimetro di sicurezza nazionale

C.5.6 Certificazione di processo e il GDPR

C.6 I falsi miti della certificazione

D Common Criteria (ISO/IEC 15408) e FIPS 140-3

D.1 Common Criteria (ISO/IEC 15408)

D.1.1 Generalità

D.1.2 Tecnica della valutazione

D.1.3 Problemi dovuti a una scarsa conoscenza dei Common Criteria

D.2 FIPS 140-3

D.2.1 Generalità

D.2.2 Tecnica della valutazione

D.2.3 Problemi dovuti all'impiego della FIPS 140-3

E Requisiti per i cambiamenti

E.1 Requisiti funzionali di controllo accessi

E.2 Requisiti sulla connettività

E.3 Requisiti funzionali relativi alla crittografia

E.4 Requisiti di monitoraggio

E.5 Requisiti di capacità

E.6 Requisiti architetturali

E.7 Requisiti applicativi

E.8 Requisiti di servizio

F Requisiti per contratti e accordi con i fornitori

F.1 Requisiti per i fornitori di prodotti

F.2 Requisiti per i fornitori di servizi non informatici

F.3 Requisiti per i fornitori di servizi informatici

G I controlli della ISO/IEC 27002:2022

Bibliografia

Presentazione e ringraziamenti

Pensino ora i miei venticinque lettori che impressione dovesse fare, sull'animo del poveretto, quello che s'è raccontato.

Alessandro Manzoni, I promessi sposi

La prima versione di questo libro è datata 2002. Negli anni ho fortunatamente incontrato più di 25 persone che l'avevano letto e apprezzato; purtroppo, spesso, l'avevano preso in prestito da una biblioteca e questo non ha aiutato le vendite.

Nel 2014 scrissi una seconda versione (con i moai dell'Isola di Pasqua in copertina) con le idee maturate durante i corsi di formazione, le presentazioni, le discussioni con colleghi e amici, gli incontri a livello nazionale e internazionale per scrivere la ISO/IEC 27001:2013. In alcuni casi, alcune delle convinzioni del 2002 erano cambiate, grazie ai tanti audit e progetti di consulenza.

La terza versione del 2017 (con il Perito Moreno in copertina) era un aggiornamento minore, con qualche nuovo esempio e idea nata durante la partecipazione alla scrittura della ISO/IEC 27003:2017. Ne ricavai anche una versione in lingua inglese con il supporto di Maël-Sanh Perrier e, grazie ai suoi suggerimenti, colsi l'occasione per introdurre molti miglioramenti.

Questa quarta versione (con i Giganti della Sila in copertina) nasce con la disponibilità delle bozze finali delle ISO/IEC 27001:2022 e ISO/IEC 27002:2022 e dalla necessità di aggiornare la descrizione dei controlli di sicurezza. Ho colto l'occasione per inserire ulteriori aggiornamenti sulle

tecnologie (citando IoT, OT, intelligenza artificiale, eccetera), sulle minacce e gli accreditamenti. Questa volta, per l'inglese, mi ha aiutato Simona Cifarelli, che ha fatto un ottimo lavoro, nonostante il poco tempo che le ho dato.

La prima parte riporta le basi della sicurezza delle informazioni e dei sistemi di gestione per la sicurezza delle informazioni.

La seconda parte descrive la valutazione del rischio, con un'ampia parte teorica bilanciata da molti esempi; i calcoli presentati non sono necessari per comprendere appieno i concetti esposti.

La terza parte descrive le minacce e i controlli di sicurezza. È basata sugli appunti, a loro volta basati sulla ISO/IEC 27002, che utilizzo per le attività di audit e di consulenza.

La quarta parte illustra i requisiti della ISO/IEC 27001 secondo la mia interpretazione maturata durante i lavori di scrittura della norma stessa, i corsi di formazione e le discussioni con i clienti.

Le prime tre appendici riportano alcune brevi presentazioni fatte a margine di corsi di formazione (sulla gestione degli auditor e sulla certificazione) o per l'avvio di progetti di certificazione (sui passi per realizzare un SGSI).

L'appendice sui Common Criteria e sulle FIPS 140 è un gentile omaggio di Stefano Ramacciotti.

Le successive appendici sulla gestione dei cambiamenti e dei fornitori sono tratte da alcune mie liste di riscontro. L'ultima correla i controlli della ISO/IEC 27002:2022 con i paragrafi di questo libro.

Ci tengo a precisare che questo testo si basa molto sulla ISO/IEC 27001, ma non è una guida ufficiale alla sua interpretazione: quella è pubblicata come ISO/IEC 27003:2017.

Questo libro è stato scritto per quanti vogliono imparare e approfondire cos'è la sicurezza delle informazioni; ho infatti cercato di rispondere a tutte le domande che mi sono state rivolte in questi anni.

Credo inoltre che alcune riflessioni possano interessare chi conosce già la materia ed essere lo spunto per nuove discussioni. Ciascuno ha i propri punti di vista, anche diversi dai miei, e un confronto potrebbe migliorare le nostre competenze.

Il testo delle norme qui riportato non è identico a quello delle traduzioni ufficiali, sia per questioni di diritto d'autore, sia perché, in alcuni casi, volevo rendere il testo più significativo.

Alcune definizioni sono state lievemente modificate da quelle ufficiali per renderle, a mio parere, più comprensibili. Tra parentesi quadre sono riportate eventuali aggiunte. Le cancellazioni sono evidenziate dal simbolo “[...].”

Ci tengo a ringraziare tre persone per l'aiuto dato nella scrittura di questo libro, in rigoroso ordine alfabetico:

Massimo Cottafavi, esperto di Governance, risk and compliance, con cui discuto da tanti anni e che ha letto le bozze e mi ha dato un po' di testo da copiare oltre, per ogni edizione, utili idee;

Roberto Gallotti, inflessibile correttore di bozze e fornitore di idee; anche se non può dichiararsi esperto di sicurezza delle informazioni, è un professionista da cui vorrei imparare di più;

Stefano Ramacciotti, con cui ho discusso di sicurezza delle informazioni in giro per il mondo durante alcuni meeting dell'SC 27 e che ha anche contribuito a delle parti di testo (in particolare, l'appendice sui Common Criteria, aggiornata a ogni edizione, l'esempio di Fort Knox e quanto riguarda le tre e le quattro P);

Monica Perego, la prima idraulica della privacy, bravissima e apprezzatissima da chiunque la conosce (e infatti le vendite aumentano ogni volta che cita questo libro); ho avuto l'onore di considerarla mia amica e di ricevere i suoi suggerimenti per migliorare questo libro.

Queste persone sono tra i professionisti più preparati e simpatici che abbia avuto modo di conoscere in questi anni e sono molto orgoglioso di essere riuscito a rubare loro tempo e energie.

Ringrazio anche Franco Ruggieri, Pierfrancesco Maistrello e Francesca Lazzaroni con i quali ho avuto modo di discutere di molte cose in questi anni e che mi hanno fornito preziosi riscontri. Ringrazio anche gli Idraulici della privacy, che mi hanno permesso di migliorare le mie conoscenze in ambito privacy e con i quali ho pubblicato un libro [65] il cui ricavato va in beneficenza.

Infine ringrazio tutti coloro (clienti, colleghi, concorrenti, partecipanti ai corsi, eccetera) con cui in questi anni mi sono confrontato e che non hanno avuto paura a condividere con me idee e incompetenze reciproche anche attraverso il mio blog blog.cesaregallotti.it e la mia newsletter mensile: persone preparate, ma

consapevoli che la nostra materia è estremamente mutevole e non esiste nessuno più bravo degli altri.

Contatti

Per contattarmi, segnalare errori e proporre miglioramenti, i miei riferimenti sono disponibili su www.cesaregallotti.it.

Invito quanti sono interessati ad abbonarsi alla mia newsletter. Le modalità sono riportate sul mio sito web.

Avvertenza

I link riportati in questo libro sono stati verificati il 22 dicembre 2021.

Capitolo 1

Introduzione

Cosa [...] c'era da interpretare in “Fate i bravi”?

John Niven, A volte ritorno

Da sempre l'uomo sente la necessità di avere le proprie informazioni al sicuro. In particolare desideriamo che i dati personali (per esempio, il nostro stato di salute e il nostro estratto di conto) siano accessibili solo a poche fidate persone e siano accurati e corretti, che non vengano utilizzati impropriamente per telefonarci a casa o diffamarci pubblicamente sui social network e che siano velocemente disponibili, soprattutto su Internet.

Quanto detto riguarda la percezione individuale di cosa si intende per “sicurezza delle informazioni”. Anche un’impresa o un qualsiasi ente ha una percezione di cosa si intende per “sicurezza delle informazioni”; per esempio: segretezza dei progetti innovativi e dell’elenco dei propri clienti e partner, accuratezza di tutti i dati economici e di produzione, disponibilità dei sistemi informatici.

Nella prima parte di questo libro sono illustrati i concetti fondamentali relativi alla sicurezza delle informazioni, inclusa la sua stessa definizione.

Il termine sicurezza, però, cela in sé una contraddizione. Sicurezza, infatti, fa venire in mente qualcosa di assoluto e incontrovertibile, cioè qualcosa di impossibile nella realtà.

Spesso si dice che Fort Knox, dove si trovano le riserve monetarie degli USA, è

uno dei luoghi più sicuri al mondo: sofisticati sensori, barriere perimetrali e allarmi sono tutti ai massimi livelli. Come se non bastassero, è sede di un comando di Marines pronti a intervenire per qualsiasi problema. Fort Knox è riconosciuto come sinonimo di luogo sicuro. Ma come reagirebbe la struttura a un impatto con un meteorite di un chilometro di diametro?

Come si può vedere da questo semplice esempio, non ha senso parlare di sicurezza in senso assoluto, ma solo in senso relativo. Fort Knox non è infatti resistente a un grosso meteorite. Per questo motivo bisogna diffidare di chiunque offre prodotti o soluzioni sicuri al 100%. Una tale affermazione classifica subito la persona come scarsamente competente o come un imbonitore che vuole vendere qualcosa.

Deve essere individuato il livello adeguato di sicurezza che si vuole ottenere attraverso la valutazione del rischio. Il livello di sicurezza deve essere raggiunto attraverso opportune azioni di trattamento. Nel caso in cui quel livello non possa essere raggiunto, le carenze devono essere analizzate e, se il caso, accettate.

Nel tempo, la valutazione deve essere ripetuta per verificare se il livello di sicurezza desiderato e quello attuato siano ancora validi. Queste attività di valutazione, azione o accettazione e ripetizione costituiscono la gestione del rischio (risk management), oggetto della seconda parte del libro.

Nella terza parte sono illustrati i controlli di sicurezza, ossia le misure utili per garantire la sicurezza delle informazioni. Queste sono soprattutto di tipo organizzativo e non tecnologico. Infatti, buoni processi portano a scegliere buoni e adeguati prodotti e a gestirli correttamente. Non è vero l'inverso: un buon prodotto non conduce ad avere buoni processi.



Buoni
processi

Buone scelte
tecnologiche

Figura 1.0.1:

Processi e prodotti

La quarta parte tratta dei requisiti della ISO/IEC 27001 per i sistemi di gestione per la sicurezza delle informazioni.

Un po' di storia

Come già accennato, la sicurezza delle informazioni è stata oggetto di attenzione sin dagli albori dell'umanità, basta pensare ai misteri collegati a diverse religioni. Per quanto riguarda il passato, Cesare parla di sistemi per evitare l'intercettazione dei messaggi in guerra (al capitolo 48 del libro V del De bello gallico); l'utilizzo della partita doppia per garantire l'integrità della contabilità, descritta nel 1494 da Luca Pacioli, è sicuramente precedente al Duecento.

Nelle imprese, fino alla diffusione dell'informatica, la sicurezza delle informazioni si riferiva ai documenti cartacei e alle comunicazioni orali; oggi deve comprendere anche la sicurezza informatica.

Questa, fino agli anni Novanta, era gestita dagli addetti informatici, senza alcun collegamento con la tutela del patrimonio, ossia con la corporate security, anche se i rischi di furto di informazioni e di spionaggio erano comunque presi in considerazione.

In quegli anni si verificarono fenomeni importanti relativamente all'informatica

e al contesto economico e sociale:

la diffusione degli strumenti informatici, grazie ai personal computer e a interfacce sempre più intuitive: Microsoft Windows è del 1985 e Mosaic, il primo browser grafico per navigare sul web, è del 1993;

l'aumento delle persone e dei dispositivi connessi su Internet (a sua volta non progettato per la sicurezza [148]);

l'aumento delle minacce informatiche note al grande pubblico: il primo virus, quello di Morris, è del 1988;

la pubblicazione di normative con riferimento alla sicurezza informatica: nel 1993 fu emendato il Codice Penale per includervi i casi di criminalità informatica (Legge 547) e nel 1996 fu emanata la prima versione della Legge sulla privacy (Legge 675) a cui fu affiancato nel 1999 un disciplinare tecnico (DPR 318);

l'aumento della conflittualità sociale dovuto alle ristrutturazioni di tante imprese;

il ricorso a sempre più numerosi fornitori e l'aumento di relazioni con attori esterni rappresentate in figura 1.0.2.

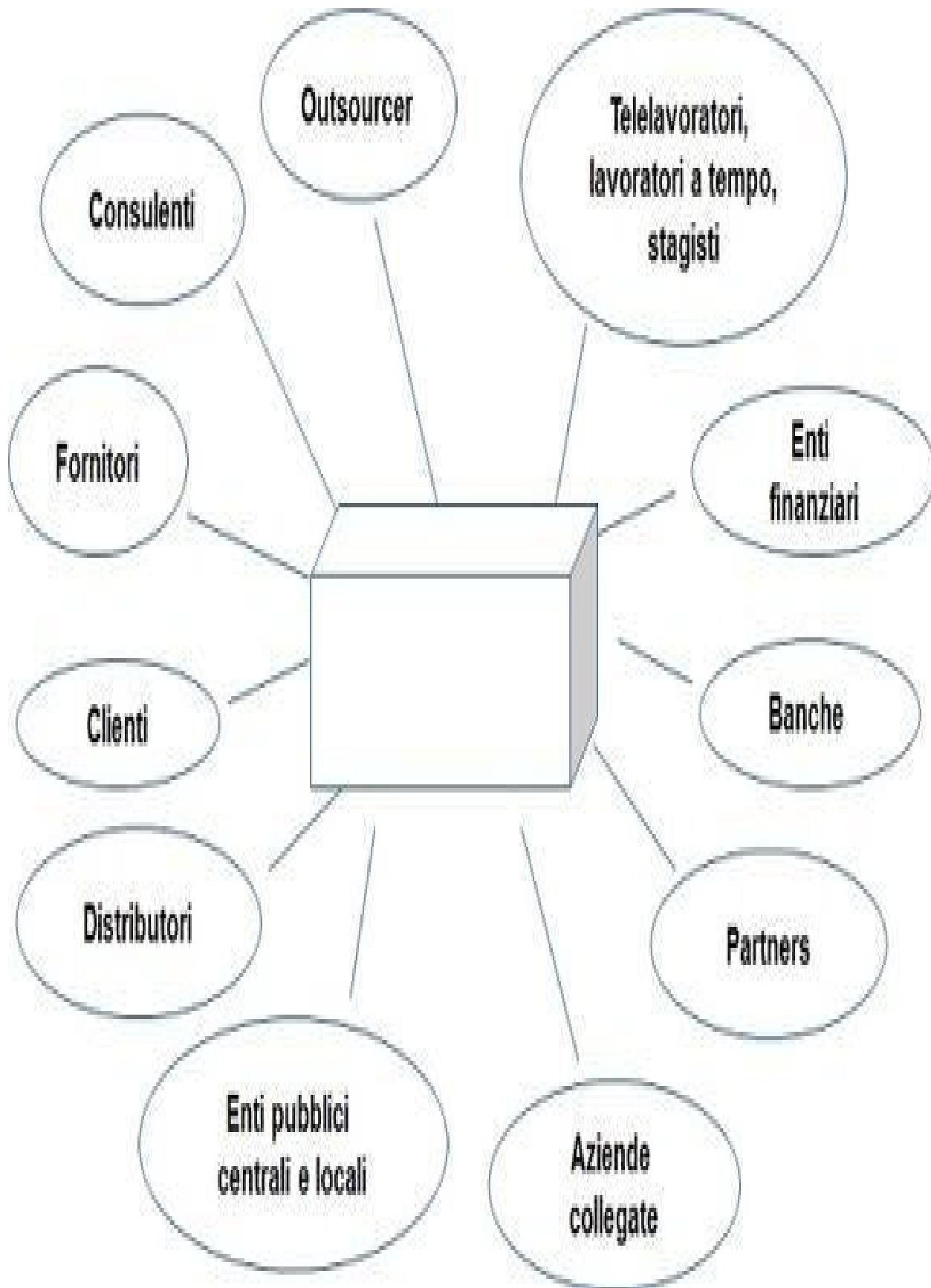


Figura 1.0.2:

L'impresa aperta

Tutto questo ha fatto percepire come rilevanti le minacce relative alla sicurezza delle informazioni in generale e informatica in particolare, come illustrato in figura 1.0.3.

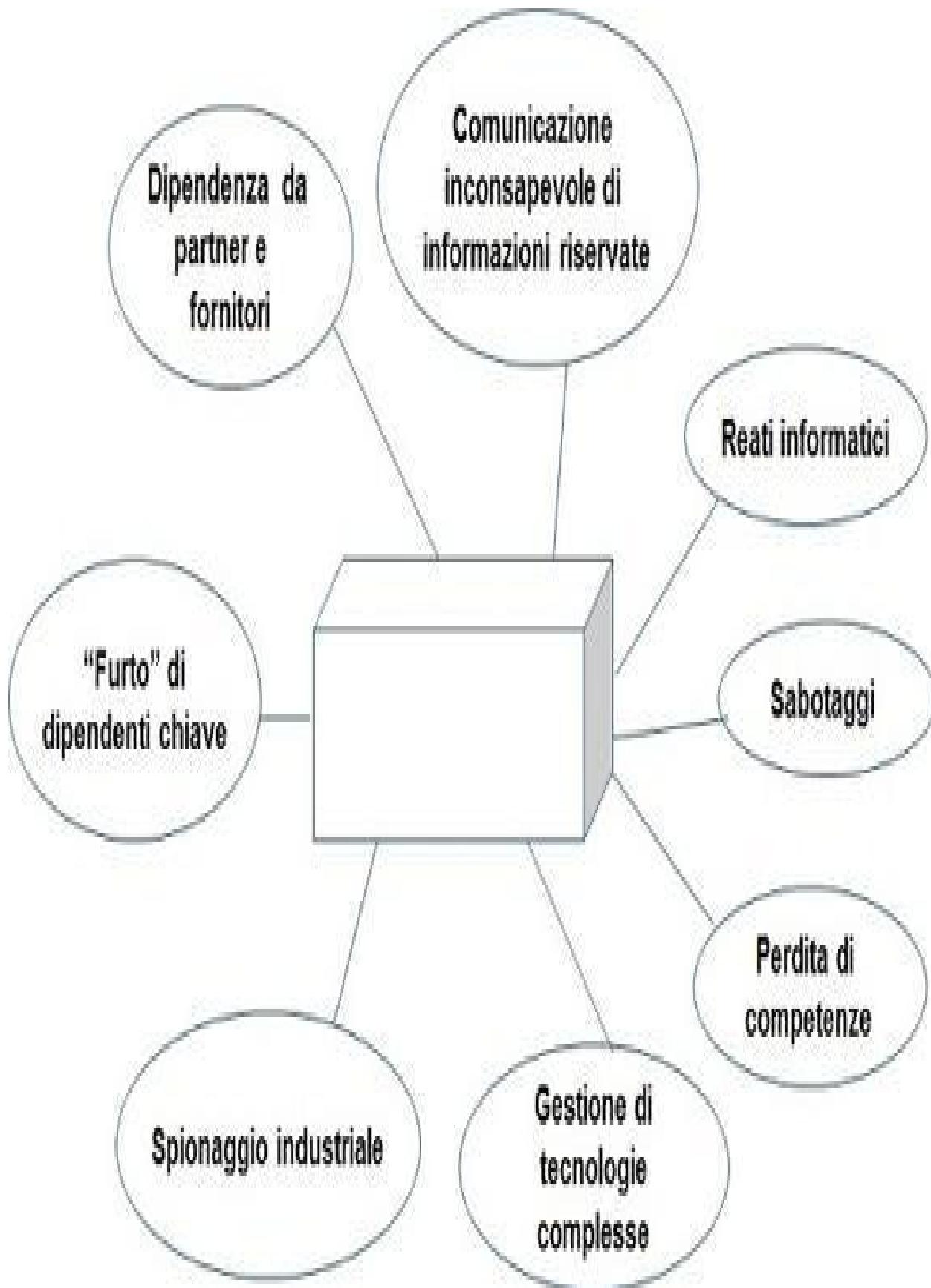


Figura 1.0.3:

Nuove minacce

Negli anni Novanta cambia anche l'approccio alla sicurezza delle organizzazioni: si specializzano gli ambiti di intervento (informatica, siti fisici, persone) perché richiedono diverse competenze, si stabiliscono delle priorità di intervento sulla base di valutazioni del rischio e, in generale, si percepisce la sicurezza come attività indispensabile per garantire la sostenibilità delle organizzazioni nel tempo.

Negli anni, le esigenze di sicurezza non si sono ridotte. Questo a causa degli eventi più recenti (11 settembre, spionaggio industriale, eccetera), delle evoluzioni normative in materia di sicurezza delle informazioni e della sempre crescente globalizzazione delle imprese.

Per tutti questi motivi sono state introdotte metodologie e pratiche per rendere più strutturate le attività riguardanti la sicurezza delle informazioni. Tra le iniziative più importanti si ricordano quelle relative alla sicurezza dei prodotti e sistemi informatici (TCSEC del 1983, ITSEC del 1991, Common Criteria del 1994 e le Special Publication del NIST¹ emesse dai primi anni Novanta), alla sicurezza delle informazioni (BS 7799 del 1995, di cui si approfondirà la storia nel paragrafo 13.5) e alle metodologie di valutazione del rischio relativo alla sicurezza delle informazioni (CRAMM del 1987, Marion del 1990 e Mehari del 1995) [27].

Negli anni 2000, molti Paesi presero consapevolezza dell'importanza della protezione delle reti informatiche e di Internet (rendendo diffusi i termini cyberspace e cybersecurity). Inizialmente gli USA promossero iniziative

legislative (tra cui il Cybersecurity and Infrastructure Security Agency Act del 2018), avviarono agenzie specializzate (nel 2018 fu creata la Cybersecurity & Infrastructure Security Agency, ma già in precedenza operavano il NIST e l’NSA) e programmi per ridurre i rischi informatici delle infrastrutture critiche (nel 2013 iniziarono i lavori per la pubblicazione del NIST Cybersecurity Framework). Successivamente altri Paesi avviarono iniziative simili; tra di essi l’Unione Europea, che aveva già creato nel 2004 ENISA (European Network and Information Security Agency, oggi European Union Agency for Cybersecurity) e poi approvò la Direttiva NIS del 2018 e il Cybersecurity act del 2019, a cui l’Italia affiancò la normativa relativa al “perimetro di sicurezza nazionale cibernetica” nel 2019.

Dall’altra parte furono considerati come sempre più importanti i diritti dei cittadini nell’ambito digitale. Da questo punto di vista, le iniziative furono avviate principalmente dall’Unione europea, con la Direttiva privacy del 1995, seguita dall’importantissimo GDPR del 2016 (vedere il paragrafo 12.15.1.9), imitato da moltissimi Paesi inclusa la Cina. Ma non solo: la UE avviò nel 2018 il programma “New Deal for Consumers”, anche per migliorare ulteriormente le normative già attuate e relative al commercio elettronico e alla protezione dei consumatori in generale, dopo aver comunque segnalato le esigenze di sicurezza informatica in numerose altre normativa, inclusa quella relativa alla sicurezza dei dispositivi medici.

Queste normative richiedono solitamente alle organizzazioni di valutare il rischio relativo alla sicurezza delle informazioni e di trattarlo con opportuni controlli di sicurezza. Il risultato fu un aumento generale della sicurezza delle informazioni, ma anche, in molti casi, degli oneri burocratici per molte organizzazioni.

Un ulteriore fenomeno si è affermato negli stessi anni e ne comprende altri: Internet of Things (IoT), Operational technology (OT) e domotica. Si tratta dell’informatizzazione e della connessione a Internet di dispositivi e strumenti, sempre più numerosi, con limitate capacità, ma spesso collegati a reti

informatiche complesse, con attive anche connessioni wi-fi. Questi dispositivi sono ormai dappertutto: nelle case e negli uffici con le TV smart e gli elettrodomestici “intelligenti”, negli impianti anche necessari per la sicurezza delle persone, negli impianti produttivi, nelle reti di distribuzione di gas, energia elettrica e acqua, nei trasporti e nelle infrastrutture ferroviarie e stradali. L’elenco è ormai infinito e include tecnologie molto diverse tra loro. Per la loro facilità di connessione, i loro costi sempre più ridotti e la diversità di tecnologie sono difficilmente controllabili dalle organizzazioni.

È in questo contesto che si è reso necessario un ulteriore allargamento del perimetro della sicurezza, non solo legata alla sicurezza delle informazioni, ma alla sicurezza di tutti gli strumenti attaccabili con dispositivi informatici, importantissimi per la produttività, ma difficilmente configurabili e, anche se sembra paradossale, facili da compromettere. I potenziali impatti non sono più sulle informazioni, ma sulla sicurezza fisica e la salute delle persone, la qualità e disponibilità delle produzioni nel settore manifatturiero e l'affidabilità di innumerevoli servizi.

Ulteriore fenomeno in crescita riguarda l’intelligenza artificiale, che va progettata in modo da non compromettere le persone e la proprietà e protetta durante il suo funzionamento, ma che può anche essere usata come strumento di difesa e di attacco.

Note

¹<http://csrc.nist.gov>.

Parte I

Le basi

Capitolo 2

Sicurezza delle informazioni e organizzazione

Where is the life we have lost in living?

Where is the wisdom we have lost in knowledge?

Where is the knowledge we have lost in information?

Thomas Stearns Eliot, The rock

In questo capitolo sono fornite le definizioni di base della sicurezza delle informazioni. Nel capitolo successivo è specificato cos'è un sistema di gestione per la sicurezza delle informazioni.

Può essere interessante svolgere un piccolo esercizio: elencare i casi di notizie lette sul giornale o di eventi di cui siamo stati testimoni o vittime, collegati alla sicurezza delle informazioni. Ad esempio:

nel 48 p.e.v. la biblioteca di Alessandria fu incendiata con la conseguente distruzione del patrimonio librario²;

nel 1998, il Ministero delle Finanze inviò milioni di cartelle esattoriali sbagliate ai contribuenti³;

nel 2003 l'Italia sperimentò un blackout dovuto a un albero caduto sulla linea dell'alta tensione in Svizzera e che in alcune zone durò anche più di 24 ore⁴ rendendo indisponibili, tra gli altri, servizi informatici e di comunicazione;

nel 2007 alcuni disegni della F2007 della Ferrari entrarono in possesso della sua concorrente McLaren⁵;

nel 2010, il capo dell’antiterrorismo di Scotland Yard dovette rassegnare le dimissioni perché fotografato con un documento classificato “secret” sotto braccio e in bella vista⁶;

a settembre 2013, i social network di Alpitour furono violati e alcuni link modificati per indirizzare a siti web malevoli⁷;

a inizio 2013, i servizi di antispamming della Spamhaus furono bloccati da un attacco⁸;

a fine 2019, un’organizzazione, a causa di un colpo di vento, si vide volare numerosi documenti cartacei per strada⁹;

nel maggio 2020, EasyJet fu attaccata da malintenzionati che rubarono i dati dei passeggeri, inclusi numeri di carte di credito¹⁰;

nel marzo 2021, il data centre di OVH a Strasburgo andò a fuoco e molti sistemi rimasero indisponibili¹¹;

nell’agosto 2021, i sistemi informatici per la prenotazione dei vaccini COVID-19 della Regione Lazio rimasero indisponibili per quattro giorni a causa di un ransomware¹²;

a ottobre 2021 Facebook, WhatsApp e Instagram rimasero rimasti bloccati per 6 ore a causa di un errore di configurazione¹³.

Questi esempi illustrano come la sicurezza delle informazioni debba occuparsi di molti potenziali eventi negativi: incendi, eventi naturali, guasti di apparecchiature e impianti, errori umani, attacchi di malintenzionati, eccetera.

2.1

Dati e informazioni

Prima di discutere di dati e informazioni, è opportuno fornirne la definizione, presente in precedenti versioni dello standard ISO/IEC 27000. Nelle ultime versioni dello standard questa definizione non è più riportata, forse perché si preferisce far riferimento ai normali dizionari [118].

Informazione (Information data): conoscenza o insieme di dati che hanno valore per un individuo o un'organizzazione.

Le informazioni sono archiviate e trasmesse su supporti. Essi possono essere analogici o non digitali come la carta, le fotografie e i film su pellicola, o digitali come i computer e le memorie rimovibili (per esempio: chiavi USB, CD e DVD). Un caso particolare di supporto non digitale è l'essere umano, che nella sua mente conserva informazioni. Per la trasmissione si possono usare: posta tradizionale, telefono (ormai basato su tecnologia mista), reti informatiche e, sempre considerando il caso particolare degli esseri umani, conversazioni tra persone.

Da questo ragionamento risulta che, quando si parla di sicurezza delle informazioni, non ci si limita alla sicurezza informatica, ossia relativa alle informazioni in formato digitale e trattate dai sistemi dell'Information and communication technology, ma a tutti i sistemi utilizzati per raccogliere, modificare, conservare, trasmettere e distruggere le informazioni.

Questo è uno dei motivi per cui si preferisce parlare di “informazioni” e non di “dati”: il termine, intuitivamente, ha una valenza più ampia.

Più rigorosamente, la sicurezza delle informazioni include quella dei dati, come si deduce dalle quattro tipologie di rappresentazione della conoscenza [107]:

dati: insieme di singoli fatti, immagini e impressioni;

informazioni: dati organizzati e significativi;

conoscenza: informazioni recepite e comprese da un singolo individuo;

sapienza: conoscenze tra loro connesse che permettono di prendere decisioni.

Per completezza è necessario ricordare che il termine inglese information è un mass noun e quindi in italiano va tradotto al plurale.

2.2

Sicurezza delle informazioni

La ISO/IEC 27000 [83] definisce:

Sicurezza delle informazioni (Information security): preservazione della riservatezza, integrità e disponibilità delle informazioni.

È quindi necessario definire le tre proprietà sopra riportate (tra parentesi quadre vi sono delle aggiunte rispetto alla ISO/IEC 27000).

Riservatezza (Confidentiality): proprietà di un'informazione di non essere disponibile o rivelata a individui, entità o processi non autorizzati;

Integrità (Integrity): proprietà di accuratezza e completezza;

Disponibilità (Availability): proprietà di essere accessibile e utilizzabile [entro i tempi previsti] su richiesta di un'entità autorizzata.

Ci si riferisce spesso a queste proprietà come parametri RID e nel seguito sono descritte più approfonditamente.

2.2.1

Riservatezza

Alcuni riducono la sicurezza delle informazioni a questo parametro, ma si tratta di un approccio riduttivo.

In ambito informatico si estremizza dicendo che “il computer sicuro è il computer spento o, meglio, rotto”, oppure che “l’unico sistema realmente sicuro è un sistema spento, affogato in un blocco di cemento, sigillato in una stanza con pareti schermate col piombo e protetto da guardie armate; e anche in questo caso, si potrebbero avere dei dubbi” [28]. È evidente che questo approccio non considera la disponibilità delle informazioni.

La riservatezza è spesso associata alla segretezza, però la necessità di mantenere riservate le informazioni non implica la necessità di non rivelarle ad alcuno, ma di stabilire chi ha il diritto ad accedervi.

Non è semplice stabilire le caratteristiche di riservatezza di ogni informazione e chi può accedervi, come dimostra l’esempio seguente.

-

Esempio 2.2.1. In un’azienda italiana, i dati sul personale sono sicuramente riservati, ma persone diverse devono accedervi: il medico competente, l’amministrazione, i dirigenti, certi uffici pubblici, il commercialista e l’ufficio legale.

Ciascuno non dovrebbe accedere a tutti i dati, ma solo a una parte di essi: l’amministrazione alla sola busta paga, il medico ai soli dati sanitari, eccetera.

Il livello di riservatezza di un'informazione può variare nel tempo. Il caso più rappresentativo di questo concetto è il Freedom of Information Act statunitense che prevede la declassifica (ossia la rimozione dei vincoli di segretezza) delle informazioni governative non oltre i 50 anni dalla loro creazione.

Esempio 2.2.2. Le caratteristiche di un nuovo modello di automobile vanno tenute riservate. In fase di progettazione devono essere disponibili ai soli progettisti, in fase di produzione anche agli operai, ma in fase di commercializzazione devono, seppur parzialmente, essere disponibili al pubblico.

2.2.2

Integrità

Se un dato è scorretto o alterato in modo non autorizzato, vuol dire che non è sicuro.

Esempio 2.2.3. Richard Pryor, in Superman III del 1983, riesce a rubare soldi alla propria azienda dopo averne alterato il sistema di contabilità.

Senz'altro era autorizzato ad accedere al sistema e a vedere le informazioni registrate, dato che lavorava nell'ufficio della contabilità, ma non avrebbe dovuto alterarlo senza autorizzazione.

La cancellazione di un'informazione è una forma estrema di alterazione e, pertanto, riguarda l'integrità.

2.2.3

Disponibilità

La maggior parte delle persone, come già detto, intende la sicurezza delle informazioni come mantenimento della loro riservatezza. Molti informatici, per contro, soprattutto se impiegati in aziende commerciali, intendono la sicurezza delle informazioni come la capacità di renderle immediatamente disponibili a chi le richiede. Non è però possibile pretendere l'immediatezza in tutte le occasioni e quindi la proprietà di disponibilità può essere riformulata così: “le informazioni devono essere disponibili entro i tempi stabiliti a coloro che le richiedono e ne hanno il diritto”.

Esempio 2.2.4. I “tempi stabiliti” dipendono da vari fattori: nel contesto della borsa azionaria si tratta di qualche millisecondo, nel contesto di un sito web di commercio elettronico pochi secondi, in un’agenzia bancaria pochi minuti.

La disponibilità può avere impatti sulla riservatezza o l’integrità. È compito della Direzione stabilire a quali parametri dare maggiore importanza e comunicare questa scelta nella politica di sicurezza delle informazioni (paragrafo 12.2).

Esempio 2.2.5. I backup migliorano la disponibilità dei dati, ma aumentano i rischi di perdita di riservatezza a causa della duplicazione dei dati e della possibilità che possano essere rubati.

2.2.4

Altre proprietà di sicurezza

Le tre proprietà sopra descritte costituiscono la definizione classica di sicurezza delle informazioni. Alcuni preferiscono aggiungerne altre: autenticità, completezza, non ripudiabilità, tracciabilità e la possibilità di assicurare il diritto all'oblio.

Le informazioni sono autentiche quando attestano la verità. Questa proprietà è caso particolare di integrità: un'informazione non autentica equivale a un'informazione modificata senza autorizzazione.

La proprietà di completezza di un'informazione richiede che non abbia carenze. Una carenza è equivalente a una cancellazione, totale o parziale, non autorizzata di dati e quindi è un caso particolare di integrità.

Un'informazione corretta, ma successivamente smentita dal suo autore è un'informazione ripudiata. È facile capire quanto sia importante avere informazioni non ripudiabili: le promesse sono mantenute e i debiti pagati nei tempi stabiliti.

Un'informazione non ripudiabile, per esempio, è quella riportata da un documento firmato dal suo autore. In altre parole, un'informazione è non ripudiabile se è completa di firma o di un suo equivalente; quindi anche questa proprietà può essere vista come caso particolare dell'integrità.

La tracciabilità è la possibilità di sapere chi ha o avuto accesso a un'informazione e chi l'ha modificata. È possibile osservare che i dati necessari

per tracciare l'informazione devono far parte dell'informazione stessa e quindi anche la tracciabilità può essere visto come caso particolare di quello di integrità,

La normativa in materia di privacy ha evidenziato il diritto alla cancellazione, diventato noto come diritto all'oblio. Questo prevede che le informazioni relative a una persona fisica siano eliminate quando dichiarato in fase di raccolta dei dati o, in certe condizioni, e se non in contrasto con la normativa vigente, quando richiesto dalla persona stessa. La necessità di soddisfare questa proprietà richiede di predisporre archivi e sistemi informatici in modo da soddisfare le richieste¹⁴.

2.2.5

Gli impatti sui parametri RID

Ciascun evento può avere impatti su uno o più parametri RID.

Esempio 2.2.6. Possiamo considerare alcuni eventi riportati nella successiva tabella 2.2.1.

Alcune attribuzioni non sono condivisibili da tutti. Una delle ragioni è che bisogna stabilire se un parametro vada assegnato considerando l'effetto diretto dell'evento o anche quello indiretto: in caso di furto delle password, come accadde alla Sony nel 2011¹⁵, il danno diretto riguarda strettamente la riservatezza, ma poi potrebbe riguardare l'integrità (se quelle password sono usate per alterare dei dati) e la disponibilità (la Sony dovette bloccare il sito per più mesi).

L'incendio viene associato all'integrità e alla disponibilità, ma potrebbe essere associato anche alla riservatezza se l'evacuazione di un edificio consente l'accesso a persone non autorizzate oppure comporta la dispersione fuori sede di documenti cartacei riservati.

Esempio di incidente	R	I	D
Incendio	x		x
Cartelle esattoriali sbagliate		x	
Blackout			x

Virus blocca i sistemi informatici	X	X	X
Furto disegni industriali	X		
Diffusione documenti	X		
Guasto impianto			X
Modifica scorretta sistema IT	X	X	X
Furto di password da parte di esterni	X	X	X
Modifica non autorizzata di informazioni		X	X
Attacchi di Denial of Service			X

Tabella 2.2.1:

Esempio eventi e parametri RID

2.3

Sicurezza informatica e cybersecurity

Si parla di sicurezza informatica quando ci si limita alla sicurezza delle informazioni sui sistemi informatici. A rigore, alcuni sistemi informatici (per esempio quelli industriali) potrebbero non essere considerati come pertinenti le informazioni.

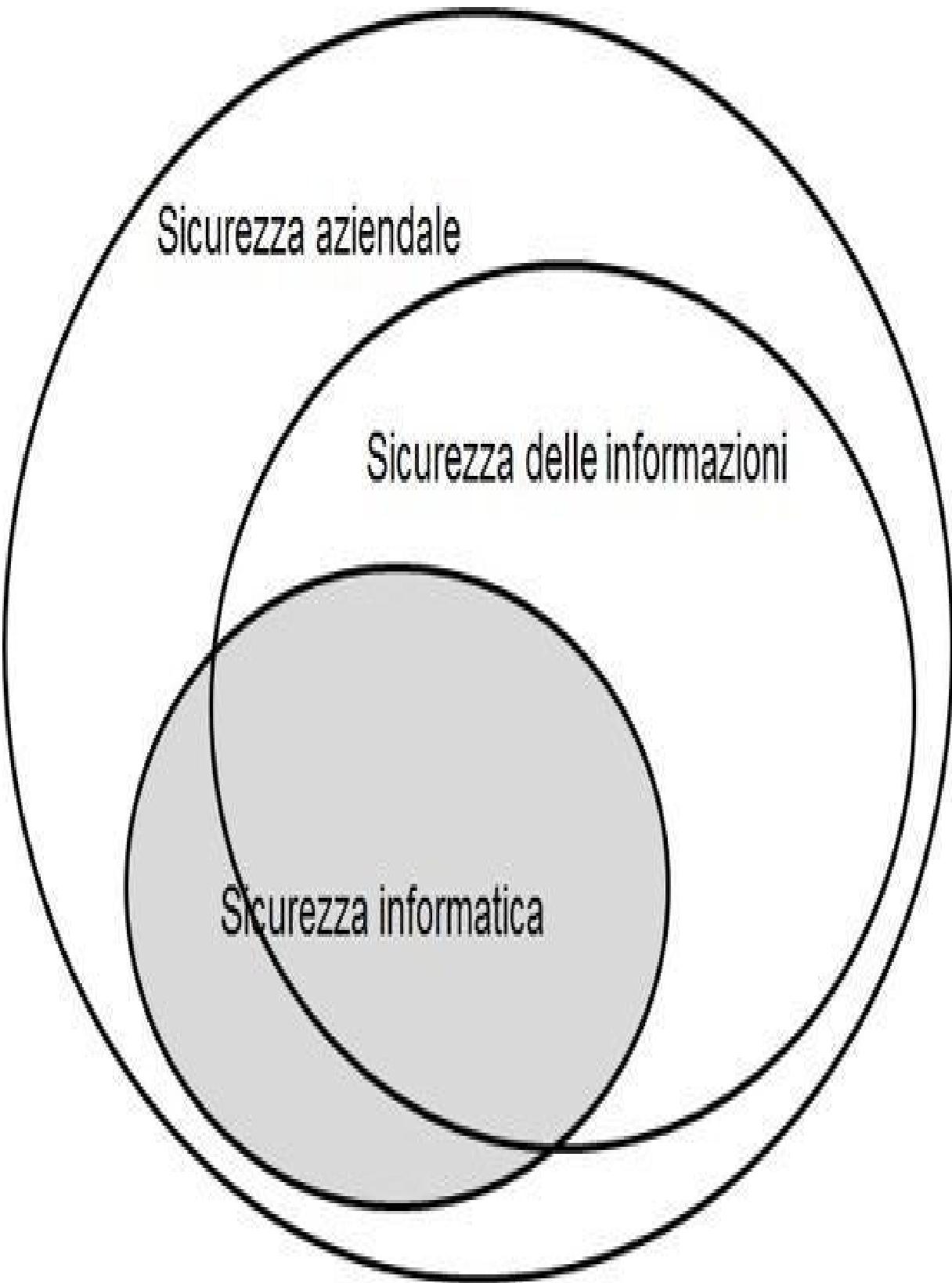


Figura 2.3.1:

Sicurezza delle informazioni e sicurezza informatica

Esempio 2.3.1. Nel 2016 alcuni appartamenti in Finlandia rimasero senza acqua calda per una settimana perché il sistema di riscaldamento fu oggetto di attacco informatico¹⁶.

Questo non è propriamente un attacco con impatto sulle informazioni, ma è sicuramente un incidente di sicurezza informatica.

Esempio 2.3.2. Nel 2021 uno sconosciuto riuscì ad accedere ai sistemi informatici di un impianto di trattamento dell'acqua in Florida (USA) e modificò alcuni dosaggi¹⁷.

Questo attacco, anche se ha avuto impatti sulle informazioni dei dosaggi, è visto da alcuni come relativo agli impianti industriali e non alla sicurezza delle informazioni.

In questo libro non si usa il termine cybersecurity in quanto si tratta della stessa sicurezza informatica, solo con un nome ritenuto più suggestivo. Esso è tratto dal

termine cyberspace, inventato da William Gibson nel 1986 nell’ambito della letteratura cyberpunk forse perché il termine “Internet” non era abbastanza diffuso. Lo stesso Gibson ha ammesso di avere usato il termine greco “cyber” (timone, da cui sono anche tratti i termini “governo” e “cibernetica”) senza saperne il significato ma solo perché interessante.

Negli anni in molti hanno cercato di giustificare l’uso dei termini cybersecurity e cyberspace in ambito scientifico, ma senza trovare una soluzione condivisa o rigorosa e, anzi, creando confusione e false aspettative. È importante capire il punto chiave della questione: sicuramente la cybersecurity riguarda sistemi informatici, ma non solo quelli che trattano informazioni vere e proprie (ossia documenti e tabelle), bensì anche parametri di configurazione, comunque essenziali per il funzionamento di molte infrastrutture come reti di distribuzione di gas ed elettricità, impianti di riscaldamento e raffreddamento, sistemi industriali e domotici, eccetera.

Una buona definizione è la seguente¹⁸:

cybersecurity: la capacità di rendere sicuri gli oggetti vulnerabili attraverso l’informatica.

Questa vuol dire che essa include la sicurezza di:

Internet of things (IoT), inclusi i dispositivi usati in ambito industriale (Industrial IoT o IIoT) e domotico;

Operational technology, che a sua volta include i sistemi industriali (industrial control systems o ICS), che a loro volta includono le reti supervisory control and data acquisition (SCADA) che controllano le reti di distribuzione di gas, elettricità, acqua, eccetera;

sistemi di domotica.

In questi ambiti si usa preferibilmente il termine resilienza, per molti versi simile a quello di disponibilità, però meno legato alle informazioni in senso stretto.

Vuole anche dire che è esclusa dalla cybersecurity la sicurezza fisica e ambientale dei sistemi informatici.

C’è anche chi usa il termine cybersecurity per indicare la sicurezza di Internet includendo fenomeni come il bullismo online (cyberbullying).

La definizione del NIST, che è l’ente che ha reso popolare il termine con il suo Cybersecurity framework o CSF [113], è troppo generica: “Il processo di protezione delle informazioni attraverso la prevenzione, rilevazione e risposta agli attacchi”. Va anche detto che le misure di sicurezza proposte dal CSF sono normali misure di sicurezza informatica.

In Italia, regnando la confusione, c’è chi ha tradotto “cybersecurity” con “sicurezza cibernetica”, non sapendo evidentemente cosa sia la cibernetica e non riflettendo sul fatto che in inglese non si usa l’espressione cybernetics security.

Con il DL 82 del 2021, convertito con la Legge 109 del 2021, è stata fornita una definizione italiana alla cybersicurezza: “l’insieme delle attività necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l’integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell’interesse nazionale nello spazio cibernetico”.

Qui è chiaro che si limita la materia alla sicurezza dei sistemi informatici, escludendo quindi le informazioni su altri supporti, ma includendo sistemi che non trattano propriamente informazioni, ma solo parametri di configurazione, comunque essenziali per il funzionamento di molte infrastrutture: reti di distribuzione di gas ed elettricità, impianti di riscaldamento e raffreddamento, sistemi industriali e domotici, eccetera.

Nella definizione italiana il termine confidenzialità è usato al posto di riservatezza perché quest'ultimo può essere confuso con quello delle classifiche di segretezza nell'ambito della sicurezza dello Stato; da notare che altri, per esempio nei Paesi anglosassoni, sono meno precisi, visto che usano sempre il termine “confidential”, sia nell’ambito delle classifiche di segretezza, sia in altri contesti¹⁹.

2.4

Organizzazione, processi e funzioni

In conformità con le norme ISO è qui adottato il termine organizzazione per indicare ogni forma di impresa, azienda, ente, associazione, agenzia, eccetera.

Altra definizione da segnalare è quella di business: molte norme distinguono tra attività di business, ossia quelle principali di un’organizzazione, e quelle di supporto. In alcuni testi con il termine business si intendono le persone non coinvolte nelle attività di gestione dei sistemi informatici.

Questa differenziazione potrebbe invitare a vedere l’informatica come estranea alle altre attività dell’organizzazione e pertanto in questo libro non si utilizza quel termine.

Nel seguito è descritto come si compone un’organizzazione, ossia in processi e funzioni.

2.4.1

I processi

La definizione di processo fornita dalla ISO/IEC 27000 è la seguente.

Processo: insieme di attività fra di loro interrelate o interagenti che trasforma elementi in ingresso (input) in elementi in uscita (output).

Apparentemente banale, nasconde diverse complessità.

Esempio 2.4.1. Si consideri il processo di gestione della formazione del personale. Gli input sono le esigenze di formazione e l'output è il miglioramento delle competenze delle persone coinvolte.

Ma non è così semplice: gli input comprendono anche i costi, il budget, le date in cui tenere il corso, la disponibilità (se il caso) dell'aula, le offerte e fatture dei fornitori, le giornate in cui il docente e il personale sono disponibili. Tra gli output vi sono: la valutazione dei costi rispetto al budget, la scelta del metodo di formazione, le richieste di offerta, gli ordini e i pagamenti ai fornitori, la convocazione al corso, i risultati degli esami.

Le attività sono numerose: raccolta delle esigenze di formazione, verifica dei costi e comparazione con il budget, scelta dei corsi da erogare e delle date, dei partecipanti prescelti e delle sedi, convocazione dei partecipanti, conferma al fornitore, pagamento al fornitore, raccolta e invio dei risultati degli esami e così via.

Ciascuna di queste attività può essere svolta con diversi strumenti (informatici o non informatici).

Una caratteristica dei processi, implicita nella definizione, è che devono essere tenuti sotto controllo, in modo che forniscano gli output previsti e si possano prevenire o rilevare scostamenti da quanto previsto.

Il controllo può essere esercitato quotidianamente dai singoli operatori e dai loro responsabili e periodicamente dal personale addetto alle verifiche o con misurazioni di efficacia ed efficienza, dove, usando la ISO 9000 [70]:

Efficacia: grado rispetto al quale le attività pianificate sono realizzate e i risultati pianificati raggiunti.

Efficienza: relazione tra risultati ottenuti e risorse utilizzate.

Esempio 2.4.2. Per misurare il processo di gestione della formazione è possibile elaborare dati sui risultati dei test sostenuti, sui costi e sulla soddisfazione dei responsabili delle persone da formare e dei partecipanti alla formazione.

Ecco quindi di seguito le caratteristiche di ogni processo:

ogni processo ha elementi in ingresso (input), provenienti da funzioni interne o entità esterne, come clienti, fornitori e partner;

per ogni attività del processo sono utilizzati strumenti (i moduli e i mezzi di comunicazione per le attività burocratiche; le macchine e gli impianti per le attività manifatturiere; i programmi software per i sistemi informatici);

per ogni attività sono indicati i responsabili e gli esecutori;

sono stabilite le modalità per tenere sotto controllo il processo;

ogni processo ha elementi in uscita (output) e destinatari, ossia funzioni interne o esterne.

È necessario conoscere due termini: si mappano i processi così come sono e si modellano così come si desidera modificarli.

Nel mapparli o modellarli bisogna evitare di descrivere ogni possibile dettaglio: la vita reale è sempre più complicata di ogni sua possibile descrizione. L'importante è disporre di descrizioni sufficienti per tenere sotto controllo il processo, illustrarlo alle parti interessate (compresi coloro che devono attuarlo) e migliorarlo.

2.4.2

Le funzioni

Un'organizzazione è strutturata in funzioni, ossia gruppi di persone corrispondenti alle caselle degli uffici riportati in organigramma.

I processi descrivono come le funzioni interagiscono tra loro o al loro interno, come schematizzato in figura 2.4.1.

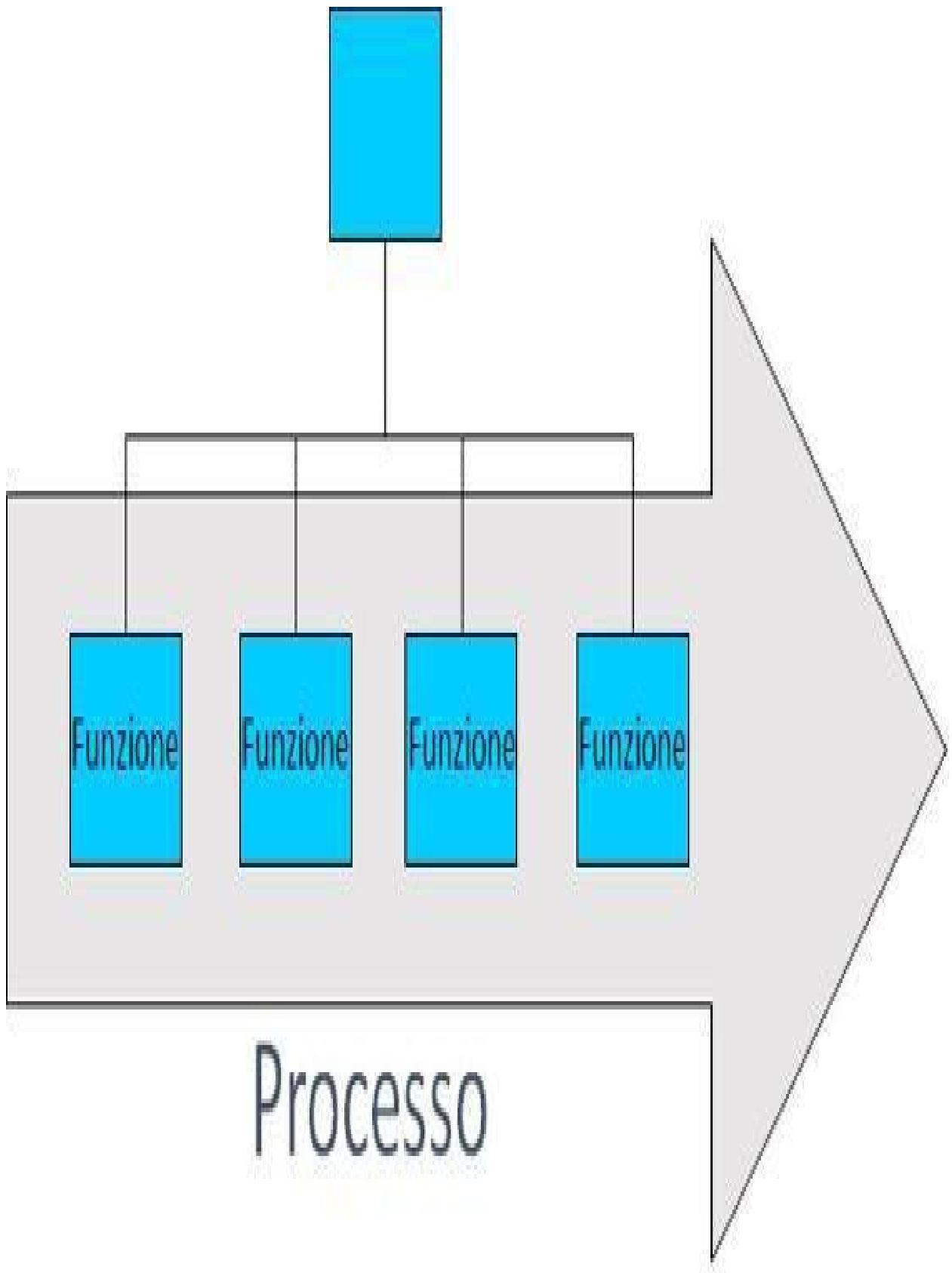


Figura 2.4.1:

Processo e funzioni

Le comunicazioni, all'interno delle stesse funzioni o tra funzioni distinte, devono avvenire con modalità concordate.

Esempio 2.4.3. Per il processo di formazione, potrebbero essere coinvolti, oltre al responsabile delle persone da formare, l'ufficio personale, l'amministrazione e l'ufficio acquisti.

Queste funzioni possono comunicare tra loro via e-mail, applicazioni informatiche, moduli cartacei o oralmente.

2.5

Processi, prodotti e persone

È stata sottolineata l'importanza dei processi per la realizzazione di un sistema di gestione per la sicurezza delle informazioni, ma questi non sono certamente sufficienti. Sono fondamentali anche le persone e i prodotti.

È infatti necessario avvalersi di persone qualificate, in grado di comprendere e conseguire la sicurezza delle informazioni, attraverso l'applicazione di giusti processi e l'impiego di prodotti idonei. Si parla quindi delle 3 P: processi (o procedure), persone e prodotti. In appendice B è introdotta una quarta P, per i fornitori (partner).

Esempio 2.5.1. Un'auto da corsa data in mano a un neo-patentato presumibilmente non vincerebbe alcun premio e il pilota metterebbe a repentaglio la sua vita, anche per la scarsa conoscenza delle procedure, inesperienza alla guida e probabile sopravvalutazione delle sue capacità.

Un'auto meno impegnativa, data in mano a un bravo pilota, otterrebbe quasi certamente risultati superiori, grazie alla maggiore preparazione e alle migliori conoscenze sia teoriche che pratiche. Solo però una corretta combinazione di auto, pilota (con il suo team di meccanici) e procedure porta a raggiungere i migliori risultati e vincere la gara.

Quale delle tre P è la più importante? Nessuna: tutte devono partecipare in modo bilanciato al conseguimento dell'impresa.

Trattando di sicurezza delle informazioni, l'antivirus è sicuramente un prodotto importante, ma lo sono anche la procedura per tenerlo aggiornato e la persona addetta alla sua installazione e configurazione.

Quando si parla di persone, è sempre opportuno intendere una pluralità di soggetti con compiti differenti. Esattamente come nella Formula Uno, dove ci sono meccanici, ingegneri e persone specializzate, addestrate e controllate anche per cambiare il bullone della ruota ai pit stop. Il mondo della sicurezza delle informazioni è ormai un campo così complicato che non si può parlare di uno, ma di molti specialisti che si occupano di alcuni processi e impiegano più prodotti.

Per esempio sono necessari: lo specialista della gestione sicura delle informazioni, strettamente collegato con il responsabile dei sistemi informativi, dal quale dipendono gli specialisti dei vari apparati di rete, dei server, dei dispositivi personali e dei software applicativi.

Note

²http://it.wikipedia.org/wiki/Biblioteca_di_Alessandria.

³www.contribuenti.it/cartellepazze/cartellepazze1.asp.

⁴www.repubblica.it/2003/i/sezioni/cronaca/blackitalia/blackitalia/blackitalia.html.

⁵news.bbc.co.uk/sport2/hi/motorsport/formula_one/6994416.stm.

⁶www.theguardian.com/uk/2009/apr/09/bob-quick-terror-raids-leak.

⁷www.pierotaglia.net/facebook-fai-da-te-alpitour-ahi-ahi-ahi-pagine-facebook-hackerate.

⁸www.theregister.co.uk/2013/03/27/spamhaus_ddos_megaflight.

⁹<https://www.key4biz.it/idiot-wind-bob-dylan-puo-aiutare-nella-valutazione-del-rischio-aziendale/307656/>.

¹⁰[https://www.bbc.com/news/technology-52722626](http://www.bbc.com/news/technology-52722626).

¹¹<https://www.wired.it/internet/web/2021/03/10/incendio-data-center-ovh-strasburgo/>.

¹²<https://www.cybersecurity360.it/nuove-minacce/regione-lazio-vaccini-bloccati-poco-pronta-contro-il-ranwomare-ecco-perche/>.

¹³https://www.corriere.it/esteri/21_ottobre_05/facebook-instagram-whatsapp-down-costa-zuckerberg-6-miliardi-dollari-d6f5c632-2586-11ec-9c26-509de9bc1f2d.shtml.

¹⁴http://www.repubblica.it/tecnologia/2014/05/13/news/causa_contro_google_cor

tore_di_ricerca_responsabile_dati-85985943/.

¹⁵attrition.org/security/rant/sony_aka_sownage.html.

¹⁶http://www.theregister.co.uk/2016/11/09/finns_chilling_as_ddos_knocks_out_broadband_system/

¹⁷<https://www.zdnet.com/article/following-oldsmar-attack-fbi-warns-about-using-teamviewer-and-windows-7/>

¹⁸<https://www.cisoparameter.com/profiles/blogs/understanding-difference-between-cyber-security-information>.

¹⁹Si preferisce non ribadire i commenti sull'uso del termine “cibernetico”.

Capitolo 3

Sistema di gestione per la sicurezza delle informazioni

Comme de longs échos qui de loin se confondent

Dans une ténébreuse et profonde unité,

Vaste comme la nuit et comme la clarté,

Les parfums, les couleurs et les sons se répondent

Charles Baudelaire, Correspondances

La sicurezza delle informazioni si può raggiungere attraverso idonei processi organizzativi. Sono infatti necessari processi per stabilire qual è il livello di sicurezza adeguato, individuare le carenze, decidere come colmarle e con quali prodotti, programmare i tempi e i responsabili delle attività di adeguamento, formare il personale e mantenere le soluzioni adottate.

Esempio 3.0.1. Si consideri il sistema di tornelli per accedere agli uffici. Bisogna stabilire se offre il livello di sicurezza desiderato, quali tecnologie adottare anche considerando le normative vigenti, quale fornitore incaricare dell'installazione, quali contratti stipulare per la manutenzione, come abilitare e disabilitare gli utenti per l'accesso, come agire in caso di guasto.

Non è ovviamente vero l'inverso: buoni prodotti di sicurezza non garantiscono il raggiungimento dei risultati desiderati. Sono numerosi i casi di acquisto di strumenti rimasti inutilizzati perché non integrabili con i sistemi già in uso o perché nessuno ha ricevuto l'adeguata formazione per installarli e mantenerli.

I processi non sono tra loro isolati e indipendenti, ma correlati e interagenti.

Esempio 3.0.2. Tornando all'esempio dei tornelli, si vede facilmente come più processi interagiscano tra loro: analisi dei rischi per valutare le necessità, gestione degli acquisti e formazione.

A tornelli attivi, sono coinvolti ulteriori processi: controllo degli accessi, gestione del personale (per stabilire chi è autorizzato ad accedere), gestione dei fornitori (per gli addetti alla manutenzione), gestione degli incidenti (da attivare in caso di guasto o allarme); verifica periodica dell'adeguatezza dei tornelli.

In questo capitolo si definiscono quindi i sistemi di gestione e i sistemi di gestione per la sicurezza delle informazioni. Si fanno anche delle considerazioni sulla loro pianificazione e attuazione.

3.1

Sistema di gestione

Come già detto in precedenza, i processi sono tra loro interrelati e interagenti. Può quindi risultare chiara la seguente definizione, fornita dalla ISO/IEC 27000.

Sistema di gestione (management system): Insieme di elementi interrelati o interagenti di un'organizzazione per stabilire politiche e obiettivi e processi [a loro volta interrelati o interagenti] per raggiungere tali obiettivi.

La definizione prevede di stabilire politiche, obiettivi e processi e poi fare in modo che gli obiettivi siano raggiunti. Non è quindi previsto che siano date politiche, obiettivi e processi e poi ci si disinteressi del loro funzionamento e della loro realizzabilità.

In sintesi, sacrificando la teoria e tornando alla pratica, possiamo dire che:

ogni organizzazione ha uno scopo (missione);

il sistema di gestione di un'organizzazione è il suo insieme di pratiche organizzative (processi) e di strumenti atti a raggiungere il suo scopo;

tali processi e strumenti sono tra loro interrelati;

ciascun cambiamento organizzativo, anche se potenzialmente piccolo, può avere impatti su molte aree dell'organizzazione e sui clienti, fornitori e partner, derivanti delle interrelazioni dei processi;

quando si operano cambiamenti va prestata attenzione ai loro impatti sin da quando sono pianificati.

3.2

Sistema di gestione per la sicurezza delle informazioni

In un'organizzazione non tutte le attività sono dedicate o coinvolte nella sicurezza delle informazioni. Difatti si deriva la seguente definizione dalla ISO 9000.

Sistema di gestione per la sicurezza delle informazioni (SGSI): parte di un sistema di gestione che riguarda la sicurezza delle informazioni.

Per indicare il sistema di gestione per la sicurezza delle informazioni si usa spesso il suo acronimo (SGSI) o la dicitura inglese information security management system (ISMS).

Altre parti del sistema di gestione di un'organizzazione possono riguardare: la qualità, l'ambiente, la sicurezza e la salute dei lavoratori.

È importante distinguere gli ambiti di ciascun sistema di gestione, le loro interrelazioni e le loro sovrapposizioni, per evitare di trattare materie estranee a una disciplina o moltiplicare inutilmente gli sforzi.

Esempio 3.2.1. La sicurezza delle informazioni non si occupa, se non marginalmente, di rischio di credito, di protezione del brand aziendale e della sicurezza fisica e igiene dei lavoratori: sono altre discipline, che richiedono competenze diverse e sono trattate da altri sistemi di gestione.

La prevenzione degli incendi è materia comune alla sicurezza delle informazioni, alla sicurezza fisica, alla protezione dell’ambiente e alla sicurezza e salute del personale. Deve quindi essere affrontata in modo da evitare inutili sovrapposizioni e garantire l’adeguamento delle misure intraprese alle esigenze di tutti.

Per un SGSI è importantissimo il ruolo della Direzione, che ne è la proprietaria. La Direzione deve dimostrare impegno nell’attuazione del SGSI, usarlo come strumento per controllarne gli elementi interrelati e interagenti e assicurare che sia efficace (ossia che soddisfi gli obiettivi di sicurezza delle informazioni).

3.3

Le certificazioni relative alla sicurezza delle informazioni

Come essere sicuri che siano stati adottati i processi adeguati, che il personale sia preparato e che i prodotti e servizi utilizzati siano affidabili? Occorre effettuare delle valutazioni condotte da un ente terzo e indipendente, a sua volta controllato da appositi organismi.

Le valutazioni prevedono la raccolta e l'analisi degli elementi di prova secondo criteri stabiliti, in modo da valutarli obiettivamente e nel rispetto delle norme. Il risultato finale può dare luogo a una certificazione.

Nell'ambito della sicurezza delle informazioni esistono schemi per la certificazione dei processi (il più importante è quello basato sulla ISO/IEC 27001 [84] di cui si tratta più diffusamente in appendice C), dei prodotti (il più importante è quello basato sulla ISO/IEC 15408 [78, 79, 80], detti anche Common criteria e di cui si tratta più diffusamente in appendice D), dei servizi e delle persone [54, 149].

La certificazione serve a dare una ragionevole fiducia che:

le decisioni siano prese da persone competenti;

le persone impieghino prodotti a loro volta verificati e ritenuti affidabili;

le procedure impiegate siano state a loro volta verificate con esito positivo.

Solo attraverso la misura della fiducia che si può riporre in un prodotto, in un

servizio, in una persona o in una procedura, si ha la ragionevole certezza che le cose vadano nella giusta direzione.

Il sistema di certificazione ha anch'esso dei difetti, il primo dei quali è che gli organismi di certificazione sono pagati dalle stesse entità che richiedono la certificazione. Ciò non toglie che questi meccanismi contribuiscano a una maggiore sicurezza.

Parte II

La gestione del rischio

Capitolo 4

Rischio e valutazione del rischio

I'd call that a bargain

the best I ever had.

Pete Townshend (The Who),

Bargain

Nei paragrafi e capitoli seguenti è spiegato cos'è il rischio e come valutarlo, in modo da decidere come trattarlo. Le fasi della valutazione del rischio (risk assessment) sono riportate in figura 4.0.1 e sono:

identificazione del rischio;

analisi del rischio;

ponderazione del rischio.

Queste fasi devono essere precedute da una comprensione del contesto e dell'ambito in cui si valuta il rischio e seguite dal trattamento del rischio e dal suo monitoraggio. L'insieme di queste fasi costituisce la gestione del rischio. A ciascuna di queste fasi sono dedicati i capitoli da 5 a 9.

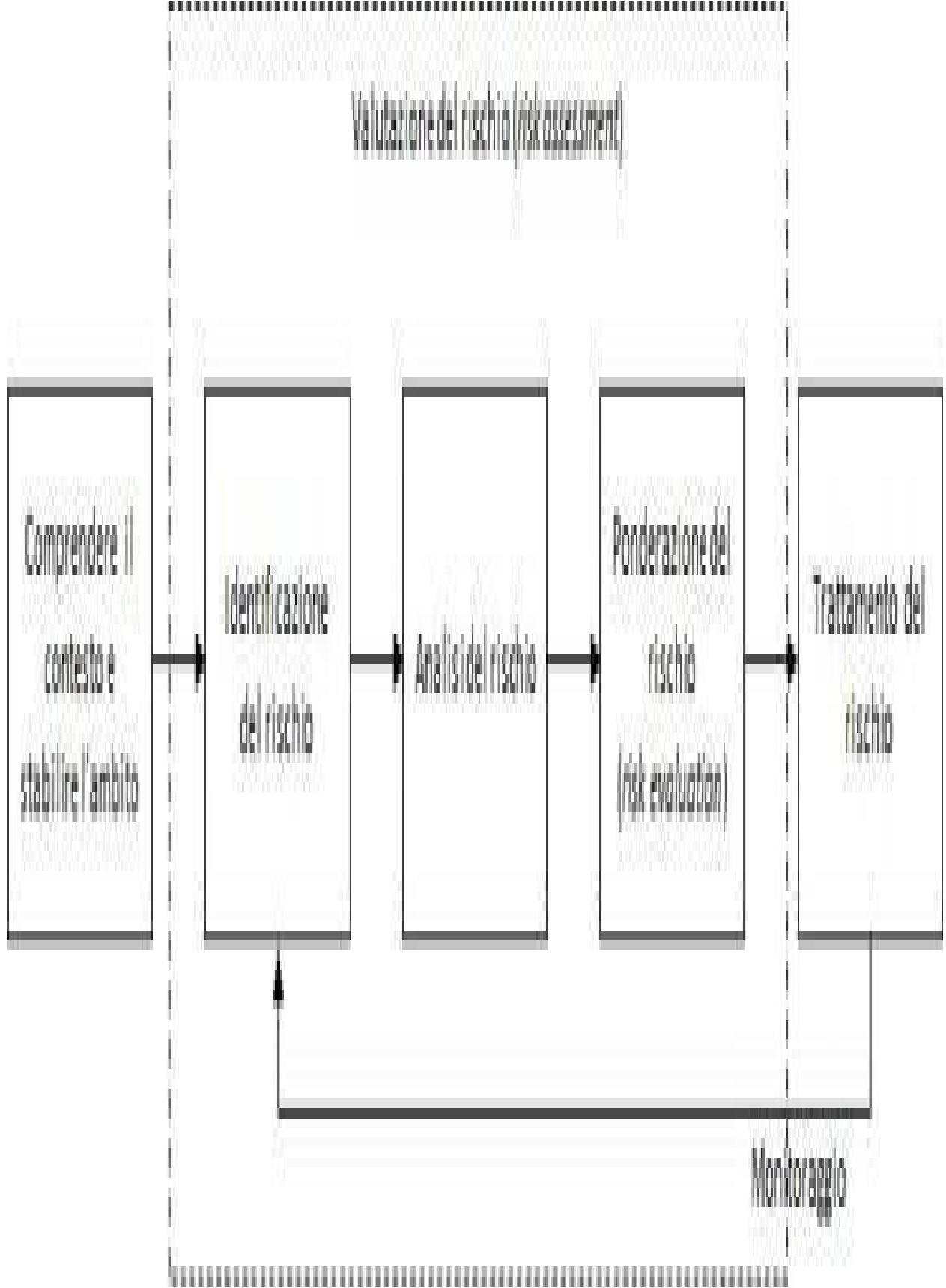


Figura 4.0.1:

Le fasi della gestione del rischio

L'ultimo capitolo di questa parte si occupa del monitoraggio e della rivalutazione del rischio, attività necessarie perché il rischio venga gestito nel tempo.

4.1

Cos'è il rischio

Per parlare di valutazione e trattamento del rischio, bisogna innanzitutto definire il rischio, utilizzando la ISO/IEC 27000.

Rischio: effetto dell'incertezza sugli obiettivi.

Note: I rischi sono spesso riferiti come eventi potenziali e conseguenze o una loro combinazione.

L'incertezza è dovuta ad eventi, che possono avere effetti (o conseguenze o impatti) negativi o positivi.

Gli impatti sono quelli immediati, corrispondenti ai costi diretti che vedremo più avanti (paragrafo 7.2.1), mentre le conseguenze includono quelle a breve, medio e lungo termine. Nella valutazione del rischio si preferisce valutare le conseguenze.

Sin da ora è necessario chiarire che non si può identificare il rischio reale, ma solo quello percepito e le valutazioni sono sempre soggettive. Le tecniche di identificazione, analisi e ponderazione del rischio non devono quindi avere la pretesa di rappresentare una realtà oggettiva, ma di guidare verso risultati il più possibile completi, pertinenti e riferibili.

4.1.1

I rischi positivi e negativi

I rischi possono generare effetti negativi, come per esempio:

danno di immagine a causa di eventi negativi e di dominio pubblico;

perdita di quote di mercato a causa delle azioni dei concorrenti, incluse quelle di riduzione dei prezzi, innovazione e spionaggio;

perdita di competitività a causa dell'aumento del costo delle materie prime;

rallentamenti della produzione a causa della chiusura di un fornitore;

riduzione della liquidità per difficoltà di recupero crediti verso i clienti;

costi di adeguamento a nuovi dispositivi normativi;

perdite economiche a causa di scioperi, atti di sabotaggio o di terrorismo derivanti dal clima sociale e politico;

perdita di reputazione, di clienti o di liquidità economica a causa della difettosità dei prodotti e dei servizi.

I rischi possono avere conseguenze positive. Gli eventi che li generano sono indicati con il termine di opportunità. Conseguenze positive e relative opportunità possono essere:

miglioramento dell'immagine per il tempestivo adeguamento a nuovi dispositivi normativi;

aumento della clientela grazie all'elevata innovazione;

miglioramento della reputazione e della produttività grazie alla buona gestione del personale.

Alcuni rischi potrebbero essere sia positivi sia negativi. Per esempio:

un nuovo cliente può avere conseguenze positive, soprattutto sul fatturato, oppure conseguenze negative se risulta essere un cattivo pagatore (la Pubblica amministrazione italiana è nota per i suoi ritardi nei pagamenti e molte imprese sono fallite per questo²⁰);

un'innovazione o l'apertura di una nuova sede o l'aggiunta di una nuova linea di produzione possono avere conseguenze positive se apprezzate dai clienti, oppure conseguenze negative se non generano guadagni tali da coprire i costi sostenuti per realizzarle;

ogni cambiamento e riorganizzazione possono migliorare l'efficacia e l'efficienza dei processi, ma possono anche peggiorarle o scontentare il personale.

La sicurezza delle informazioni si occupa solo dei rischi con effetti negativi, oggetto di questo e dei prossimi capitoli. Delle opportunità relative al sistema di gestione si discuterà nel paragrafo 15.6.

4.1.2

Il livello di rischio

Per comprendere come agire di fronte a un rischio, è opportuno stabilirne il livello, ossia una misura di grandezza. Sempre dalla ISO/IEC 27000 si ha la definizione seguente.

Livello di rischio: grandezza di un rischio espresso come combinazione delle sue conseguenze e della loro verosimiglianza.

Anche intuitivamente:

più sono elevate le conseguenze di un possibile evento, più alto è percepito il rischio;

più è verosimile o probabile che si verifichi un evento negativo, più alto è percepito il rischio.

La ISO/IEC 27001 utilizza il termine verosimiglianza e non probabilità per evitare che venga interpretato come richiesta di calcolare il rischio in termini quantitativi (paragrafo 7.1). In questo libro, per contro, lo si utilizzerà spesso perché ritenuto più intuitivo.

Si consideri, come esempio, nel contesto dei viaggi aerei, l'imbarco del bagaglio su un aereo: il rischio relativo al furto è più elevato quanto più gli oggetti nel bagaglio hanno valore e quanto più la compagnia aerea o gli aeroporti dove si transita sono noti per l'elevato numero di furti avvenuti.

Si può rappresentare questa relazione con una formula matematica, dove il rischio r è direttamente proporzionale alla probabilità p di accadimento di un evento e alle sue conseguenze i (si osservi che tradizionalmente si usa la i di impatti):

$$r \propto p \cdot i \quad (4.1.1)$$

Quando si imbarca un bagaglio, i rischi non si riducono a quelli collegati al furto, ma anche ad altri, come quelli collegati alla perdita o al ritardo nel riceverlo; in questo caso le probabilità di accadimento e le conseguenze saranno diverse. Quindi, il rischio dipende dall'evento o minaccia m e la formula 4.1.1 andrebbe più correttamente riscritta così:

$$r(m) \propto p(m) \cdot i(m) \quad (4.1.2)$$

Più valore ha il bagaglio, più il rischio è elevato e quindi il rischio aumenta se aumenta il valore degli oggetti su cui agisce la minaccia. Questi oggetti, la cui definizione ufficiale è al paragrafo 6.1, sono detti asset e indicati con la lettera a. Il rischio che il bagaglio sia rubato (minaccia) è direttamente proporzionale alla probabilità del furto $p(m)$ e alla conseguenza $i(m,a)$ del furto m sull'asset a. La formula 4.1.2 va quindi riscritta così:

$$r(m, a) \propto p(m) \cdot i(m, a) \quad (4.1.3)$$

Se il bagaglio non ha serratura, è più vulnerabile e il rischio aumenta. Il rischio dipende quindi anche dalle vulnerabilità v e dalla loro gravità $g(v)$. Più le vulnerabilità sono elevate, più il rischio è alto. La formula 4.1.3 può essere quindi scritta anche così:

$$r(m, a, v) \propto p(m) \cdot i(m, a) \cdot g(v) \quad (4.1.4)$$

Se si applicano misure o controlli di sicurezza c al bagaglio (per esempio, l'aggiunta di un lucchetto o la stipula di una polizza assicurativa), il rischio relativo al furto diminuisce. Si può vedere la robustezza dei controlli di sicurezza $r(c)$ come l'inverso delle vulnerabilità (se il bagaglio è munito di serratura, è meno vulnerabile) e ottenere la seguente formula:

$$r(m, a, c) \propto p(m) \cdot i(m, a) / r(c). \quad (4.1.5)$$

I controlli possono modificare la probabilità di riuscita di una minaccia (se si usa un lucchetto) o le conseguenze (per esempio, se si stipula una polizza di assicurazione). Probabilità e conseguenze sono quindi dipendenti da c e la formula 4.1.3 può essere riscritta così:

$$r(m, a, c) \propto p(m, c) \cdot i(m, a, c). \quad (4.1.6)$$

Un controllo carente rappresenta una vulnerabilità. Per questo si possono sostituire i controlli c con le vulnerabilità v , si ottiene questa formula:

$$r(m, a, v) \propto p(m, v) \cdot i(m, a, v). \quad (4.1.7)$$

Da quanto detto, è possibile elencare i parametri di valutazione del rischio:

il contesto;

l'asset e il suo valore, da cui dipendono le conseguenze;

la minaccia e la sua verosimiglianza o probabilità;

le vulnerabilità e la loro gravità o i controlli di sicurezza e la loro robustezza.

Il bagaglio può essere rubato o perso, danneggiato o arrivare in ritardo; inoltre, se il bagaglio è composto da più valige, queste minacce possono avere conseguenze diverse a seconda della valigia coinvolta. Quindi “il” rischio relativo al bagaglio è composto da più rischi “singoli” dovuti alle diverse minacce e alle loro conseguenze sull’insieme degli asset. È per questo che alcuni usano l’espressione mappa del rischio.

Una volta calcolato il livello di rischio, è necessario prendere decisioni per affrontarlo o trattarlo. Utilizzando ancora l’esempio del furto dei bagagli, le possibili decisioni sono:

prevenire il furto e non imbarcare il bagaglio;

ridurre le potenziali conseguenze del furto e imbarcare solo parte del bagaglio;

evitare il rischio di furto del bagaglio all’aeroporto e prendere il treno;

eliminare il rischio e viaggiare senza bagaglio (ipotesi molto difficile da realizzare);

condividere il rischio con una compagnia di assicurazioni e stipulare una

polizza;

accettare il rischio e imbarcare il bagaglio.

L'accettazione o non accettazione del rischio dipendono dal livello di accettabilità stabilito da ciascuno: c'è chi imbarca sempre tutto il bagaglio e c'è chi cerca di portare quanto più bagaglio a mano possibile.

Ciascuna scelta non elimina il rischio, ma ne può introdurre di nuovi: il bagaglio a mano può essere anch'esso rubato, in treno si verificano ugualmente furti di bagagli e la compagnia di assicurazione potrebbe fallire e non pagare quanto dovuto.

Più avanti tutti questi concetti sono descritti compiutamente e in relazione con la sicurezza delle informazioni.

4.2

Cos'è la valutazione del rischio

Prima di tutto, è necessario fornire la definizione ufficiale della ISO/IEC 27000.

Valutazione del rischio (risk assessment): processo complessivo di identificazione, analisi e ponderazione del rischio.

In parole più semplici, la valutazione del rischio è un insieme di attività volte a identificare i rischi (ossia gli asset, le minacce e le vulnerabilità), calcolarne il livello e decidere se sono accettabili.

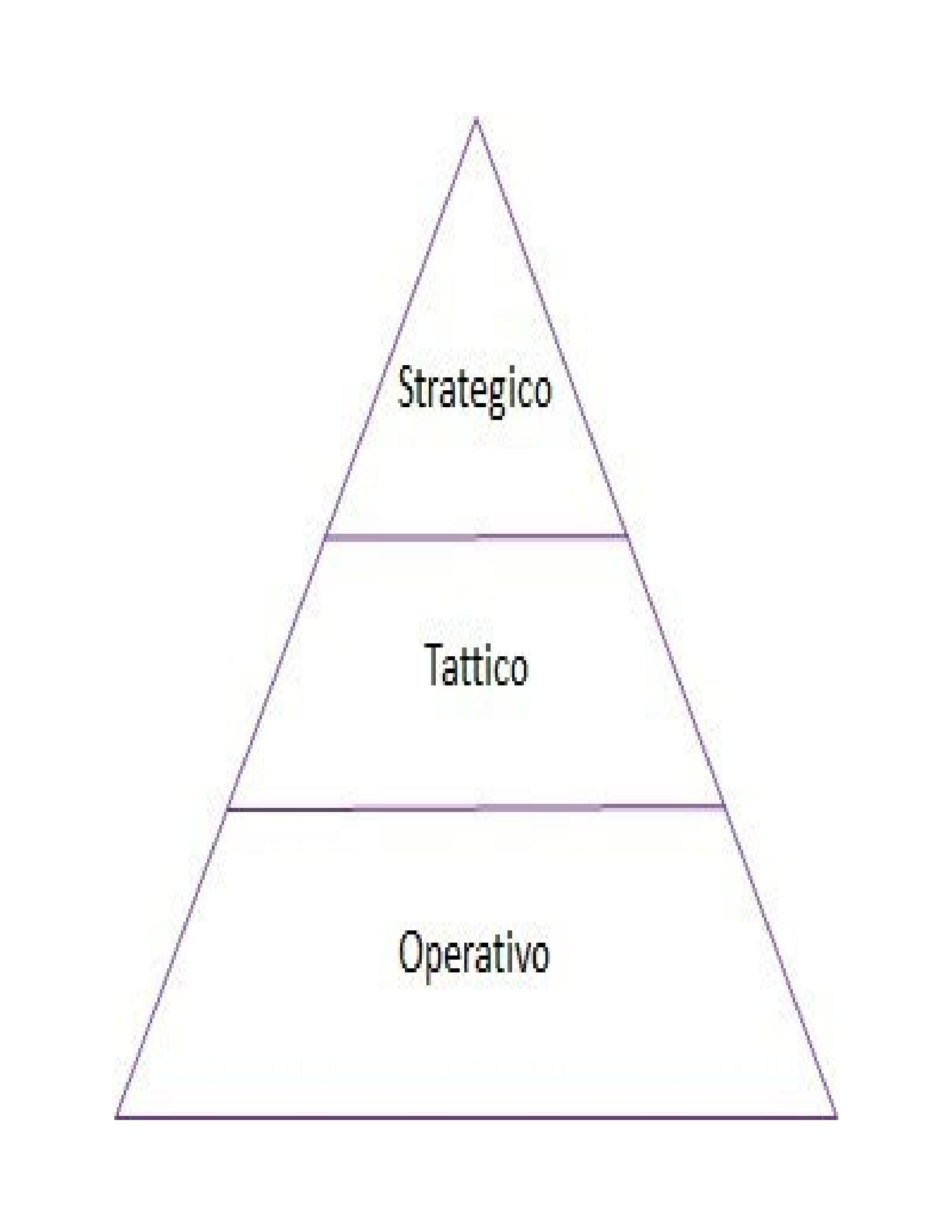
La definizione non riguarda solo la valutazione del rischio per la sicurezza delle informazioni, ma è generale e potrebbe essere applicata anche all'analisi dei rischi strategici, finanziari, sulla sicurezza dei lavoratori, di progetto [128], sulla privacy²¹, eccetera.

Nel nostro caso è corretto utilizzare la dicitura valutazione del rischio relativo alla sicurezza delle informazioni, anche se spesso, per brevità e quando non ci possono essere confusioni, in questo libro si usa solo la dicitura valutazione del rischio.

Bisogna avere chiara la finalità della valutazione del rischio in modo da individuare i metodi adeguati.

Per questo si riporta in figura 4.2.1 la rappresentazione di un'organizzazione

attraverso la piramide di Anthony [145] (si osservi che in altri contesti, per esempio militari, i termini hanno significato diverso).



Strategico

Tattico

Operativo

Figura 4.2.1:

La piramide di Anthony



A livello strategico sono richiesti dati stimati e approssimati, utili per dare indirizzi con prospettive a lungo termine (qualche anno);

a livello tattico sono richiesti dati consuntivi, arrotondati e abbastanza tempestivi, utili per avere indicazioni sull'andamento delle attività operative e prendere decisioni con prospettive a medio termine (qualche mese);

a livello operativo i dati devono essere esatti e in tempo reale, poiché servono a effettuare e tenere sotto controllo le attività in corso.

Per realizzare un sistema di gestione per la sicurezza delle informazioni è necessario individuarne gli elementi, in particolare i processi e le loro interrelazioni, e prendere decisioni in merito alle misure di sicurezza da adottare. Questo riguarda i livelli strategici e tattici, che hanno bisogno di dati aggregati e non particolarmente accurati. Parafrasando il principio del rasoio di Occam, per prendere una decisione è inutile avere più dati di quelli strettamente necessari.

Di conseguenza il livello di dettaglio e di approfondimento necessario alla valutazione del rischio deve essere basso, anche quando il valore delle informazioni che si vogliono proteggere è alto: analisi del rischio molto dettagliate forniscono troppi dettagli inutili per prendere delle decisioni a livello strategico e tattico.

Avere la pretesa di descrivere completamente la realtà e identificare nel dettaglio

ogni asset, minaccia e vulnerabilità sarebbe un inutile spreco di lavoro: l'identificazione del rischio, per quanto accurata, permetterà solo di avere un modello della realtà, e mai potrà rappresentarla correttamente e in ogni suo dettaglio. Per illustrare questo concetto, Korzybski (anche se in altro contesto) diceva che la mappa non è il territorio e Magritte che il disegno di una pipa non è una pipa.

Esempio 4.2.1. In un'organizzazione, dopo 6 mesi di raccolta di dati molto accurati per la valutazione del rischio, il responsabile della sicurezza si accorse che l'organizzazione aveva subito tanti cambiamenti da richiedere una nuova esecuzione del lavoro.

I cambiamenti, peraltro, erano stati condotti senza considerare i rischi relativi alla sicurezza delle informazioni, dimostrando ulteriormente quanto poco utile era stato considerato il lavoro svolto.

Chi vuol fare un “lavoro accurato” confonde la finalità (avere elementi per decidere) con il suo mezzo (avere un’accurata analisi del rischio).

È quindi opportuno iniziare da un’analisi non troppo accurata di livello tattico. Questa potrebbe evidenziare la necessità di analizzare a livello operativo e con maggior dettaglio alcuni sistemi informatici (server, apparati di rete, applicazioni, PC, dispositivi portatili come cellulari, smartphone e tablet), aree o servizi, per i quali adottare metodi di analisi più accurati. Tra questi metodi vi sono i vulnerability assessment (paragrafo 12.15.4) e le gap analysis rispetto a best practice. Si osservi che questi metodi non sono valutazioni del rischio poiché evidenziano solo vulnerabilità.

Esempio 4.2.2. In una grande organizzazione si decise di raccogliere i dati necessari a identificare il rischio di ciascuna funzione organizzativa. Ciò permise di raccogliere molte informazioni utili, ma si rivelarono eccessivamente numerose. Inoltre, la diversa sensibilità dei rappresentanti delle funzioni organizzative comportò una forte disomogeneità tra i risultati.

L'analisi non permise neanche di rilevare le carenze a livello tattico, come la mancanza di regole comuni per la gestione delle chiavi fisiche e per l'archiviazione delle informazioni, per la configurazione dei backup e l'esecuzione dei test di continuità operativa.

Con un altro approccio, adottato in un secondo tempo e più utile, si individuarono inizialmente i rischi dovuti a carenze nelle regole generali in modo da rendere le procedure adottate da ciascuna entità omogenee alle altre e in linea con il livello di sicurezza desiderato per l'azienda nel suo complesso; successivamente si analizzarono i rischi delle entità più critiche e relativi alle minacce e vulnerabilità non adeguatamente affrontate nella prima fase; infine si analizzarono le restanti aree privilegiando il metodo di gap analysis, ossia analizzando se in esse erano attuate le misure stabilite per l'insieme dell'organizzazione e intervenendo quando necessario.

Alcuni studi [98] dicono che analisi meno accurate portano a risultati altrettanto significativi di quelle più accurate ma meno ottimistiche e dunque più prudenti, il che non è certamente un male quando si parla di sicurezza.

4.3

I metodi per valutare il rischio

In questo libro viene proposto un approccio “classico” alla valutazione del rischio, basato su asset, minacce e vulnerabilità (o contromisure), come è evidente dalle formule del paragrafo 4.1.2.

Altri propongono metodi apparentemente non allineati a questo approccio. Se però si analizzano attentamente, questi metodi sono sempre riconducibili a quello classico, anche se usano termini diversi (per esempio, scenari al posto di asset o aggregazioni di asset, oppure eventi o scenari di rischio o casi di errore al posto di minacce) e punti di partenza diversi: il metodo classico parte dagli asset per individuare le minacce e le vulnerabilità, mentre il metodo “basato sugli eventi” parte dalle minacce per poi individuare gli asset che potrebbero danneggiare.

Esempio 4.3.1. Molte organizzazioni adottano un approccio basato sull’importanza delle informazioni da cui derivano le scelte per tutelarle, indipendentemente dagli asset in cui sono contenute.

Se si analizza da vicino questo metodo, si osserva che sono analizzate le informazioni (ossia gli asset) e le minacce per calcolare il livello di rischio intrinseco (paragrafo 7.4) e sono successivamente individuate delle misure di sicurezza da applicare per evitare che vi siano vulnerabilità inaccettabili. In altre parole, ancora una volta si valutano asset, minacce e contromisure.

Il metodo classico nella sua forma più pura, che porta ad analizzare il rischio per

ciascun asset, è peculiare della sicurezza delle informazioni ed è in uso, almeno, dalla fine degli anni Ottanta, quando la sicurezza delle informazioni era decisamente diversa da quella attuale. Per questo motivo qui non se ne raccomanda l'adozione.

In questo libro viene presentato un metodo simile a quello classico, che però prevede una valutazione quasi indipendente di asset e minacce.

Un metodo valido di valutazione del rischio deve avere le seguenti caratteristiche:

completezza: devono essere considerati, al giusto livello di sintesi, tutti gli asset, tutte le minacce e tutte le vulnerabilità;

ripetibilità: valutazioni condotte nello stesso contesto e nelle stesse condizioni devono dare gli stessi risultati;

comparabilità: valutazioni condotte in tempi diversi nello stesso contesto devono permettere di comprendere se il rischio è cambiato e come;

coerenza: a fronte di valori di asset, minacce e vulnerabilità più elevati di altri, il livello di rischio deve essere più elevato.

4.3.1

I programmi software per la valutazione del rischio

Si trovano in commercio molti programmi software per effettuare valutazioni del rischio. Essi presentano un percorso guidato per censire gli asset, le minacce e le vulnerabilità, assegnare loro dei valori ed elaborare dei prospetti sul livello di rischio.

Questi programmi possono essere utili in organizzazioni molto grandi perché permettono di organizzare le attività delle persone interessate e di inserire tutti i dati raccolti. Sono utili anche quando le persone coinvolte nella valutazione del rischio (compresi i consulenti) non sono particolarmente esperte e hanno bisogno di uno strumento che li guida passo dopo passo.

Purtroppo questi programmi hanno difetti che è opportuno conoscere.

Il primo difetto consiste nella quantità di dati da inserire: spesso sono moltissimi e richiedono molto tempo. Questo non garantisce affatto risultati precisi, utili o validi.

Esempio 4.3.2. In un'organizzazione erano in corso due progetti: uno di introduzione di tornelli all'ingresso e uno di riesame e aggiornamento delle utenze di un'applicazione. Nonostante ciò, i risultati della valutazione del rischio evidenziavano solo la scarsa consapevolezza del personale e non problemi relativi all'accesso alla sede o alle utenze.

La valutazione del rischio era stata condotta raccogliendo molti dati precisi,

come richiesto dal programma prescelto, e aveva richiesto alcuni mesi di lavoro. Nonostante ciò, evidentemente, non era riuscita a fornire risultati utili a giustificare i progetti avviati.

Il secondo difetto, comune a molti prodotti, consiste nella segretezza dell'algoritmo di calcolo. In questo modo, a fronte di risultati non accettabili, non ne è possibile comprendere l'origine per correggerla o per convincersi della validità dei risultati.

Il terzo difetto consiste nella configurazione iniziale del prodotto. Spesso i questionari e le misure di sicurezza sono impostati considerando un'organizzazione "tipo". Il più famoso software per la valutazione del rischio, ossia il CRAMM²², negli anni Novanta era parametrizzato secondo le medie imprese commerciali inglesi (infatti i questionari riportano le Sterline); molti altri sono configurati considerando organizzazioni grandi o grandissime. Spesso la configurazione è inadeguata al contesto in cui si vuole valutare il rischio.

Il quarto difetto è la difficoltà di riconfigurazione di questi strumenti. Questo si verifica in particolare quando si vogliono modificare i parametri di riferimento o aggiungere nuove minacce o nuove vulnerabilità.

Esempio 4.3.3. In molte banche si effettuano valutazioni del rischio relativo all'Internet banking. Molto spesso la minaccia di phishing non è prevista dai prodotti commerciali e, per quanto sia importantissima nel contesto di riferimento, non può essere censita a causa delle rigidità del prodotto usato per la valutazione del rischio.

Il quinto difetto è che gli utilizzatori di un software commerciale tendono ad adottarlo in modo meccanico, quando invece dovrebbero adattare il metodo al proprio contesto.

È evidente quanto un programma software possa essere utile per raccogliere i dati ed effettuare i calcoli necessari. Un foglio di calcolo può essere sufficiente ed essere configurato facilmente secondo le necessità.

4.3.2

Avvertenza

Quanto segue si basa su teorie consolidate nel tempo in merito all’analisi del rischio, non sempre relativo alla sicurezza delle informazioni. Infatti gli approcci più diffusi e propagandati in materia di analisi del rischio relativo alla sicurezza delle informazioni prevedono analisi molto accurate e di dettaglio, preferibilmente aiutate da software commerciali venduti da consulenti-venditori.

Per quanto riguarda le metodologie qualitative presentate nel seguito, alcune delle idee sono state tratte dall’esperienza maturata facendo uso di un semplice foglio di calcolo disponibile liberamente sul web [52, 53].

Ciò nonostante si raccomanda lo studio di diversi metodi per poi decidere quale utilizzare o svilupparne uno nuovo, adeguato alle proprie necessità. Sono disponibili alcuni cataloghi di metodi in pubblicazioni [93] o siti web²³. Alcuni di questi metodi non sono relativi alla sicurezza delle informazioni, ma possono fornire idee utili a chi voglia approfondire l’argomento e sviluppare nuove soluzioni. Quelli relativi alla sicurezza delle informazioni presentano tutti i passi descritti in questo libro, anche se talvolta utilizzano termini alternativi, aggregano alcune fasi o propongono algoritmi di calcolo diversi.

Esempio 4.3.4. Un esempio di metodo alternativo (“basato sugli eventi”) si basa sulla variante della fault tree analysis e prevede di analizzare le minacce e le loro conseguenze senza apparentemente identificare gli asset nel dettaglio.

Nella realtà, per identificare le minacce è necessario sapere quali elementi (asset) possono sfruttare (un’intrusione ai sistemi informatici può avvenire attraverso

una wi-fi pubblica, un'applicazione web, una rete informatica esposta su Internet) e quali controlli di sicurezza, necessariamente collegati a degli asset, la contrastano.

4.4

Chi coinvolgere

Tutte le parti interessate dovrebbero essere coinvolte nella valutazione del rischio: personale interno, inclusi i responsabili di funzione, clienti, fornitori e partner.

Nei capitoli successivi sono indicate altre figure da coinvolgere.

Ovviamente a ciascuno deve essere comunicato solo quanto necessario affinché possa contribuire alle diverse fasi.

Il coinvolgimento del personale, dei clienti, dei fornitori e partner può essere utile a:

identificare il rischio (ossia gli asset, le minacce e le vulnerabilità);

valutare il rischio, grazie alla condivisione del loro punto di vista e delle loro percezioni;

ponderare il rischio;

stabilire il piano di trattamento del rischio, perché devono contribuire alla pianificazione e attuazione delle azioni;

ridurre le incomprensioni in merito alle azioni da attuare;

ridurre le resistenze al cambiamento;

avere conseguenze positive sull'immagine dell'organizzazione percepita dai

propri clienti, fornitori e partner e dal personale.

I successivi paragrafi riguardano due ruoli particolari (i proprietari del rischio e i facilitatori), che meritano un approfondimento e sono richiamati nel seguito.

4.4.1

I responsabili del rischio

Una figura richiesta dalla ISO/IEC 27001 è quella di responsabile del rischio, la cui definizione è fornita dalla ISO/IEC 27000.

Responsabile del rischio (risk owner): persona o entità con la responsabilità e con il potere per gestire un rischio.

Il ruolo di responsabile del rischio, poiché deve avere potere di spesa, coincide spesso con quello della Direzione (paragrafo 12.3.1.1). Essa può delegare altre funzioni affinché facciano delle proposte in merito alla gestione del rischio e alle spese corrispondenti e coordinino le attività relative. La Direzione è sempre e comunque il responsabile ultimo del rischio (il termine “responsabile del rischio” è usato dalla ISO/IEC 27001 per allineamento alla ISO 31000, che non usa il termine “Direzione”).

In tutti i casi, i responsabili del rischio devono essere individuati a un livello gerarchico con adeguati poteri decisionali e di spesa, poiché devono decidere quali controlli di sicurezza attuare e mantenere.

Se le informazioni sono conservate, archiviate, comunicate o elaborate da fornitori, outsourcer o da altre entità, il responsabile del rischio deve essere comunque una persona interna all’organizzazione e può coincidere con il referente dei rapporti con queste entità esterne.

Se un rischio riguarda più aree dell’organizzazione, occorre stabilire come concordare le decisioni pertinenti, oppure se attribuire la responsabilità a un

livello gerarchico superiore comune.

4.4.2

I facilitatori

Alcune metodologie [4] invitano ad avvalersi di facilitatori per la conduzione degli incontri tra le parti interessate e per coordinare le diverse attività di descrizione del contesto, individuazione dell’ambito, identificazione, analisi, ponderazione e trattamento del rischio.

Spesso questo ruolo è ricoperto da uno o più consulenti esterni. Persone interne, con adeguate competenze, potrebbero ricoprirlo validamente, favoriti anche dalla più precisa conoscenza dell’organizzazione.

4.5

I documenti di gestione del rischio

Per la gestione del rischio, come si vedrà nel seguito, sono prodotti alcuni documenti. Alcuni di essi riportano anche carenze e vulnerabilità e pertanto vanno mantenuti riservati. Si deve anche ricordare che questi documenti possono essere scambiati tra più persone.

Vanno quindi applicati opportuni controlli di sicurezza, soprattutto di controllo degli accessi (paragrafo 12.6 e sugli scambi di informazioni (paragrafo 12.10.4).

Note

²⁰<https://www.money.it/imprese-fallite-stato-non-paga-crediti-commerciali>.

²¹<https://europrivacy.info/it/2015/07/21/pia-concept-directive-9546-current-draft-eu-part-1/>

²²Il link ufficiale www.cramm.com non risulta più attivo.

²³ENISA propone un catalogo alla pagina <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory>.

Capitolo 5

Il contesto e l'ambito

*JAQUES. All the world's a stage,
And all the men and women merely players.*

William Shakespeare, As you like it, Atto II, Scena VII.

In questo capitolo si descrivono le fasi preliminari alla valutazione del rischio. Queste prevedono un'analisi del contesto in cui si vuole operare in modo da decidere in quale ambito valutare il rischio.

Si potrà decidere di valutare il rischio per tutta l'organizzazione, di estendere l'attività anche a parti esterne o di ridurla a un perimetro più limitato (per esempio, ai soli servizi offerti ai clienti).

5.1

Il contesto

La definizione della ISO 9000:2015 fornisce una prima indicazione.

Contesto di un'organizzazione: combinazione di fattori interni ed esterni che possono avere degli effetti sullo sviluppo e raggiungimento degli obiettivi di un'organizzazione.

È utile presentare l'elenco degli elementi da includere nella descrizione del contesto [92]. Questi elementi si dividono in fattori (issues) interni ed esterni. Tra i fattori interni vi sono:

le strategie attuali e future e le relative priorità;

il livello di innovazione, attuale e prevista;

le caratteristiche delle attività principali svolte in termini di servizi e prodotti offerti e le modifiche previste al portafoglio dei prodotti e servizi offerti;

la struttura organizzativa, inclusi i fornitori principali e i processi affidati all'esterno (in outsourcing o esternalizzati);

le caratteristiche delle sedi;

le tipologie di informazioni trattate;

le caratteristiche principali del sistema informativo dell'organizzazione, tra cui:

i principali servizi informatici e le relative tecnologie infrastrutturali e applicative;

il tipo di dispositivi portatili in uso, se presenti, tra cui cellulari, smartphone e tablet;

gli archivi non informatici come quelli cartacei;

i luoghi dove sono collocati i sistemi informatici e gli archivi non informatici, inclusi quelli gestiti da fornitori;

quali sistemi informatici sono condivisi con altre entità (clienti, fornitori, partner e altri soggetti esterni) e chi ne ha la proprietà (un'organizzazione può usare alcuni sistemi dei clienti, fornitori o partner per comunicare con loro);

i rapporti con il personale interno (indipendentemente dalla tipologia di contratto tra le parti) e le loro competenze informatiche;

le aspettative delle parti interne interessate (stakeholder), ossia del personale, degli azionisti e dei soci; tra queste aspettative vi è il rispetto dei contratti e degli accordi e la buona qualità dell'ambiente di lavoro.

Tra i fattori esterni che potrebbero avere impatti sulla sicurezza delle informazioni vi sono:

i concorrenti e i potenziali concorrenti;

la normativa applicabile e se ne sono previste modifiche nel medio periodo;

la situazione economica attuale e prevista nelle zone in cui opera l'organizzazione;

il clima politico e sociale nelle zone in cui opera l'organizzazione;

la disponibilità sul mercato e i costi delle risorse utili all'organizzazione;

le strategie di mercato, attuali e previste, dei clienti, fornitori e partner attuali e potenziali;

le aspettative delle parti esterne interessate, tra cui i clienti, i fornitori e i partner

attuali e potenziali, le società dello stesso gruppo dell’organizzazione e gli enti normativi e di controllo; tra queste aspettative vi è il rispetto dei contratti e degli accordi, degli accordi intra-gruppo e della normativa vigente.

Quando si descrive il contesto non è necessario descrivere tutti i punti sopra elencati, ma solo quelli significativi per la sicurezza delle informazioni.

Esempio 5.1.1. La descrizione del contesto di un’azienda casearia potrebbe essere il seguente.

Caratteristiche dei servizi e prodotti. L’azienda si occupa di produzione e vendita di prodotti caseari. Essa ha un fatturato annuo di circa 10 milioni di Euro.

Struttura organizzativa. La struttura organizzativa è descritta nell’organigramma (figura 5.1.1). Ulteriori fornitori, oltre al commercialista e agli agenti commerciali, sono: lo sviluppatore del CRM, un operatore di telecomunicazioni, una società di vigilanza e un’impresa di pulizie.

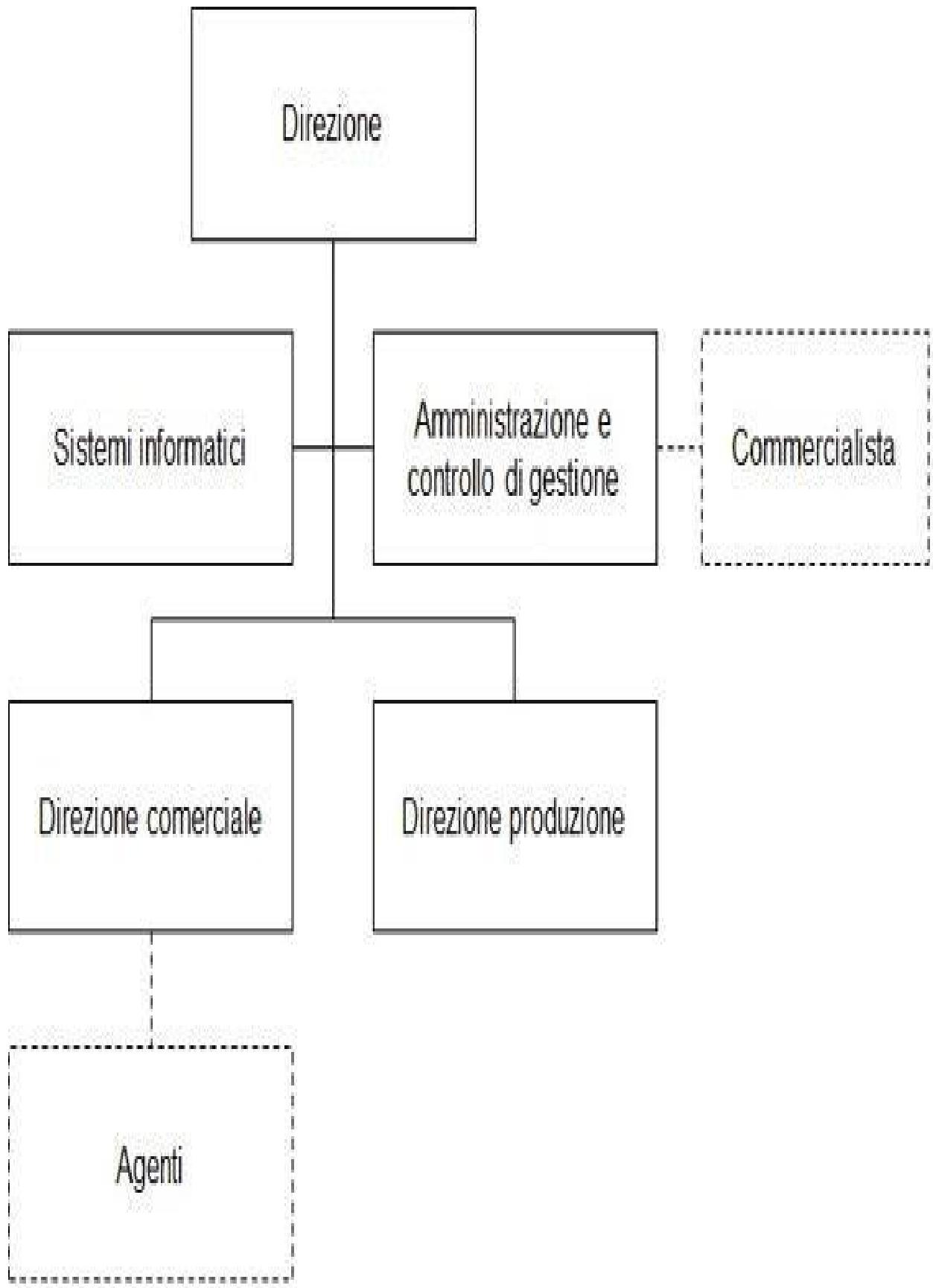


Figura 5.1.1:

Esempio di organigramma

Ubicazioni fisiche. L’azienda ha sede in una cascina di proprietà, non condivisa con altre organizzazioni, nel comune di Basilio (MI).

Informazioni trattate. Le informazioni trattate sono quelle relative ai clienti, ai fornitori, ai partner, al personale e ai prodotti (le ricette e le verifiche di qualità). Per evitare di avvantaggiare la concorrenza, è molto importante garantire la riservatezza delle informazioni sui clienti, sui fornitori e sui partner; per il rispetto della normativa vigente in materia di privacy è importante trattare correttamente i dati del personale e, per salvaguardare il patrimonio di conoscenze aziendali, è necessario garantire la riservatezza e integrità delle ricette e dei verbali di verifica.

Sistema informatico. Da un punto di vista sistemistico, l’architettura si basa su sistemi Microsoft Windows per i server e i PC. Le applicazioni e i servizi più importanti sono: sistema di posta elettronica, file server, CRM (customer relationship management) e un sistema sviluppato internamente per il controllo del magazzino e della produzione. Gli agenti possono accedere al CRM e quindi all’anagrafica clienti e allo stato degli ordini da qualsiasi strumento dotato di web browser.

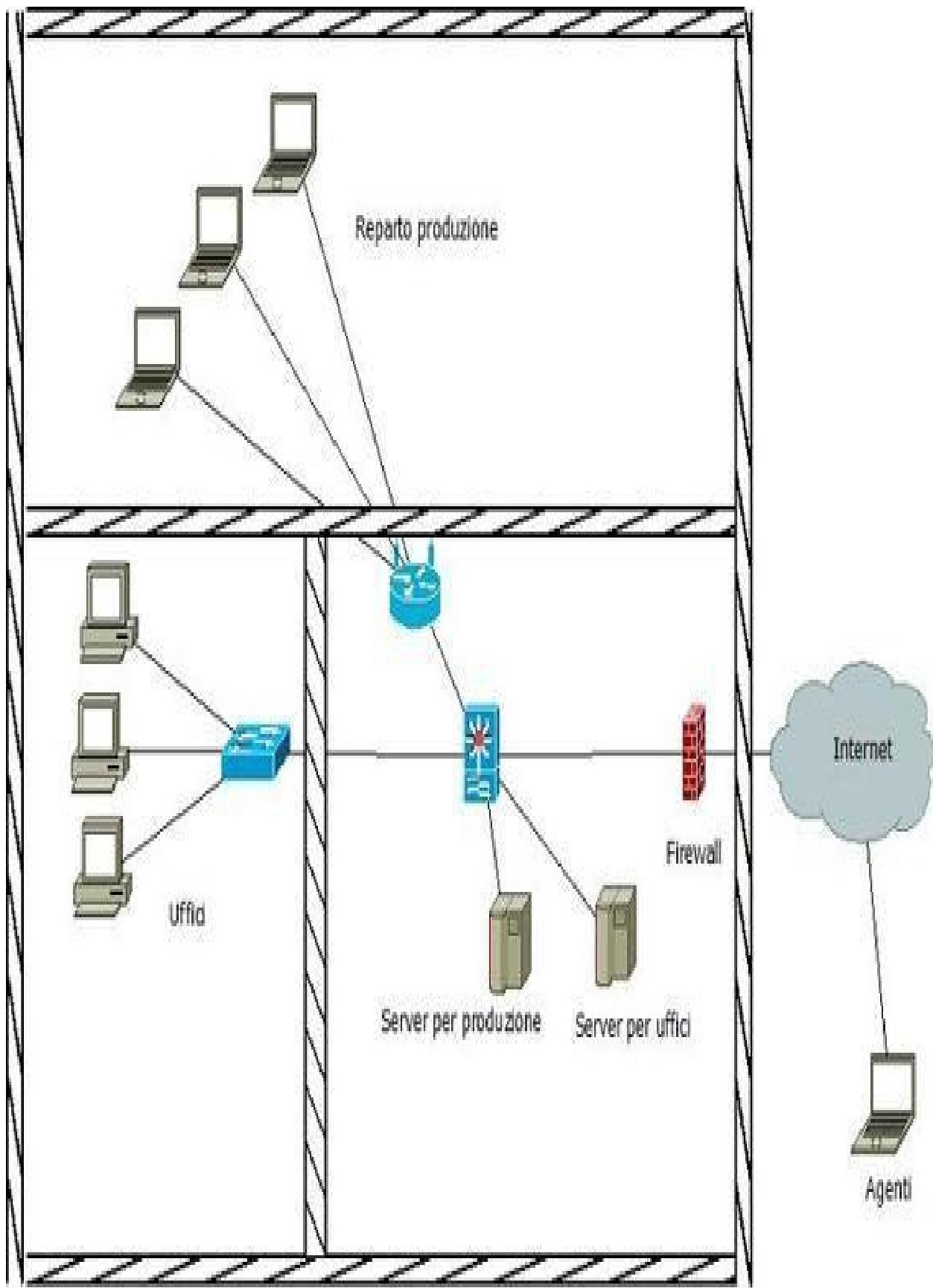


Figura 5.1.2:

Esempio di rete IT



Archivi cartacei. Tutti i dati possono essere anche in copie cartacee, archiviate in sede in appositi archivi o, limitatamente ai dati di tipo contabile e amministrativo, nello studio del commercialista.

Concorrenti. La concorrenza è molto sentita nel settore, ma non è tale da far temere attività di spionaggio industriale.

Clienti. I clienti richiedono il rispetto delle scadenze e la qualità dei prodotti, in linea con i contratti stipulati e la normativa vigente.

Fornitori. Oltre agli agenti, i fornitori principali sono quelli di materie prime e imballi e si attendono di veder apprezzati i loro sforzi per soddisfare le richieste dell'azienda e di essere pagati secondo le scadenze pattuite.

Personale interno. Composto da 13 persone tra impiegati e operai, con istruzione e formazione non elevata e senza competenze specifiche sull'uso dei sistemi informatici, tranne i due addetti al loro sviluppo e manutenzione. Si aspettano di lavorare in un buon posto di lavoro, rispettoso della normativa vigente (tra cui lo Statuto dei lavoratori e la privacy) e delle scadenze dei pagamenti. Il clima aziendale è buono e non si sono registrate contestazioni rilevanti negli ultimi venti anni.

Normativa vigente. La normativa richiede estrema cura nel mantenimento delle informazioni sui prodotti immessi sul mercato e per questo è vitale garantire l'integrità dei dati relativi alla produzione. Non sono previste modifiche di rilievo nel lungo periodo, ma occorre tenerla sotto controllo.

Livello di innovazione. Le innovazioni sono necessarie per mantenere la competitività sul mercato (informatizzazione del magazzino, comunicazioni con i

fornitori via strumenti elettronici, eccetera).

5.2

L'ambito

Dopo aver individuato il contesto, è possibile decidere l'ambito (in inglese scope) in cui effettuare la valutazione del rischio relativo alla sicurezza delle informazioni. Esso può comprendere tutta l'organizzazione o una parte di essa.

Spesso il fattore relativo alla percezione dei clienti è ritenuto così importante che si riduce l'ambito ai soli servizi loro offerti.

Esempio 5.2.1. L'azienda casearia potrebbe decidere di valutare il rischio relativo alla sicurezza delle informazioni per tutta l'organizzazione perché ogni area ha impatti sui tre fattori ritenuti fondamentali dalla Direzione: rapporti con i clienti, qualità del prodotto e soddisfazione del personale.

La stessa azienda potrebbe limitare l'ambito alla produzione, sia a causa degli impatti sui clienti, sia perché richiesto dalla normativa vigente nel campo alimentare.

L'ambito potrebbe essere esteso anche ai fornitori, nel caso in cui trattino dati dell'organizzazione o forniscano prodotti critici.

Alcuni processi non possono essere completamente esclusi dall'ambito, in particolare se la finalità della valutazione del rischio è la certificazione del sistema di gestione per la sicurezza delle informazioni.

Esempio 5.2.2. Se l'azienda casearia decidesse di valutare i rischi relativi alla sicurezza delle informazioni solo nell'ambito della produzione, dovrebbe comunque considerare alcuni processi apparentemente esterni a essa. Per esempio, la gestione del personale è esterna alla produzione, ma molto importante per la sicurezza delle informazioni (paragrafo 12.4). Per questo deve, almeno parzialmente, essere inclusa nell'ambito.

Se l'azienda casearia ha un fornitore di servizi informatici, anch'esso deve essere incluso.

Quando si stabilisce l'ambito, ne devono essere analizzati i confini.

Esempio 5.2.3. Quando si stabilisce l'ambito dell'azienda casearia, è necessario rilevare che i suoi sistemi informatici sono connessi a internet, che il CRM è accessibile via web da qualsiasi PC e che alcuni dati sono accessibili agli agenti esterni.

L'ambito dovrebbe quindi essere descritto riportando:

le tipologie di informazioni che si vogliono proteggere;

le caratteristiche dei servizi erogati o dei prodotti realizzati dall'organizzazione e pertinenti le informazioni da proteggere;

la struttura organizzativa coinvolta nelle attività comprese nell’ambito e i suoi rapporti con la parte di organizzazione esclusa dall’ambito;

la tecnologia adottata, uno schema della rete informatica e una descrizione delle sue interfacce con altri sistemi informatici dell’organizzazione o dei fornitori esclusi dall’ambito;

le sedi e i locali dove sono trattate le informazioni oggetto dell’ambito e dove sono collocati gli archivi e i sistemi informatici compresi nell’ambito, inclusi quelli presso fornitori o altre parti esterne;

i fornitori più importanti coinvolti nella sicurezza delle informazioni, inclusi quelli che sviluppano o conducono i sistemi informatici dell’organizzazione.

Capitolo 6

Identificazione del rischio

Sarebbe un inutile sfoggio di potenza.

(That's much too vulgar a display of power).

Dal film L'esorcista

Iniziamo dalla definizione della ISO/IEC 27000.

Identificazione del rischio: processo di individuazione, riconoscimento e descrizione del rischio.

Nel capitolo 4 abbiamo già visto che questo processo richiede l'identificazione di:

asset;

minacce;

vulnerabilità e controlli di sicurezza;

relazioni tra asset, minacce e vulnerabilità.

6.1

Gli asset

Cominciamo con il riportare la definizione ora non più presente nella ISO/IEC 27000, ma sempre utile.

Asset (bene): qualsiasi cosa che abbia valore per l'organizzazione.

Nota: esistono molti tipi di asset, tra cui: informazioni, software e programmi per computer, elementi fisici (per esempio i computer), servizi, persone e le loro qualifiche, competenze ed esperienze, reputazione e immagine dell'organizzazione.

I primi asset da identificare sono le informazioni per poi correlarle a tutti gli asset che le contengono o le trattano, inclusi quelli gestiti da fornitori.

Alcuni estendono l'ambito dell'analisi e identificano l'immagine dell'organizzazione o le automobili. La loro protezione è spesso estranea alla sicurezza delle informazioni e pertanto queste estensioni sono inappropriate, anche se erano previste dalla definizione.

La ISO/IEC 27002 usa in molti punti l'espressione “information and other associated assets” e pertanto questo paragrafo tratta inizialmente delle informazioni e poi degli “altri asset”.

Categorie di asset sono:

le informazioni in formato digitale;

i server fisici e virtuali;

le applicazioni, inclusi i database management system, le applicazioni server e quelle accessibili da Internet;

i personal computer fissi;

i personal computer e i dispositivi informatici portatili (cellulari, smartphone, tablet, hard disk portatili, eccetera);

la rete informatica;

le apparecchiature della rete informatica;

il personale interno ed esterno;

i fornitori;

i documenti in formato non informatico e gli archivi cartacei;

la sede e i locali;

i processi e le unità organizzative;

l'organizzazione nel suo complesso.

6.1.1

Informazioni

Molte cose possono andare male quando le informazioni sono statiche e conservate in un sistema informatico o in un archivio. Ancora più cose possono andare male (e lo fanno) quando le persone cominciano a trattare le informazioni. Le persone devono trattarle, altrimenti sarebbero inutili: le usano, le creano, le modificano, le conservano, le distruggono, le condividono, eccetera.

Per individuare le informazioni conviene partire dai processi dell'organizzazione.

Esempio 6.1.1. Nell'azienda casearia descritta precedentemente, le informazioni sono:

quelle per la gestione commerciale e operativa dei clienti;

quelle per la gestione commerciale e operativa dei fornitori e delle forniture;

quelle sul personale aziendale: dati anagrafici, competenze e formazione, stato di salute;

quelle sui prodotti in magazzino e sulla programmazione della produzione;

le ricette e i resoconti delle verifiche dei prodotti realizzati.

Non è necessario specificare la composizione delle informazioni (per esempio indicando, per quelle sui clienti, ragione sociale, Partita IVA, indirizzo di fatturazione, fatture, indirizzi di spedizione, referenti, eccetera): l'importante è

aggregarle convenientemente affinché l'analisi dei rischi non diventi troppo dispersiva o troppo generica.

Un approccio per identificare e valutare le informazioni consiste nel seguire le attività di un processo e chiedere al loro responsabile quali informazioni sono usate, se sono usate solo come riferimento o sono create, modificate, distrutte o trasmesse e quali sono le conseguenze per ogni attività se le informazioni non sono disponibili, rese note a persone non autorizzate o non corrette. Questo approccio permette ai responsabili di realizzare quanto sono dipendenti dalle informazioni.

6.1.2

Gli altri asset

Dopo aver individuato le informazioni è necessario individuare gli altri asset utilizzati per trattarle o conservarle.

Esempio 6.1.2. Nell'azienda casearia descritta precedentemente, gli asset utilizzati per trattare le informazioni sono:

i servizi informatici di supporto con relativi archivi informatici: PC del personale e server per la gestione delle e-mail e la condivisione dei file;

il servizio CRM con relativo archivio informatico; esso è accessibile dal personale interno e dagli agenti;

il sistema informatico di controllo del magazzino e della produzione con relativo archivio informatico; esso è accessibile dal personale interno;

gli archivi cartacei presso la sede e la sede stessa;

gli archivi cartacei e informatici presso il commercialista.

Non è necessario elencare ogni singolo asset, quanto individuare delle loro aggregazioni, basate su:

omogeneità geografica per gli asset fisici;

uso di procedure omogenee per la loro gestione;

le persone responsabili della loro gestione e sicurezza (asset owner).

Esempio 6.1.3. Ai fini della valutazione del rischio, non è necessario sapere esattamente quanti e quali armadi sono presenti in un ufficio, ma sapere se ci sono e quali informazioni sono lì conservate. Sarà sufficiente identificare “armadi dell’ufficio x”.

Questi armadi sono infatti nello stesso luogo, hanno caratteristiche tecniche simili, le modalità di accesso sono regolate dalle medesime procedure e il loro responsabile è il medesimo.

Per l’azienda casearia è possibile aggregarli sotto la voce “archivi sede”.

Esempio 6.1.4. Un CRM come quello dell’azienda casearia è composto da più asset: il server fisico, il sistema operativo, il programma applicativo, eccetera.

In questo caso, con il termine “CRM” si intende quindi un’aggregazione di asset.

Il dettaglio degli asset è importante per la gestione operativa (come si vedrà in 12.5), non per la valutazione del rischio. Alcuni identificano, inutilmente in questa fase, singoli server, firewall, apparati di rete, PC, applicazioni, software di base, eccetera.

Le analisi del rischio basate sulla valutazione minuziosa degli asset portano a degli errori di valutazione.

Esempio 6.1.5. Nel 2006 la TJX, grande azienda commerciale, fu attaccata e dei malintenzionati hanno avuto accesso alla sua rete sfruttando la wi-fi di un suo negozio: da questa riuscirono ad accedere alla rete interna e copiarono i dati delle carte di credito di 46 milioni di clienti e altri dati di altre 450.000 persone²⁴.

Sicuramente, la “wi-fi dei negozi” fu correttamente identificata, ma valutata come poco critica e non si considerarono i rischi a essa collegati.

È sempre opportuno identificare i fornitori (inclusi quelli di vigilanza e di pulizia) e l’organizzazione nel suo complesso, perché a essi dovranno essere applicati i controlli di sicurezza.

Si devono quindi identificare le relazioni tra informazioni e asset utilizzati per trattarle e conservarle.

Esempio 6.1.6. Le relazioni tra le informazioni e gli altri asset dell’azienda casearia sono riportate nella tabella 6.1.1.

	Server file e e-mail	CRM	Sistemi IT mag. e prod.	Archivi sede	Archivi Commerciali	PC desktop	Fornitori pulizie	Sede	Organizzazione
Informazioni clienti	X	X	X	X	X	X	X	X	X
Informazioni fornitori	X	X	X	X	X	X	X	X	X
Informazioni personale	X			X	X	X	X	X	X
Informazioni produzione	X		X	X		X	X	X	X
Informazioni ricette	X		X	X		X	X	X	X

Tabella 6.1.1:

Esempio di relazioni tra informazioni e asset

Anche se è necessario aggregare e semplificare, è comunque necessario disporre di una descrizione dettagliata dei diversi gruppi di asset affinché nel seguito si possano identificare le misure di sicurezza applicabili ai diversi ambiti, come è descritto nel paragrafo 7.5.2.

6.1.3

Chi identifica gli asset

Per l'identificazione delle informazioni si dovrebbero coinvolgere i responsabili delle aree dell'organizzazione comprese nell'ambito. Essi dovrebbero identificare le informazioni create e utilizzate dalla propria area.

Gli stessi responsabili dovrebbero identificare gli asset con i quali svolgono le operazioni di trattamento delle informazioni, in particolare le applicazioni informatiche e gli archivi fisici.

Questi responsabili possono essere chiamati responsabili delle informazioni, ma, per evitare confusioni con la normativa privacy (paragrafo 12.15.1.9), si preferisce usare le espressioni referenti per le informazioni o utenti responsabili.

I referenti per le informazioni potrebbero coincidere con i responsabili del rischio a esse relativo, oppure essere altre persone con le competenze per identificare e valutare le informazioni e collaborare alla valutazione del rischio, ma senza il potere per gestirlo.

Sovente sono delegati a svolgere questa attività il responsabile dei sistemi informatici o quello della sicurezza fisica. Nel limite del possibile bisognerebbe invece coinvolgere tutti i livelli gerarchici dell'organizzazione, anche in riunioni congiunte, in modo che acquistino consapevolezza sui rischi relativi alla sicurezza delle informazioni.

I responsabili dei sistemi informatici dovrebbero descrivere le architetture delle applicazioni, i server, i segmenti di rete e gli interfacciamenti con altri sistemi.

I responsabili della sicurezza fisica dovrebbero fornire indicazioni su come sono organizzate le sedi, gli uffici, gli archivi e le sale server.

Alcuni preferiscono inviare un questionario da far compilare ai responsabili soprattutto quando sono numerosi e l'organizzazione è distribuita su un territorio molto vasto.

È invece preferibile un incontro personale tra i facilitatori e i referenti per le informazioni, soprattutto se questi ultimi non hanno mai affrontato in precedenza il compito e quindi necessitano di assistenza per capire la finalità della raccolta dati. Ciò può anche far emergere aspetti che, di fronte a un questionario da affrontare in solitudine, potrebbero restare inespressi. Una riunione ben condotta può richiedere al massimo un paio d'ore per ottenere tutti i dati necessari.

6.2

Le minacce

Le minacce, lo ricordiamo, sono le variabili m viste nelle formule del paragrafo 4.1.2. Se ne fornisce la definizione della ISO/IEC 27000, insieme a quella di evento e incidente.

Evento relativo alla sicurezza delle informazioni: occorrenza identificata dello stato di un sistema, servizio o rete che identifica una possibile violazione delle politiche di sicurezza o un errore nei controlli o una situazione precedentemente sconosciuta che può essere significativa per la sicurezza.

Incidente relativo alla sicurezza delle informazioni: uno o più eventi relativi alla sicurezza delle informazioni che hanno una significativa probabilità di compromettere le attività di un’organizzazione e minacciare la sicurezza delle informazioni.

Minaccia: causa potenziale di un incidente, che può comportare danni a un sistema o all’organizzazione.

Si osservi che altre norme utilizzando il termine fonte di rischio (risk source) al posto di minaccia.

Nel seguito, quando si tratta di eventi e incidenti ed è chiaro il contesto, non è specificato “relativi sicurezza delle informazioni”, anche se sarebbe sempre opportuno utilizzare questa espressione.

È necessario cogliere la differenza tra evento e minaccia: la minaccia è potenziale, mentre un evento è qualcosa che accade realmente. In altre parole, una minaccia è un possibile evento.

Eventi e incidenti potrebbero non comportare danni. Per esempio, l'intrusione di uno sconosciuto nella sede dell'organizzazione è un incidente, anche se viene fermato prima che possa compiere dei danni. Alcuni testi [77] utilizzano il termine accidente per indicare un incidente con danni, altri ancora usano l'espressione near miss per indicare un incidente senza danni. La ISO/IEC 27001 usa solo il termine "incidente".

Esempio 6.2.1. Il furto in casa è una minaccia che tutti percepiamo come effettiva, anche se non l'abbiamo mai sperimentato.

L'arrivo in città di una celebre banda di topi di appartamento è un evento relativo alla sicurezza delle informazioni (situazione precedentemente sconosciuta e significativa per la sicurezza), così come il guasto dell'antifurto (errore nei controlli).

L'ingresso di ladri nell'appartamento e il furto di un PC con dati critici è un incidente di sicurezza delle informazioni. Lo è anche se il PC non venisse rubato (i ladri potrebbero preferire i gioielli) perché c'era comunque una significativa probabilità che lo fosse.

L'identificazione di una minaccia può essere svolta a diversi livelli di dettaglio: normalmente si effettua una prima analisi non troppo dettagliata, per poi migliorarla nei successivi riesami periodici.

Esempio 6.2.2. È accettabile identificare e valutare la minaccia “Malware” senza dettagliarla ulteriormente. In un secondo tempo si potrebbe distinguere tra virus, trojan, spyware, eccetera.

La minaccia “furto di materiale” potrebbe essere successivamente raffinata considerando il materiale all’interno o all’esterno dell’organizzazione.

L’analisi del rischio relativo alla sicurezza delle informazioni richiede di identificare e valutare tutte le minacce relative alla sicurezza delle informazioni. È quindi inaccettabile, per esempio, identificare minacce solo informatiche oppure solo quelle più significative. Questo è contrario alla finalità stessa dell’analisi del rischio (in caso contrario si denominerebbe analisi di alcuni rischi), che presuppone analisi sistematiche e complete. Si possono escludere le minacce con probabilità bassa, ma solo dopo averle esplicitamente valutate, come descritto nel paragrafo 7.3.

Per rendere sistematica l’analisi delle minacce, è opportuno iniziare da una lista predefinita (vedere anche il capitolo 11), in modo da non dimenticarne nessuna.

Per meglio individuare le minacce, si inizia dall’individuazione degli agenti di minaccia, per poi individuare le tecniche di minaccia.

6.2.1

Gli agenti di minaccia

Una classificazione delle minacce può essere basata sull’agente di minaccia, ossia sull’entità responsabile del manifestarsi della minaccia. Gli agenti possono essere i seguenti:

le persone malintenzionate;

le persone non malintenzionate;

gli strumenti tecnici;

la natura.

Prima di procedere, si definisce servizio condiviso un servizio utilizzato da più organizzazioni e gestito da una di esse: alcuni clienti impongono ai fornitori di utilizzare i propri sistemi informatici; viceversa, un fornitore può mettere a disposizione dei propri clienti un sistema informatico.

6.2.1.1 Le persone malintenzionate

Questi agenti di minaccia sono i più complessi e variegati da analizzare e possono essere:

persone esterne all’organizzazione, inclusi:

gli utenti dei servizi pubblici offerti dall’organizzazione; essi possono accedere ai locali dell’organizzazione (per esempio, in un’agenzia bancaria) o a parte dei

sistemi informatici (per esempio ai siti web o ai social network);

i clienti, che potrebbero avere accesso ai locali dell’organizzazione quando sono in visita e ai servizi informatici condivisi;

i fornitori generici, che possono avere accesso ai locali dell’organizzazione, quando sono in visita o devono consegnare del materiale, e ai servizi informatici condivisi;

i fornitori di servizi informatici, che possono avere accesso privilegiato e temporaneo ai sistemi informatici (se coinvolti in progetti limitati nel tempo) oppure non temporaneo (se offrono servizi continuativi di conduzione e manutenzione dei sistemi e delle applicazioni informatiche);

persone interne all’organizzazione, con ruoli di utenti non privilegiati o di utenti privilegiati dei sistemi informatici (i cosiddetti amministratori disistema).

È possibile suddividere gli agenti di minaccia malintenzionati sulla base delle loro motivazioni:

esibizionisti: persone che intendono pubblicare informazioni riservate o rendere indisponibili i sistemi informativi dell’organizzazione per poi attribuirsi pubblicamente il “merito”; in questa categoria possono rientrare gli squilibrati;

attivisti: persone spinte da ragioni politiche o filosofiche che intendono danneggiare l’organizzazione rendendo indisponibili i sistemi informativi o pubblicando informazioni riservate; in questo gruppo sono da includere, anche se adottano tecniche e hanno motivazioni tra loro diverse, i terroristi, i sabotatori e i vandali; i promotori della pubblicazione di informazioni coperte da segreto di Stato²⁵ possono rientrare in questa categoria;

spie: persone che intendono accedere a informazioni riservate dell’organizzazione per profitto o proprio vantaggio; le spie possono essere singole persone, organizzazioni private (inclusi concorrenti, clienti, fornitori e partner) o organizzazioni governative; affini alle spie sono gli agenti di influenza, che intendono modificare i dati dell’organizzazione allo scopo di

cambiare la percezione delle persone su un determinato argomento;

ladri: persone che rubano risorse materiali dell'organizzazione per profitto personale o estorcono denaro attraverso ricatti;

truffatori: persone che intendono conoscere o modificare informazioni dell'organizzazione per profitto personale;

entità straniere ostili: entità che possono partecipare a un conflitto, anche non convenzionale, o svolgere attività di spionaggio;

personale scontento: persone spinte da insoddisfazione verso l'organizzazione per cui lavorano e che intendono danneggiarla, rendendo indisponibili i sistemi informativi o pubblicando informazioni riservate; sono anche indicati con il termine insider.

Non sono compresi gli hacker. Il termine è utilizzato per indicare esperti di informatica o persone che attaccano sistemi informatici spinti da diverse motivazioni.

La corretta definizione di hacker è da sempre al centro di lunghi e accesi dibattiti nella comunità degli esperti di sicurezza informatica. Basti dire che si possono utilizzare altri termini:

cracker o blackhat: hacker malintenzionati;

greyhat: esibizionisti che, una volta introdotti nei sistemi, divulgano alcuni dettagli dell'impresa e non arrecano ulteriori danni (a parte all'immagine dell'organizzazione colpita);

whitehat o ethical hacker: coloro che eseguono vulnerability assessment sui sistemi di loro clienti dopo averne avuto il mandato (paragrafo 12.15.4).

6.2.1.2 Le persone non malintenzionate

Le persone fanno errori o azioni senza essere consapevoli degli impatti sulla sicurezza delle informazioni.

Gli errori possono essere compiuti da persone interne ed esterne, inclusi utenti dei sistemi informatici e visitatori, clienti, fornitori e partner. Il personale interno, e in particolare gli amministratori di sistema, in caso di errori, potrebbero fare più danni rispetto agli esterni: sono numerosi i casi di configurazioni o cambiamenti ai sistemi informatici autorizzati ma disastrosi a causa di errori.

6.2.1.3 Gli strumenti tecnici

Gli strumenti tecnici possono manifestare dei comportamenti imprevisti dovuti alla loro scorretta progettazione o produzione e a cause naturali come polvere, temperature estreme o obsolescenza.

6.2.1.4 La natura

La natura, lo sappiamo bene, può essere un avversario terribile e può manifestarsi in molti modi e con impatto sulla disponibilità delle informazioni: terremoti, precipitazioni abbondanti, temperature estreme, uragani, eccetera.

6.2.2

Tecniche di minaccia

Nel capitolo 11 sono illustrate delle minacce normalmente pertinenti a tutte le organizzazioni.

Esse sono di tipo generale ed è buona norma, quando si riesamina la valutazione del rischio, ampliare questo elenco con minacce più dettagliate.

Esempio 6.2.3. L'esaurimento di risorse (paragrafo 11.19) potrebbe essere ulteriormente specificato con:

attacco di Denial of Service da parte di esterni malintenzionati;
uso eccessivo e involontario delle risorse da parte degli utenti;
sciopero;
malattia.

A questo scopo è importante trovare dei metodi per essere aggiornati sugli incidenti occorsi ad altre organizzazioni (vedere paragrafo 12.3.5).

6.2.3

Le minacce e il rischio privacy

Quando si valuta il rischio relativo alla privacy, è possibile identificare minacce specifiche per la privacy. Tra di esse vi sono:

rappresentazione scorretta, se i dati relativi a una persona sono o sbagliati o presentati o elaborati in modo scorretto; questa minaccia può anche riguardare i risultati della profilazione di una persona (che, per esempio, potrebbe essere esclusa da programmi sanitari o economici), anche con strumenti basati sull'intelligenza artificiale;

distorsione, ossia l'interpretazione volutamente o inavvertitamente scorretta dei dati, con potenziali impatti negativi sulla singola persona; questa minaccia è, in parole poche, quella del pettegolezzo e della maledicenza, che può portare al biasimo, alla stigmatizzazione, all'isolamento e anche alla perdita di libertà di una persona;

sorveglianza, attraverso l'uso dei dati, soprattutto in ambito informatico; è necessario riconoscere la differenza tra logging (ossia la raccolta di dati per assicurare la sicurezza delle persone e della proprietà) e la sorveglianza (che porta, anche se non sempre per scelta deliberata, a discriminazione, perdita di fiducia, autonomia o libertà, danni fisici);

blocco alla conoscenza dei dati trattati, ossia segretezza in merito al fatto che i dati personali sono trattati e alle modalità con cui lo sono; questo può portare all'uso dei dati personali iniquo e, per le singole persone fisiche, alla mancanza di auto determinazione, alla perdita di fiducia e a perdite economiche;

6.2.4

Chi individua le minacce

Le minacce dovrebbero essere inizialmente individuate dai referenti per le informazioni, ma spesso non hanno le competenze per farlo. È quindi utile coinvolgere i responsabili dei sistemi informatici, della sicurezza fisica, della gestione del personale, dell'ufficio legale e dell'ufficio acquisti. Queste persone possono riferire su eventi e incidenti avvenuti nel passato o in contesti simili a quello oggetto di analisi.

Come per l'identificazione delle informazioni (paragrafo 6.1.3), l'invio di un questionario ai rappresentanti delle diverse aree può essere utile in organizzazioni di grandi dimensioni, ma sono sempre preferibili incontri con i facilitatori.

Questa attività è spesso effettuata insieme alla valutazione delle minacce, di cui si discuterà nel paragrafo 7.3.2.

6.3

Associare le minacce agli asset

Tutte le metodologie, più o meno esplicitamente, associano le minacce agli asset per valutarne la verosimiglianza.

Nella maggior parte dei casi non è necessario stimare la probabilità di accadimento di ogni singola minaccia rispetto a ogni singolo asset, ma rispetto a tutti gli asset della medesima categoria e considerando il contesto generale. Infatti, il valore della minaccia non cambia in funzione del singolo asset, ma dei fattori interni ed esterni e delle motivazioni e capacità degli agenti.

Bisogna prestare molta attenzione alle eccezioni a questa regola.

Esempio 6.3.1. Può non essere opportuno aggregare le sedi quando si trovano in luoghi con caratteristiche diverse. Per esempio, se si ha una sede in Lombardia e una in Campania, dove le probabilità di terremoto sono diverse.

Solitamente non è opportuno aggregare gli strumenti portatili assegnati al personale con quelli fissi, perché i primi sono più frequentemente oggetto di furto.

Per quanto riguarda le minacce di tipo informatico, il malware è più diffuso per i sistemi Windows e Android rispetto ad altri; inoltre i servizi informatici disponibili al pubblico sono maggiormente attaccati di quelli disponibili ai soli clienti, fornitori e partner o al solo personale interno.

In questa fase è quindi necessario effettuare una primissima valutazione delle minacce (da approfondire in una fase successiva, descritta nel paragrafo 7.3), in modo da individuare le relazioni significative tra minacce e asset.

Esempio 6.3.2. Nell’azienda casearia, è possibile individuare i seguenti gruppi di asset, a cui associare le minacce:

server, che includono il file server e l’e-mail server, il CRM e il sistema informatico per il controllo del magazzino e della produzione;

gli archivi della sede e del commercialista;

i personal computer fissi;

i fornitori, inclusi quelli delle pulizie e il commercialista;

la sede e i locali;

l’organizzazione.

Questi gruppi di asset sono associati alle minacce in tabella 6.3.1, dove gli elenchi di asset e minacce non sono esaustivi.

	Server	Archivii	Pc fissi	Fornitori	Sedie e Locali	Organizzazione
Malware	X		X	X		X
Accesso non autorizzato ai sistemi IT	X		X	X		X
Lettura e copia non autorizzate di documenti digitali	X		X	X		X
Danneggiamento di apparecchiature fisiche	X	X	X	X	X	X
Invio di dati a persone non autorizzate	X	X	X	X		X

Tabella 6.3.1:

Esempio di relazione tra minacce e asset

6.4

Collegare le minacce alle conseguenze

Nel paragrafo 2.2 si era visto come un incidente di sicurezza delle informazioni possa essere collegato a uno o più parametri di riservatezza, integrità e disponibilità. Si può adottare lo stesso procedimento alle minacce.

Esempio 6.4.1. Riprendendo l'esempio 2.2.6 e modificando leggermente la prima colonna, si ottiene la tabella 6.4.1.

Minaccia	R	I	D
Incendio		X	X
Modifica non autorizzata di documenti informatici da non malintenzionati		X	
Modifica non autorizzata di documenti informatici da malintenzionati		X	
Blackout elettrici		X	X
Malware		X	X
Lettura e copia non autorizzate di documenti digitali	X		
Invio di dati a persone non autorizzate	X		
Danneggiamento di apparecchiature fisiche	X	X	X
Danneggiamenti dei programmi informatici	X	X	X
Accesso non autorizzato ai sistemi IT	X	X	X
Attacchi di esaurimento risorse			X

Tabella 6.4.1:

Esempio di relazione tra minacce e parametri RID

Questo esercizio sarà utile in seguito, quando si dovrà calcolare il livello del rischio.

6.5

Le vulnerabilità e i controlli di sicurezza

Le vulnerabilità sono il terzo elemento che contribuisce al calcolo del livello di rischio, come visto nelle formule del paragrafo 4.1.2. La definizione è la seguente, secondo la ISO/IEC 27002.

Vulnerabilità: debolezza di un asset o di un controllo di sicurezza che può essere sfruttata da una o più minacce.

Con le formule 4.1.5 e 4.1.6 è possibile utilizzare il loro inverso, ossia i controlli di sicurezza (la cui mancanza costituisce una vulnerabilità).

In questa fase deve essere elaborata una lista di vulnerabilità o controlli di sicurezza, in modo da renderne sistematica l'identificazione e valutazione. Può essere utile partire dai controlli di sicurezza della ISO/IEC 27002 e in tabella 6.5.1 ne è riportato uno stralcio di esempio.

Controllo ISO/IEC 27001	Note
A.6.1 Profilo del personale (Screening)	<ul style="list-style-type: none"> - Presenza di curriculum e copie degli attestati pregressi. - Rispetto Statuto dei Lavoratori.
A.8.7 Protezione contro il malware	<ul style="list-style-type: none"> - Presenza di antivirus su tutti i PC desktop e su tutti i server. - Presenza antivirus sul server e-mail e sul web proxy. - Aggiornamento automatico degli antivirus. - Autorizzazioni per disinstallare gli antivirus solo agli amministratori di sistema.
A.5.20 Sicurezza negli accordi con i fornitori	<ul style="list-style-type: none"> - Presenza delle clausole su: diritto di audit, requisiti tecnici, SLA, requisiti legali e loro aggiornamento, BCP e DR. - Accordi di riservatezza.

Tabella 6.5.1:

Esempio di lista di riscontro per i controlli di sicurezza

Questa fase non prevede l'individuazione delle vulnerabilità o dei controlli di sicurezza esistenti, ma solo la preparazione della lista di riscontro. Per proseguire, infatti, bisogna prima individuare i controlli ideali sulla base del livello di rischio e poi stabilire quanto sono adeguati e conformi quelli attuati. Queste attività saranno trattate nel paragrafo 7.5.

6.6

Correlare le vulnerabilità agli asset

Le vulnerabilità da analizzare sono comuni agli asset della medesima categoria.

Solitamente è necessario identificare le vulnerabilità o i controlli associati alle medesime categorie elencate nel paragrafo 6.3.

Si può quindi sviluppare una tabella come la 6.6.1, dove sono elencati solo 3 dei 114 controlli della ISO/IEC 27001:2013, gli stessi asset utilizzati per l'esempio 6.3.2 e gli stessi controlli presentati in tabella 6.5.1.

	Server	Archivii	PC fissi	Fornitori	Sedie e Locali	Organizzazioni
A.6.1 Profilo del personale (Screening)						X
A.8.7 Protezione contro il malware	X		X			
A.5.20 Sicurezza negli accordi con i fornitori				X		

Tabella 6.6.1:

Esempio di relazione asset - controlli (vulnerabilità)

6.7 Correlare le vulnerabilità e i controlli alle minacce

Ulteriore correlazione riguarda le minacce e le vulnerabilità.

In tabella 6.7.1 è riportato un estratto di esempio, sulla base di quanto indicato nell'esempio 6.3.2 e nella tabella 6.5.1.

	Controlli di sicurezza		
Rischio	A.6.1 Profilo del personale (Screening)	A.8.7 Protezione contro il malware	A.5.20 Sicurezza negli accordi con i fornitori
Mitraglio			
Malware		X	
Accesso non autorizzato ai sistemi IT	X	X	
Lettura e copia non autorizzate di documenti digitali	X	X	X
Danneggiamento di apparecchiature fisiche			X
Invio di dati a persone non autorizzate	X		X

Tabella 6.7.1:

Esempio di relazioni tra minacce e controlli di sicurezza

Per ogni minaccia sono associati più controlli tra loro alternativi, compensativi, complementari o correlati. Inoltre questi controlli possono essere di diversa natura: prevenzione, recupero o rilevazione. Queste differenze sono illustrate nei due paragrafi successivi.

Quando si associano i controlli alle minacce bisogna, per quanto possibile, accertarsi che:

ogni minaccia sia contrastata da un insieme di controlli di prevenzione, recupero e rilevazione tra loro complementari;

per ogni controllo siano inclusi tutti quelli a esso correlati.

6.7.1 Controlli alternativi, compensativi, complementari e correlati

I controlli di sicurezza possono essere tra loro alternativi. Per esempio, per impedire l'accesso a un edificio alle persone non autorizzate si possono prevedere porte in legno o porte in acciaio. Non è infatti utile utilizzare in alcuni punti delle porte di legno e in altri delle porte in acciaio: la robustezza complessiva del controllo sarebbe equivalente alla robustezza del più debole (secondo il principio per cui una catena è robusta quanto il suo anello più debole o, in inglese, “no security solution is ultimately stronger than its weakest link”).

Meccanismi tra loro alternativi possono avere livelli di robustezza (o efficacia) diversi: è indubbio che l'accesso controllato da porta in acciaio è più robusto rispetto a quello controllato da porta in legno.

Controlli di minore efficacia utilizzati in sostituzione e in alternativa a quelli ideali sono detti controlli compensativi.

Esempio 6.7.1. Il controllo degli accessi effettuato attraverso telecamere è un controllo compensativo di un controllo effettuato tramite bussole azionate da lettore badge.

Esso è di minore efficacia perché non previene l'intrusione: al limite scoraggia malintenzionati poco motivati e permette di ricostruire a posteriori cosa è successo per ripristinare la situazione originaria.

Bussole e telecamere non sono controlli tra loro alternativi perché potrebbero essere utilizzati insieme, come si vedrà nel seguito.

Controlli diversi possono essere tra loro complementari (o, in termini elettrici, in serie) quando non sono tra loro alternativi, anche se potrebbero esserlo, e possono essere usati insieme per fornire un più elevato livello di sicurezza (difesa in profondità o defense in depth).

Esempio 6.7.2. Porte, allarmi perimetrali, allarmi interni e videocamere sono controlli tra loro complementari e non alternativi. Ciascuno di essi

migliora il livello di sicurezza fisica.

Altri esempi di controlli informatici complementari: più firewall per diverse zone della rete, antivirus sui server e sui client, richiesta di un’ulteriore password per alcune operazioni critiche.

Altri controlli possono essere tra loro correlati se non efficaci quando usati singolarmente.

Esempio 6.7.3. Controlli di sicurezza tra loro correlati sono:

porta per impedire l’accesso agli intrusi;

meccanismo per identificare le persone autorizzate ad accedere dalla porta (alcune alternative: vigilanza, lettore di badge, lettore di caratteristiche biometriche, tastierino per codice);

processo per assegnare e togliere le autorizzazioni.

Alcuni dei controlli di identificazione possono essere usati insieme e quindi sono complementari: in molti prevedono la presenza della vigilanza, a scopo di supervisione, insieme a dei meccanismi automatici.

È possibile utilizzare un ulteriore meccanismo complementare per evitare l’abuso del meccanismo di ingresso, come un blocco della porta per evitare l’accesso di più persone contemporaneamente.

6.7.2 Controlli di prevenzione, recupero e rilevazione

I controlli di sicurezza possono anche essere suddivisi nelle seguenti categorie:

prevenzione: permettono di prevenire un attacco o il suo successo (per esempio, il divieto di fumare nella sala server per il rischio di incendio o un antivirus per il rischio di malware);

recupero: permettono di ricostruire la situazione precedente l'attacco e ridurne le conseguenze (un esempio molto comune di questo controllo è il backup dei dati, utile sia in caso di incendio sia in caso di malware); alcuni testi li indicano come controlli di protezione o di mitigazione, ma questi termini possono generare confusione;

rilevazione: permettono di registrare quanto avviene ed eventualmente lanciare allarmi (per esempio il rilevatore fumi nella sala server per gli incendi e un IDS per il malware); essi svolgono anche funzioni di prevenzione, perché scoraggiano alcuni agenti, e di recupero, perché consentono di ricostruire la situazione precedente l'attacco.

6.8 Conclusione

Al termine delle attività riportate in questo capitolo si ha:

una descrizione degli asset;

un elenco di categorie di asset;

- un elenco di minacce, con i parametri RID a esse pertinenti;
- un elenco di controlli di sicurezza (o di vulnerabilità);
- una tabella di relazione tra categorie di asset e minacce;
- una tabella di relazione tra categorie di asset controlli di sicurezza (o di vulnerabilità);
- una tabella di relazione tra minacce e controlli di sicurezza (o di vulnerabilità).

Sono diffusi su Internet elenchi di minacce e di controlli di sicurezza, nonché tabelle di relazione tra minacce e controlli. Questi elenchi e queste tabelle possono essere usati per una prima valutazione del rischio e successivamente affinati per renderli più aderenti alle caratteristiche dell'ambito.

Note

²⁴http://www.theregister.co.uk/2007/05/04/txj_nonfeasance/

²⁵Uno degli esempi più recenti è il caso Snowden:
espresso.repubblica.it/googlenews/2013/06/25/news/caso-snowden-cosa-c-e-in-gioco-1.55992; uno dei canali di pubblicazione è WikiLeaks, all'indirizzo <http://wikileaks.org>.

Capitolo 7

Analisi del rischio

Ero... rimasto senza benzina.

Avevo una gomma a terra.

Non avevo i soldi per prendere il taxi.

La tintoria non mi aveva portato il tight.

C'era il funerale di mia madre!

Era crollata la casa!

C'è stato un terremoto!

Una tremenda inondazione!

Le cavallette!

Non è stata colpa mia!

Dal film Blues brothers

Iniziamo dalla definizione della ISO/IEC 27000.

Analisi del rischio: processo di comprensione della natura del rischio e di determinazione del livello di rischio.

Si tratta, in altre parole, di un’attività di stima del rischio senza alcun tipo di giudizio.

Il prossimo capitolo tratta della ponderazione del rischio e si può proporre un’analogia con gli esami medici: il tecnico di laboratorio identifica e raccoglie i campioni pertinenti ed effettua le analisi (oggetto di questo capitolo), mentre il medico pondera i risultati per stabilire se i valori determinati dalle analisi sono accettabili o non accettabili.

Per determinare il livello di rischio, come specificato dalle formule del paragrafo 4.1.2, bisogna assegnare valori agli asset, alle minacce e alle vulnerabilità (o ai controlli di sicurezza). Tali valori devono essere il più possibile oggettivi e ripetibili.

Per garantire una maggiore oggettività dei risultati occorre fornire linee guida per l’attribuzione dei valori. Vedremo dei semplici esempi nel seguito.

Per garantire la ripetibilità dei risultati, ossia la capacità di ottenere risultati uguali se le analisi sono effettuate nel medesimo contesto, una buona tecnica consiste nel giustificare per iscritto le motivazioni dei valori assegnati; così si migliora anche l’oggettività dell’analisi perché la necessità di documentare le proprie scelte rende più prudenti.

Documentare le scelte permette di effettuare affinamenti futuri: nelle successive analisi sarà possibile basarsi sulle considerazioni precedenti e concentrarsi sui cambiamenti intervenuti nel contesto e su quanto non emerso in precedenza.

L’assegnazione dei valori è indicata dalle espressioni di valutazione degli asset,

delle minacce e delle vulnerabilità, dall’inglese evaluation (tradotto spesso con ponderazione). È necessario distinguere questi termini da quelli derivati dall’inglese assessment, anch’essi tradotti con il termine valutazione come nella valutazione del rischio (risk assessment): l’evaluation è una componente dell’assessment, come sintetizzato dalla figura 4.0.1.

7.1 Metodi di analisi

I valori dipendono dalla scelta del metodo di calcolo. Vi sono due famiglie di metodi alle quali sono dedicati i paragrafi successivi: quantitativi e qualitativi.

7.1.1 Metodi quantitativi

Per i metodi quantitativi si utilizza la formula 4.1.6:

$$r(m, a, c) \propto p(m, c) \cdot i(m, a, c) \quad (4.1.6)$$

Sono utilizzate la probabilità statistica o la frequenza delle minacce per $p(m,c)$ e la valutazione economica dei danni per $i(m,a,c)$.

I metodi quantitativi sono molto apprezzati nella teoria perché ritenuti precisi e oggettivi. Nella pratica, quando si parla di sicurezza delle informazioni, non si hanno dati statistici affidabili sulle minacce e sugli attacchi e quindi questi metodi non garantiscono la precisione desiderata.

A questo bisogna aggiungere che l'analisi del rischio serve per fare ipotesi sul futuro, necessariamente soggettive e per le quali non possono esistere dati precisi. In altre parole, si può solo identificare il rischio percepito e mai quello reale. È pertanto importante prestare attenzione al falso senso di oggettività delle metodologie quantitative: la mancanza di dati precisi e affidabili potrebbe far ritenere validi dati ottimistici e creare di conseguenza un falso senso di sicurezza.

Esempio 7.1.1. Dal 2009 alcune compagnie petrolifere furono spiate da concorrenti di origine asiatica con strumenti installati nella loro rete informatica e scoperti solo nel 2011.

Non si sa né se le compagnie avessero effettuato delle valutazioni del rischio relativo alla sicurezza delle informazioni, né se utilizzassero metodologie quantitative o qualitative. È però certo che un attacco di questo genere, secondo i dati statistici disponibili all'epoca, era da considerare improbabile²⁶.

Analisi precise richiedono tempo e spese ingenti, spesso superiori ai benefici

ottenuti (tranne nei casi in cui certe società di consulenza possono aumentare i ricavi grazie ai lunghi tempi di analisi, o certi manager possono consapevolmente ritardare il momento in cui prendere delle decisioni).

Nell’ambito della continuità operativa (paragrafo 12.14), analisi quantitative possono essere condotte con risultati più soddisfacenti perché vi è maggiore disponibilità di dati storici degli eventi relativi all’interruzione delle attività (terremoti, blackout, eccetera).

Ulteriori considerazioni sui dati statistici sono nel paragrafo 7.3.

Le analisi quantitative hanno il pregio di fornire parametri economici facilmente interpretabili dalla Direzione quando deve decidere il budget economico per l’attuazione delle misure di sicurezza.

7.1.2 Metodi qualitativi

I metodi qualitativi utilizzano delle scale di valori quali “Alto”, “Medio” e “Basso” con la formula 4.1.4:

$$r(m, a, v) \propto p(m) \cdot i(m, a) \cdot g(v) \quad (4.1.4)$$

Queste analisi possono sembrare meno rigorose di quelle quantitative, finché non si riconosce che anche i valori attribuiti attraverso analisi quantitative sono soggettivi.

Infine esistono metodologie che dichiarano di essere semi-quantitative. In realtà si tratta di metodologie qualitative che utilizzano valori quantitativi come linea guida per l'assegnazione dei valori (per esempio, per il valore "Alto" è fornito il criterio "L'asset ha valore compreso tra €80 e €100"). Questo approccio presenta gli stessi problemi delle metodologie quantitative: indisponibilità di dati affidabili e falsa presunzione di oggettività.

Esempio 7.1.2. Un esempio di approccio semi-quantitativo fa uso di scale "logaritmiche" per le conseguenze (in termini economici, 1 è 1.000 Euro, 2 è 10.000 Euro, 3 è 100.000 Euro, 4 è 1.000.000 Euro, 5 è 10.000.000 Euro) e per la probabilità (1 è una volta in 10 anni, 2 è una volta all'anno, 3 è una volta al mese, 4 è una volta alla settimana, 5 è quotidiano).

7.2 Il valore degli asset

La ISO/IEC 27001 richiede di valutare le conseguenze dei rischi che si dovessero concretizzare. La valutazione delle conseguenze è equiparata alla valutazione delle conseguenze $i(m,a)$ di ciascuna minaccia m su ogni asset a .

Come metodo pratico è utile determinare inizialmente il valore dell'asset $i(a)$ in termini di riservatezza, integrità e disponibilità (parametri RID):

$i(a) = (iris(a), iint(a), idis(a))$ (7.2.1)

In questo paragrafo, si descrive prima come valutare le informazioni e poi gli asset utilizzati per trattarle o conservarle.

7.2.1 Valutare le informazioni

Le informazioni e gli altri asset sono già stati identificati come riportato nel paragrafo 6.1. Il passo successivo è quindi quello di assegnare un valore a i(a), dove a è un asset informazione.

L'approccio più rigoroso per valutare le informazioni consiste nell'assegnare loro tre valori: uno per la riservatezza, uno per l'integrità e uno per la disponibilità.

Per questo bisogna considerare i danni per l'organizzazione in termini di:

perdita di vantaggio competitivo, se un concorrente può disporre delle informazioni che hanno perso riservatezza;

perdita di ricavi a causa dell'indisponibilità delle informazioni o della loro inesattezza;

perdita di immagine a seguito di divulgazione di informazioni riservate, uso o alterazione delle informazioni per commettere frodi, pubblicazione di informazioni non accurate, indisponibilità delle informazioni e dei servizi informatici con impatto sui servizi offerti ai clienti;

sanzioni determinate dai contratti o dalla normativa vigente; per esempio, la perdita di riservatezza potrebbe essere valutata rispetto alla normativa privacy; la

perdita di disponibilità può essere sanzionata dai contratti con i clienti a causa dell'interruzione dell'attività;

impatti sul personale, conseguenti a perdita di fiducia nell'organizzazione per incidenti relativi alla sicurezza delle informazioni;

errori decisionali in caso di dati non integri (incompleti o inesatti);

costi per ripristinare l'integrità o la disponibilità delle informazioni;

costi legali per far fronte a cause intentate da clienti, partner o altre parti interessate.

In termini economici, i costi per il ripristino e le sanzioni sono detti costi diretti, quelli dovuti ai mancati ricavi sono detti costi indiretti e gli altri costi consequenziali. Nella maggior parte dei casi, i costi consequenziali, che comprendono quelli derivati dai danni di immagine, sono quelli più elevati, soprattutto nel medio-lungo periodo.

Come già indicato in precedenza, per garantire l'oggettività e la ripetibilità dell'analisi, bisogna accompagnare la valutazione con note per indicare le ragioni per cui è stato assegnato un valore.

7.2.1.1 Metodi quantitativi

I metodi quantitativi richiedono di valutare il potenziale danno economico dovuto alla perdita di riservatezza, integrità e disponibilità delle informazioni.

Esempio 7.2.1. Alle informazioni dei clienti dell'azienda casearia sono

attribuiti i seguenti valori:

riservatezza: la perdita di riservatezza delle informazioni potrebbe aiutare la concorrenza e comportare una perdita d'immagine presso i clienti; questo avrebbe però effetti trascurabili, considerando il settore di riferimento;

integrità: la ricostruzione delle informazioni alterate o perse può richiedere il lavoro di una persona per un totale di 5 giorni solari; considerando il costo di ciascun dipendente, tale attività è quantificata in €2.500;

disponibilità: l'indisponibilità delle informazioni dei clienti ha come effetto l'impossibilità di accettare gli ordini ed effettuare le spedizioni. Si stabilisce che l'indisponibilità massima è di una settimana, corrispondente al tempo necessario a ripristinare tutte le informazioni eventualmente corrotte, e questo comporterebbe una perdita del 2% del fatturato annuo, ossia €200 mila.

Alle informazioni dei fornitori sono attribuiti i seguenti valori:

riservatezza: la perdita di riservatezza delle informazioni non ha effetti significativi sull'impresa;

integrità: la ricostruzione delle informazioni alterate richiederebbe lo stesso impegno calcolato per quelle dei clienti, ossia €2.500;

disponibilità: l'indisponibilità delle informazioni dei fornitori avrebbe il medesimo effetto di quelle dei clienti perché impedirebbe la consegna delle materie prime; questo si traduce in una perdita di €200 mila.

Il valore delle informazioni è sintetizzato in tabella 7.2.1.

Informazioni	Riservatezza	Integrità	Disponibilità
Clienti	€ 0	€ 2.500	€ 200 mila
Fornitori	€ 0	€ 2.500	€ 200 mila

Tabella 7.2.1:

Esempio di valutazione quantitativa delle informazioni

La stima economica dei danni potenziali, però, è incerta: i danni maggiori sono spesso dovuti al valore di beni intangibili (le informazioni e l'immagine dell'organizzazione), per i quali non sono disponibili metodi di valutazione quantitativi affidabili²⁷.

7.2.1.2 Metodi qualitativi

Per le analisi qualitative, è possibile assegnare un valore alle informazioni facendo riferimento a una scala come quella riportata in tabella 7.2.2.

Valore	Linea guida
3	Le conseguenze possono essere disastrose per la sostenibilità dell'organizzazione.
2	Le conseguenze possono essere considerevoli per l'organizzazione, ma non ne mettono a rischio la sostenibilità.
1	Le conseguenze non sono rilevanti per l'organizzazione.

Tabella 7.2.2:

Esempio di linee guida per valori RID

Alcuni adottano scale diverse: da 1 a 7 o da 0 a 10. Nelle grandi realtà si ha la necessità di avere scale più ampie, mentre nelle piccole realtà è preferibile usare pochi valori (3 o 4).

Esempio 7.2.2. Trasformando l'esempio precedente utilizzando parametri qualitativi, si ottengono i valori riportati in tabella 7.2.3.

Si osservi che, in questo caso, è stato dato un valore “Medio” alla riservatezza delle informazioni relative ai clienti, superiore a quello assegnato ai fornitori, malgrado fosse stato dato loro lo stesso valore economico con il metodo quantitativo. Infatti la perdita di riservatezza delle informazioni dei clienti potrebbe creare maggiori danni di immagine.

Informazioni	Riservatezza	Integrità	Disponibilità
Clienti	2	2	3
Fornitori	1	2	3

Tabella 7.2.3:

Esempio di valutazione qualitativa delle informazioni

7.2.2 Il rischio privacy

Per valutare il rischio relativo alla privacy è necessario considerare le conseguenze per:

l'organizzazione, come visto negli esempi precedenti;

gli interessati.

Per i metodi qualitativi è possibile prevedere una scala di valori come in tabella 7.2.4.

Valore	Linea guida
3	Le conseguenze per gli interessati sono non reversibili sulla loro vita e possono includere: perdita di autonomia, esclusione (p.e. inabilità a lavorare), perdita di libertà, danni fisici (p.e. danni fisici o mentali a lungo termine o morte), danni alla proprietà, stigmatizzazione e perdita

del posto di lavoro, squilibrio di potere, perdita di fiducia e peggioramento della salute, perdita economica.

2

Le conseguenze per gli interessati sono rappresentate da piccole difficoltà (p.e. costi, mancato accesso a servizi, incomprensioni, stress, malanni minori, perdita di autonomia) a causa degli effetti sulla loro vita sociale o personale.

1

Le conseguenze per gli interessati sono lievi (p.e. fastidio e tempo necessario per correggere le informazioni).

Tabella 7.2.4:

Esempio di linee guida per le conseguenze sugli interessati

È quindi necessario, per il rischio relativo alla privacy, considerare il valore maggiore tra quello per l'organizzazione e quello per gli interessati.

7.2.3 Chi assegna i valori alle informazioni

Ciascun referente delle informazioni dovrebbe valutare quelle create e usate dalla propria area. Se un'informazione è utilizzata da più aree, allora si dovrebbe seguire il principio del caso peggiore: il valore dell'informazione corrisponde a quello più elevato tra quelli assegnati.

In molti casi può essere utile un incontro congiunto tra un facilitatore e tutte le parti interessate: referenti per le informazioni, utenti, tecnici informatici, analisti e sviluppatori dei programmi informatici, altri manager. In questo modo le valutazioni di ciascuno contribuiscono a ottenere un risultato coerente con la percezione di tutti.

Dopo aver raccolto tutte le valutazioni è necessario renderle tra loro coerenti. Bisogna infatti prestare attenzione a due atteggiamenti opposti: da una parte vi è chi, pur di attirare l'attenzione sulle proprie attività, fornisce valori molto alti; dall'altra chi, per paura di dover attuare misure di sicurezza molto rigorose, fornisce valori eccessivamente bassi.

Come già discusso in precedenza, l'invio di un questionario ai rappresentanti delle diverse aree può essere utile in organizzazioni di grandi dimensioni, ma è sempre preferibile un incontro con dei facilitatori.

7.2.4 Valutare gli altri asset

Per gli altri asset è necessario valutare gli archivi fisici e i sistemi informatici perché è su di essi che dovranno essere attuate le misure di sicurezza. Il valore $i(a)$ di questi asset è anch'esso composto da tre valori, corrispondenti ai tre parametri RID, dipendenti dai valori delle informazioni coinvolte.

7.2.4.1 Metodi quantitativi

Per le analisi quantitative, il valore dell'asset è determinato dalla somma dei valori delle informazioni trattate o conservate.

Esempio 7.2.3. Il CRM dell'azienda casearia, come visto nell'esempio 6.1.6 e in tabella 6.1.1, è utilizzato per trattare le informazioni dei clienti e dei fornitori. Se si indica con a e si utilizzano i valori assegnati alle informazioni nell'esempio 7.2.1, ha valore calcolato come in tabella 7.2.5.

Quindi $i(a)$ ha valore:

$$i(a) = (\text{ris}(a), \text{int}(a), \text{dis}(a)) = (\text{€ } 0, \text{€ } 5.000, \text{€ } 400.000). \quad (7.2.2)$$

Informazioni	Riservatezza	Integrità	Disponibilità
Clienti	€ 0	€ 2.500	€ 200 mila
Fornitori	€ 0	€ 2.500	€ 200 mila
CRM (Somma)	€ 0	€ 5 mila	€ 400 mila

Tabella 7.2.5:

Esempio di valutazione quantitativa di un asset

Alcuni aggiungono un ulteriore parametro relativo al costo materiale dell'asset (per esempio, del server o dell'archivio). Questo aspetto non è pertinente la sicurezza delle informazioni e quindi omesso.

7.2.4.2 Metodi qualitativi

Se si usano metodologie qualitative, il valore dell'asset è determinato dal massimo del valore delle informazioni da esso trattate o conservate.

Esempio 7.2.4. Dall'esempio 7.2.2, il CRM ha un valore calcolato come riportato in tabella 7.2.6.

Informazioni	Riservatezza	Integrità	Disponibilità
Clienti	2	2	3
Fornitori	1	2	3
CRM (Max)	2	2	3

Tabella 7.2.6:

Esempio di valutazione qualitativa di un asset

Alcuni usano la media, ma questo metodo è sconsigliabile: se in un archivio sono conservate informazioni estremamente critiche insieme a informazioni poco importanti, il valore medio potrebbe non evidenziare le prime.

D'altra parte, bisogna prestare attenzione quando si aggregano gli asset, per evitare che il risultato finale dia sempre valori massimi.

7.2.4.3 Ulteriori considerazioni

Il risultato, sia che si adottino metodologie quantitative che qualitative, potrebbe essere riesaminato e modificato considerando gli effetti delle interdipendenze:

distribuzione: i valori di uno o più parametri dell'asset possono essere diminuiti se l'asset è marginale rispetto ad altri asset (per esempio, la disponibilità di un sistema clone di un altro può essere inferiore a quella inizialmente calcolata, mentre rimarrà invariata per il sistema primario);

dipendenza: i valori di uno o più parametri dell'asset possono essere aumentati se l'asset è fondamentale per altri asset (per esempio, se un sistema di registrazione degli ordini necessita di un sistema di contabilità per funzionare, allora il sistema di contabilità deve avere un valore di disponibilità uguale o superiore a quello del sistema di registrazione degli ordini);

cumulo: i valori di uno o più parametri dell'asset possono essere aumentati se

l'asset è correlato a tante informazioni, anche se ciascuna di esse ha minore importanza (per esempio, se l'unico server è utilizzato per immagazzinare informazioni di scarsa criticità, esso ha valore elevato in quanto unico).

Esempio 7.2.5. Nel calcolo quantitativo del valore del CRM, la perdita di disponibilità delle informazioni dei clienti e dei fornitori avrebbe come effetto l'interruzione delle attività per una settimana. Quindi, applicando l'effetto di distribuzione, la disponibilità del CRM dovrebbe avere valore pari a €200 mila e non €400 mila.

7.2.5 Valutare gli asset IoT e industriali

I dispositivi IoT e industriali (detti anche OT o di operational technology) non trattano propriamente informazioni, con l'eccezione delle ricette che, per alcuni prodotti, hanno un elevato valore di riservatezza. Il loro valore, perciò, è solitamente determinato dalle conseguenze dovute alla loro indisponibilità o a malfunzionamenti (danni fisici alle persone, produzioni non conformi o inefficienti, inquinamento ambientale) e non alla perdita di riservatezza, integrità e disponibilità delle informazioni da essi trattate.

Alcuni, in questi casi, provano a considerare come informazioni le configurazioni dei dispositivi e quindi ne valutano l'integrità e disponibilità come parametri significativi. Può essere invece più opportuno considerare le peculiari caratteristiche dei sistemi OT e svolgere una valutazione del rischio distinta da quella relativa ai sistemi IT (ossia che trattano informazioni), anche usando diverse linee guida per l'attribuzione dei valori.

7.3 Valutare la verosimiglianza delle minacce

Questa attività consiste nell’attribuire un valore a $p(m)$ nella formula 4.1.4, stabilendo se un certo evento negativo m può avvenire e con quale probabilità (non necessariamente matematica).

7.3.1 Quali valori assegnare alle minacce

La verosimiglianza di una minaccia può essere espressa con valori quantitativi o qualitativi, a seconda del metodo scelto.

7.3.1.1 Metodi quantitativi

Le metodologie quantitative assegnano a ogni minaccia una determinata probabilità matematica o frequenza statistica. Per esempio, sono utilizzate tabelle per cui, in certe condizioni, la probabilità annua del furto può essere del 10% oppure del 50% e la frequenza corrispondente pari a 0,1 o 0,5 all’anno (in Italia, se calcoliamo i 4 terremoti di alto impatto negli anni 2000-2010, potremmo dire che hanno una frequenza pari a 0,4 all’anno).

Per dare maggiore senso di oggettività, si fa riferimento a statistiche (o survey) pubblicate da diversi enti, ma queste non sono affidabili a causa di molti fattori: chi riceve attacchi non li denuncia, il calcolo delle conseguenze è sempre molto approssimativo e gli accorpamenti con cui sono presentati i risultati non sono facilmente utilizzabili [47, 112]. Alcune delle pubblicazioni più interessanti degli ultimi anni [17, 131] non presentano più statistiche, ma solo un elenco ragionato degli eventi degli ultimi 6 o 12 mesi. ENISA²⁸ e lo svizzero NCSC²⁹ pubblicano alcune tra le migliori pubblicazioni di questo tipo.

Sono presenti nel mondo centri nazionali per la rilevazione degli incidenti informatici (anche italiano³⁰ ed europei³¹), ma non mettono a disposizione statistiche significative, per lo meno sui siti pubblici. Negli ultimi anni la situazione sta cambiando.

Neanche le assicurazioni dispongono di sufficienti dati attuariali perché il loro mercato sui rischi di sicurezza delle informazioni è talmente poco sviluppato ed eterogeneo da non consentirne l'elaborazione [43, 159].

Sono disponibili alcuni dati abbastanza accurati per minacce di tipo fisico: eventi naturali o dolosi quali terremoti, incendi e furti. Questo perché di dominio pubblico o ben monitorati dal mercato delle assicurazioni.

Per valutare le minacce da agenti malintenzionati, bisogna riflettere sulle capacità tecniche, le risorse disponibili, le opportunità e le motivazioni di coloro che potrebbero attaccare l'organizzazione.

L'analisi delle minacce deve tener conto di eventi non registrati o non rilevati e di eventi non ancora accaduti ma probabili. In tutti i casi, quindi, le valutazioni non possono essere né esatte né oggettive. Anche per questo si sconsiglia l'adozione di metodologie quantitative.

Esempio 7.3.1. Continuando l'esempio 7.2.3, si consideri la minaccia m di guasto hardware: la sua frequenza (detta mean time between failures o MTBF), analizzando quanto dichiarato dal produttore, è di una volta ogni due anni. Calcolando la probabilità su base annua:

$$p(m) = 0,5 \cdot (7.3.1)$$

7.3.1.2 Metodi qualitativi

I metodi qualitativi adottano delle scale da 1 a 3 come quella riportata in tabella 7.3.1.

Valore	Linea guida
3	La minaccia ha probabilità di verificarsi superiore a quelle normalmente riportate dalle ricerche più note.
2	La minaccia è mediamente probabile, in linea con le ricerche più note.
1	La minaccia è estremamente improbabile, al di sotto delle ricerche più note.

Tabella 7.3.1:

Esempio di linee guida per la valutazione delle minacce

Altre metodologie propongono diverse scale di valori, per esempio su 4 livelli (basso, medio-basso, medio-alto, alto) o su 10. Spesso si preferiscono scale con un numero pari di valori (contrariamente agli esempi qui presentati), in modo da evitare che vengano scelti i valori medi.

La linea guida in tabella 7.3.1 suggerisce di consultare delle ricerche: nonostante i limiti illustrati nel paragrafo precedente, sono importanti perché forniscono indicazioni sulle tendenze in corso e sulle minacce da analizzare.

Esempio 7.3.2. L'hardware utilizzato non presenta caratteristiche tali da prevedere guasti più o meno frequenti della media³², pertanto alla minaccia di guasto hardware si assegna un valore “medio”:

$$p(m) = 2. (7.3.2)$$

7.3.1.3 Ulteriori considerazioni

Come già detto nel caso delle valutazioni degli asset, è necessario annotare le ragioni per cui è stato assegnato un certo valore quantitativo o qualitativo a una minaccia. Queste note dovrebbero riportare le ricerche consultate, gli eventi registrati dall’organizzazione attraverso il processo di gestione degli incidenti (paragrafo 12.13), i casi noti accaduti in contesti geografici o di mercato simili.

Rimangono ancora aperti due argomenti molto teorici, ma molto importanti: come considerare le misure di sicurezza già presenti e il valore delle informazioni quando si valutano le minacce.

La risposta più rigorosa prevede di ricordare che la funzione $p(m)$ dell’equazione 4.1.4 non dipende né dalle misure di sicurezza c né dal valore degli asset a .

Quando si chiede alle persone di valutare la minaccia “virus”, la risposta più comune è: “Abbiamo già l’antivirus, quindi la probabilità è molto bassa”. Questo ragionamento è scorretto perché il valore da ricercare non riguarda la possibilità di essere attaccati con successo (e quindi dalla presenza di misure di sicurezza), ma di essere attaccati indipendentemente dal successo o meno dell’attacco.

Per la connessione tra verosimiglianza di una minaccia e valore delle informazioni è opportuno considerare l’appetibilità di queste ultime, visto che incide sulle motivazioni dei malintenzionati. Questa relazione, se considerata, deve essere annotata.

7.3.2 Chi assegna i valori alle minacce

Le stime dovrebbero essere fatte dalle stesse persone coinvolte nell’identificazione delle minacce (paragrafo 6.2.4):

- i referenti per le informazioni;
- i responsabili dei sistemi informatici;
- i responsabili della sicurezza fisica;
- i responsabili della gestione del personale, per riferire di eventuali casi di provvedimenti disciplinari collegati alla sicurezza delle informazioni;
- l’ufficio legale, per riferire di eventuali casi di reclami o segnalazioni da parte di clienti;
- i responsabili dell’ufficio acquisti, per riferire di eventuali casi che hanno coinvolto i fornitori.

Alcuni coinvolgono, per questa attività, solo pochi tecnici: il loro contributo è fondamentale, ma è comunque necessario che gli altri responsabili dell’organizzazione siano consapevoli dei rischi analizzati.

Come già segnalato in 6.1.3 e in altre parti, l’invio di un questionario ai rappresentanti delle diverse aree può essere utile in organizzazioni di grandi dimensioni, ma è sempre preferibile un incontro con dei facilitatori.

7.4 Il rischio intrinseco

La combinazione tra il valore degli asset e la probabilità di accadimento di una minaccia, senza considerare le vulnerabilità o i controlli di sicurezza attuati, prende il nome di rischio intrinseco o rischio puro.

In altre parole, dalla formula 4.1.4 per il calcolo del rischio, si ricava, togliendo $g(v)$, quella per il calcolo del rischio intrinseco r_i :

$$r_i(m, a) \propto p(m) \cdot i(m, a). (7.4.1)$$

7.4.1 Rischio intrinseco quantitativo

Per le metodologie quantitative è sufficiente osservare su quale parametro RID ha impatto la minaccia e moltiplicarne la frequenza per il valore pertinente di riservatezza, integrità e disponibilità dell'asset. Se una minaccia ha impatto su più parametri, i risultati vanno sommati.

In termini matematici, se:

$p(m)$ è la probabilità della minaccia;

$ris(m)$, $int(m)$ e $dis(m)$ sono pari a 1 se la minaccia ha impatto sui parametri di riservatezza, integrità e disponibilità e 0 in caso contrario;

$ris(a)$, $int(a)$ e $dis(a)$ sono i valori di riservatezza, integrità e disponibilità dell'asset e quindi $i(a) = (ris(a), int(a), dis(a))$,

allora la formula per calcolare il rischio intrinseco della minaccia m sull'asset a è la seguente:

$$ri(m, a) = p(m) \cdot ris(m) \cdot ris(a) + p(m) \cdot int(m) \cdot int(a) + p(m) \cdot dis(m) \cdot dis(a) \sum =$$

In questo modo, si ottiene la perdita economica media annua dovuta a una determinata minaccia sull'asset.

Esempio 7.4.1. Proseguendo l'esempio del CRM, dall'esempio 7.3.1, si ricorda che la minaccia m di guasto hardware ha:

$$p(m) = 0,5. \quad (7.4.3)$$

Questa minaccia ha impatti sull'integrità e disponibilità delle informazioni e pertanto:

$$(\text{ris}(m), \text{int}(m), \text{dis}(m)) = (0, 1, 1). (7.4.4)$$

Utilizzando i valori dell'asset riportati nell'esempio (tabella 7.2.5), è possibile calcolare il rischio intrinseco:

$$ri(m,a) = \sum p(m) \cdot z(m) \cdot z(a) \text{ per } z=\text{ris,int,dis} = p(m) \cdot \text{ris}(m) \cdot \text{ris}(a) + p(m) \cdot \text{int}$$

Ovviamente il risultato potrebbe essere riesaminato e modificato se consideriamo l'effetto di distribuzione, dipendenza o di cumulo, per cui il rischio complessivo è inferiore o maggiore rispetto alla somma dei rischi relativi ai singoli parametri (paragrafo 7.2.4.3).

Esempio 7.4.2. Un esempio molto noto di metodologia quantitativa, qui riportato per completezza, prende il nome di ALE e adotta la seguente terminologia:

la frequenza annua di una minaccia m è detta annual risk occurrence ed è indicata con $ARO(m)$;

la perdita economica media sull'asset a dovuta a ogni occorrenza della medesima minaccia m è detta single loss expectance ed è indicata con $SLE(m,a)$.

La perdita annua prevista dovuta alla minaccia m sull'asset a è detta annual loss expectance, indicata con $ALE(m,a)$ ed è il risultato della seguente equazione:

$$ALE(m, a) = ARO(m) \cdot SLE(m, a) \quad (7.4.6)$$

Il metodo ALE è sconsigliato per valutare il rischio di sicurezza delle informazioni perché non esplicita gli impatti su riservatezza, integrità e disponibilità delle informazioni. È più opportuno utilizzarne delle varianti, come nell'esempio precedente.

7.4.2 Rischio intrinseco qualitativo

Per le metodologie qualitative, la formula è la stessa delle metodologie quantitative ma con valori qualitativi e il massimo:

$$ri(m, a) = \max p(m) \cdot z(m) \cdot z(a) \text{ per } z=\text{ris,int,dis.} \quad (7.4.7)$$

Esempio 7.4.3. Proseguendo l'esempio del CRM, dall'esempio 7.3.2 si ricorda che la minaccia di guasto hardware ha:

$$p(m) = 2 \cdot (7.4.8)$$

Questa minaccia, ugualmente a quanto stabilito nell'esempio 7.4.1, ha i seguenti parametri:

$$(\text{ris}(m), \text{int}(m), \text{dis}(m)) = (0, 1, 1). (7.4.9)$$

Il CRM, dall'esempio 7.2.4, ha valore:

$$i(a) = (ris(a), int(a), dis(a)) = (2, 2, 3).(7.4.10)$$

Per il rischio intrinseco si ottiene quindi:

$$ri(m, a) = \max (2 \cdot 0 \cdot 2, 2 \cdot 1 \cdot 2, 2 \cdot 1 \cdot 3) = \max (0, 4, 6) = 6. \quad (7.4.11)$$

Altre metodologie qualitative propongono l'assegnazione del livello di rischio intrinseco rispetto a tabelle di normalizzazione per riportare i valori del rischio a una scala predefinita. Un semplice esempio nella figura 7.4.1.

Consecuencia /a/

	Alto	Medio	Alto	Alto
Medio	Basso	Medio	Alto	Alto
Basso	Basso	Basso	Medio	

Basso Medio Alto

Consecuencia /a/

Figura 7.4.1:

Tabella per il calcolo del rischio intrinseco qualitativo

Esempio 7.4.4. Dall'esempio precedente, si hanno i seguenti valori:

$$\begin{aligned} p(m) &= \text{medio}, \\ (\text{ris}(m), \text{int}(m), \text{dis}(m)) &= (0, 1, 1), \\ i(a) &= (\text{medio}, \text{medio}, \text{alto}). \end{aligned}$$

Per il rischio intrinseco, si ottiene quindi:

$$ri(m, a) = \max(0, \text{medio}, \text{alto}) = \text{alto.} (7.4.12)$$

Con questo calcolo, si possono creare grafici intuitivi, come quello in figura 7.4.2, con un esempio relativo a 5 minacce. Il valore i(a) deve corrispondere al massimo dei valori assegnati ai RID dell'asset su cui ha impatto la minaccia.

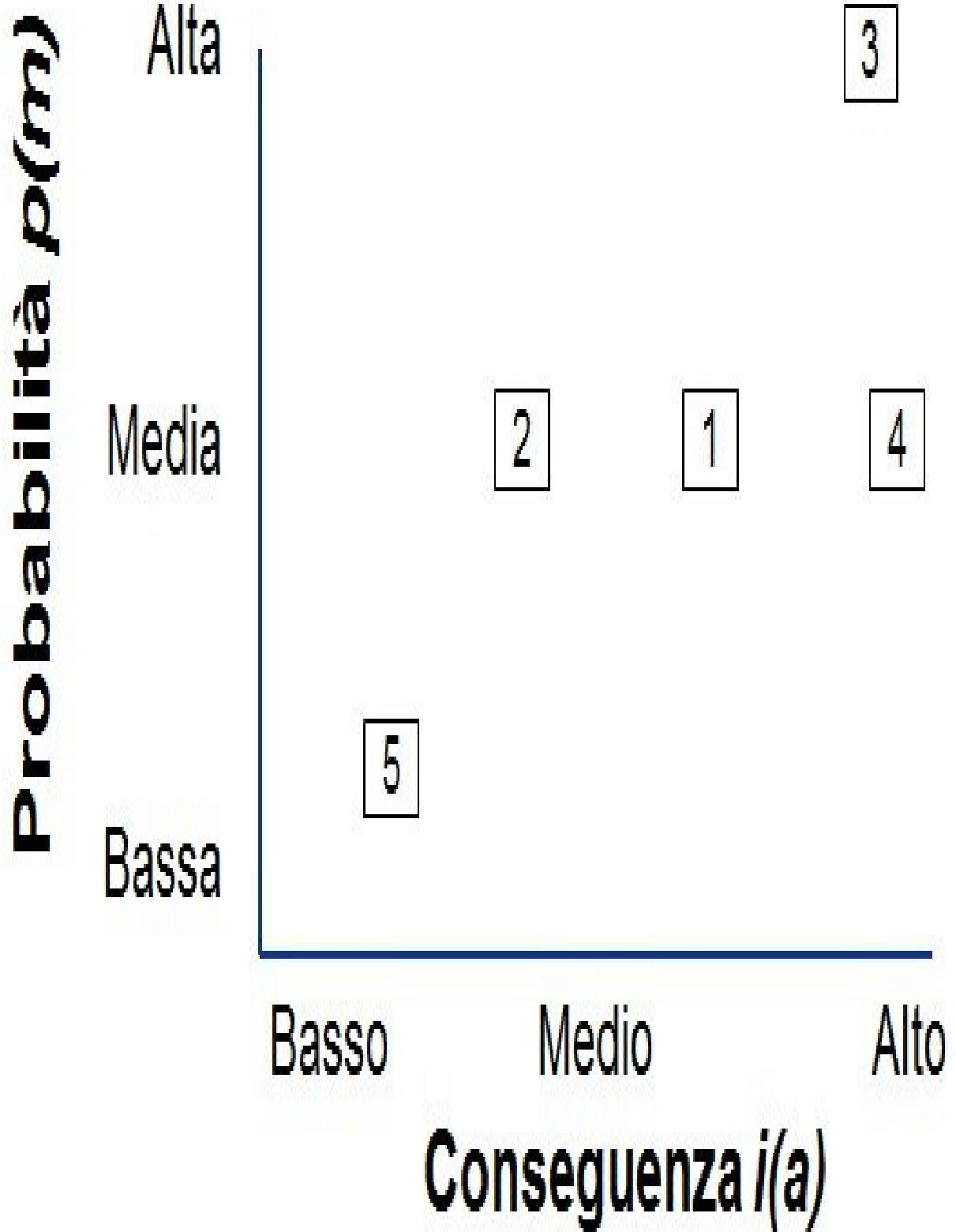


Figura 7.4.2:

Grafico per il rischio intrinseco qualitativo

Esempio 7.4.5. Dall'esempio precedente, il rischio della minaccia m di guasto hardware per l'asset a dovrebbe essere posto nella casella 4, dove $p(m)$ è medio e $i(a)$ è alto.

Il medesimo grafico può essere creato quando si utilizzano metodi quantitativi.

Anche in questi casi il valore deve essere riesaminato ed eventualmente modificato per gli effetti di distribuzione, dipendenza e cumulo.

7.5 Valutare le vulnerabilità e i controlli

Valutare le vulnerabilità è un esercizio non facile: bisogna prima individuare i controlli ideali sulla base del livello di rischio intrinseco e poi valutare quanto si discostano da quelli attualmente attivi nell'ambito.

Si ricorda che già in fase di identificazione del rischio, come illustrato nel paragrafo 6.7, venivano associati alle minacce i controlli di sicurezza descritti in termini molto generici.

A ciascuna minaccia si è ora associato un rischio intrinseco e quindi è possibile determinare i dettagli di come questi controlli devono essere realizzati in modo proporzionale a esso.

Si ricorda che un rischio può essere controllato con misure preventive, di recupero e di rilevazione tra loro complementari. È possibile stabilire quale delle opzioni deve essere preponderante facendo uso dello schema proposto in figura 7.5.1.

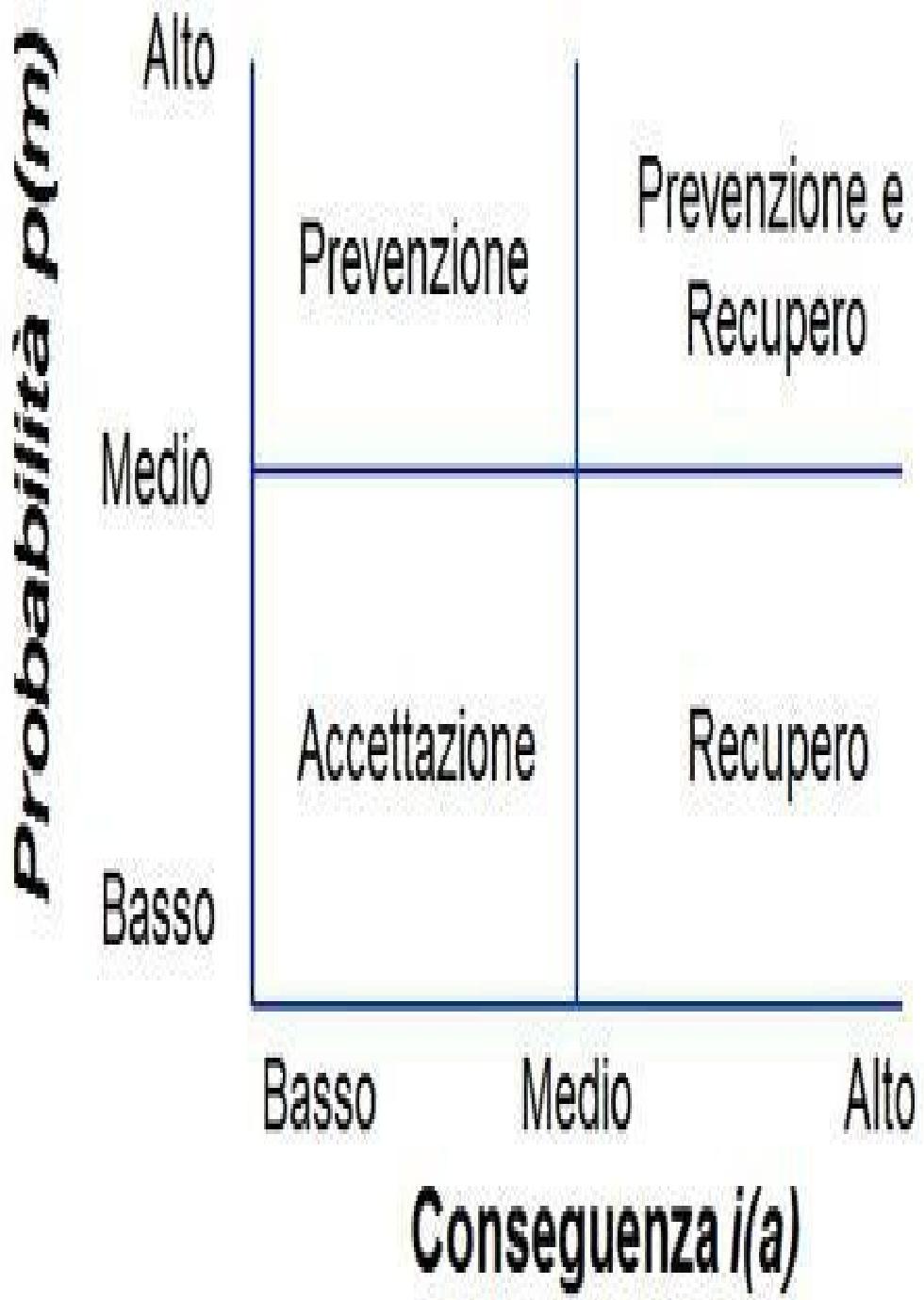


Figura 7.5.1:

Opzioni di trattamento

Esempio 7.5.1. Dall'esempio dell'azienda casearia, per contrastare la minaccia di guasto hardware si era valutato il backup, controllo di recupero certamente indicato se le conseguenze del guasto sono alte e la probabilità di accadimento media o bassa.

Nel caso di probabilità di accadimento alta, si sarebbero potute analizzare ulteriori misure di prevenzione: manutenzione più frequente, scelta di componenti hardware più resistenti, eccetera.

I controlli di recupero, come il backup, per loro natura, non hanno impatti sulla verosimiglianza, così come quelli di prevenzione, come i firewall, non riducono le conseguenze di un attacco. Va però detto che non sempre la distinzione è così netta, soprattutto per i controlli di tipo più organizzativo, come per esempio la formazione del personale.

Nei prossimi paragrafi si descrivono i controlli ideali e successivamente come valutarli.

7.5.1 Identificare i controlli ideali

I controlli possono essere ideali per l'ambito in cui si effettua la valutazione del rischio o in assoluto.

7.5.1.1 I controlli ideali per l'ambito

La prima alternativa consiste nello stabilire, dopo aver valutato le informazioni e le minacce, quali sono i controlli di sicurezza ideali da attuare, tali che siano proporzionali al rischio intrinseco specifico per l'ambito in cui si valuta il rischio.

Esempio 7.5.2. Si considerino due contesti distinti e le corrispondenti misure ideali per proteggere i progetti strategici su supporto cartaceo rispetto alla minaccia di furto. Si supponga che le informazioni abbiano valore alto e la minaccia abbia valore alto e, quindi, il rischio intrinseco sia alto.

Organizzazioni diverse possono stabilire controlli ideali diversi:

in una media azienda di produzione si prevede l'uso di una cassaforte presso l'ufficio del responsabile della progettazione;

la Coca Cola conserva la formula della famosa bevanda in una cassaforte presso una banca (e la fa visitare ai turisti)³³.

7.5.1.2 I controlli ideali assoluti

La seconda alternativa consiste nello stabilire a priori quali controlli di sicurezza prevedere per i diversi livelli di rischio intrinseco, indipendentemente dalla realtà osservata, e poi verificare se le misure previste sono attuate, parzialmente attuate o non attuate.

Esempio 7.5.3. Per contrastare il rischio di furto di informazioni in formato cartaceo, si possono stabilire le seguenti misure ideali, dipendenti dal livello di rischio intrinseco:

rischio intrinseco “alto”: conservare le informazioni in una cassaforte;

rischio intrinseco “medio”: conservare le informazioni in un armadio con chiave;

rischio intrinseco “basso”: nessuna misura specifica.

Questo è il metodo utilizzato dai programmi informatici per la valutazione del rischio perché un pacchetto software immesso in commercio deve già proporre delle misure di riferimento.

La controindicazione di questo approccio è che, nella maggior parte dei casi, le soluzioni proposte non sono adeguate al contesto in cui si svolge l’analisi. Infatti una banca adotta misure diverse da una piccola società di sviluppo software: la differenza di scala rende inapplicabili le scelte fatte per l’altra e così una proposta unica per tutti non può essere realistica.

L’uso di un programma commerciale per effettuare la valutazione del rischio può

essere sicuramente d'aiuto, ma, prima di adottarlo, occorre valutare su quali riferimenti è impostato (paragrafo 4.3.1).

7.5.2 Quali valori assegnare ai controlli

I controlli attuati per ciascun asset devono essere confrontati con quelli ideali, in modo da attribuire un valore rispetto all'adeguatezza e conformità, discusse nel paragrafo successivo.

Nel seguito sono indicate le modalità di attribuzione dei valori quando si adottano metodi quantitativi o qualitativi.

7.5.2.1 Adeguatezza e non conformità

Quando un controllo non è progettato come quello ideale, si dice che non è adeguato o sufficiente.

Esempio 7.5.4. Si supponga che il controllo ideale per la conservazione dei documenti di progettazione preveda l'utilizzo di una cassaforte.

Se questa scelta non è contemplata dalle procedure o politiche dell'organizzazione e non si dispone di cassaforte, il controllo attuato è inadeguato.

Non bisogna dimenticare, quando si valuta l’adeguatezza di un controllo, di valutare anche quelli a esso correlati e indispensabili per il suo buon funzionamento. Per esempio, non è sufficiente verificare la presenza della cassaforte, ma anche di procedure relative alla gestione delle sue chiavi, alla scelta delle persone a conoscenza della combinazione e alla modifica della combinazione.

Quando un controllo di sicurezza è adeguato ma non è attuato correttamente e come previsto, si dice che è non conforme o non corretto.

Esempio 7.5.5. Proseguendo dall’esempio precedente, si supponga che l’uso della cassaforte sia contemplato dalle procedure, ma il personale la lascia sempre aperta.

Il controllo è quindi attuato in modo non conforme.

In tutti e due i casi, si può parlare di inefficacia: inefficacia di progettazione o inefficacia di attuazione.

In organizzazioni molto complesse, inizialmente è opportuno valutare il rischio solo relativamente all’adeguatezza dei controlli: la dimensione dell’organizzazione non permetterebbe di valutarne completamente la conformità.

Nel seguito si potranno identificare delle non conformità tramite gli audit interni

(descritti nel paragrafo 15.9.2) e il processo di rilevazione degli incidenti e delle vulnerabilità (descritto nel paragrafo 12.13). La priorità di trattamento di queste non conformità potrà essere stabilita grazie alla valutazione del rischio associato a esse.

Una nota terminologica: i termini efficacia, adeguatezza e conformità sono utilizzati prevalentemente dalla ISO/IEC 27001, mentre i termini sufficienza e correttezza sono utilizzati prevalentemente dalla ISO/IEC 15408.

7.5.2.2 Metodi quantitativi

Le metodologie di tipo quantitativo prevedono di calcolare di quanto ridurre la probabilità della minaccia p o le conseguenze i grazie alla presenza dei controlli di sicurezza. In questo caso, si fa uso della formula 4.1.6, qui ricordata:

$$r(m, a, c) \propto p(m, c) \cdot i(m, a, c). \quad (4.1.6)$$

Esempio 7.5.6. Si continui l'esempio del CRM, per cui la minaccia di guasto hardware m ha probabilità 0,5 e l'asset ha valore:

$$i(a) = (\€ 0, \€ 5.000, \€ 400.000) \quad (7.5.1)$$

Si può considerare il controllo di sicurezza c relativo al sistema di backup, attualmente non disponibile. Esso avrebbe i seguenti effetti sui parametri dell'equazione 4.1.6:

probabilità: il sistema di backup è un controllo di recupero e pertanto non ha impatti sulla verosimiglianza della minaccia e quindi:

$$p(m, c) = p(m) = 0,5; (7.5.2)$$

riservatezza: il sistema di backup non ha alcun effetto sulla salvaguardia della riservatezza delle informazioni, pertanto abbiamo:

$$\text{ris}(a, c) = r(a) = \epsilon 0; (7.5.3)$$

integrità: il sistema di backup consentirebbe di avere i dati corretti e coerenti come erano, al massimo, 24 ore prima del guasto; questo permetterebbe di ridurre il tempo necessario alla ricostruzione dei dati al massimo di una giornata di lavoro, ossia un decimo di quanto inizialmente calcolato (cinque giornate per i dati dei clienti e cinque per quelli dei fornitori), pertanto abbiamo:

$$\text{int(a, c)} = € 500; (7.5.4)$$

disponibilità: la riduzione del disagio a una giornata rispetto a una settimana ridurrebbe a un quinto i ritardi di ricezione degli ordini e di consegna dei prodotti ed è quindi possibile stimare:

$$\text{dis(a, c)} = € 80.000. (7.5.5)$$

7.5.2.3 Metodi qualitativi

Le metodologie qualitative fanno riferimento alla formula 4.1.4 qui ricordata:

$$r(m, a, v) \propto p(m) \cdot i(m, a) \cdot g(v). (4.1.4)$$

È possibile assegnare un valore a $g(v)$ secondo una scala di valori basata sull'adeguatezza e conformità dei controlli, di cui è presentato un esempio in tabella 7.5.1. Questa andrebbe ampliata con esempi, in modo che persone poco esperte possano utilizzarla facilmente.

$g(v)$	Linea guida
3	<p>Controlli di sicurezza inadeguati o non attuati (ossia completamente non conformi), se non sporadicamente; oppure</p> <p>Rilevate gravi vulnerabilità.</p>
2	<p>Controlli di sicurezza non completamente adeguati oppure attuati ma non in modo sistematico o con delle non conformità; oppure</p> <p>Rilevate lievi vulnerabilità.</p>
1	<p>Controlli di sicurezza adeguati ed attuati in modo sistematico e conforme; oppure</p> <p>Non rilevate vulnerabilità.</p>

Tabella 7.5.1:

Esempio di linee guida per valutare i controlli e le vulnerabilità

Esempio 7.5.7. Nell'esempio precedente si era visto che il controllo di sicurezza relativo al sistema di backup era assente e pertanto:

$$g(v) = 3.(7.5.6)$$

Se invece fosse stato presente ma non efficacemente attuato (per esempio, nessuno ha mai controllato se il backup è stato completato correttamente), si sarebbe potuto assegnare a $g(v)$ un valore pari a 2.

7.5.2.4 Ulteriori considerazioni

Nella realtà sono presenti delle complessità che vanno considerate. Esse possono riguardare: gli asset compositi, la difformità dei controlli previsti per asset simili e la presenza di controlli compensativi. A esse sono dedicati i paragrafi successivi.

Asset compositi

In molti casi è necessario valutare l'applicazione di uno stesso controllo per più componenti di ogni singolo asset. Si consideri ad esempio il controllo degli accessi; per un servizio informatico come un CRM, questo controllo dovrebbe essere analizzato in tutte le sue componenti: sistema operativo, database management system e applicazione.

Utilizzando una metodologia qualitativa si possono riportare le singole valutazioni componente per componente, come esemplificato in figura 7.5.2 (l'esempio presenta delle note più sintetiche di quelle consigliabili).

Controllo ISO/IEC 27001	Componente	g(v)	Note
A.5.15.1 Controllo degli accessi	Sist. operativo	2	<ul style="list-style-type: none"> Procedura adeguata perché richiede utenze personali e univoche per ciascun utente. Attuata parzialmente (ossia in modo non conforme) perché sono utilizzate utenze di amministrazione condivise.
	Database	1	<ul style="list-style-type: none"> Secondo procedura; solo utenze personali.
	Applicazione	2	<ul style="list-style-type: none"> La procedura non fa esplicito riferimento alle applicazioni, ma solo ai sistemi operativi e database (non adeguata). Nella pratica, sono utilizzate solo utenze personali.

Tabella 7.5.2:

Esempio di valutazione dei controlli per singole componenti

In alternativa si possono raggruppare le valutazioni, riportando come valore di $g(v)$ il maggiore assegnato alle singole componenti, come esemplificato in tabella 7.5.3. Questo secondo metodo, anche se apparentemente più complesso, permette di semplificare il calcolo del livello di rischio se si usano semplici fogli di calcolo.

Controllo ISO/IEC 27001	$g(v)$	Note
A.5.15.1 Controllo degli accessi	2	<p>Sistema operativo - $g(v) = 2$.</p> <ul style="list-style-type: none"> - Procedura adeguata perché richiede utenze personali e univoche per ciascun utente. - Attuata parzialmente (ossia in modo non conforme) perché sono utilizzate utenze di amministrazione condivise.
		<p>Database - $g(v) = 1$.</p> <ul style="list-style-type: none"> - Secondo procedura; solo utenze personali.
		<p>Applicazione - $g(v) = 2$.</p> <ul style="list-style-type: none"> - La procedura non fa esplicito riferimento alle applicazioni, ma solo ai sistemi operativi e DBMS (non adeguata). - Nella pratica, sono utilizzate solo utenze personali.

Tabella 7.5.3:

Esempio di valutazione dei controlli per insieme di componenti

Uniformità dei controlli

La valutazione delle vulnerabilità e dei controlli, anche in realtà di piccola dimensione, è un lavoro estremamente dispendioso perché richiede l'analisi di ogni singolo asset e delle sue componenti.

Quando si valuta l'adeguatezza di un controllo, però, il lavoro potrebbe essere più semplice quando si adottano le medesime politiche e procedure in tutta l'organizzazione e per ciascun tipo di asset.

Esempio 7.5.8. In molte organizzazioni, i sistemi Windows sono tutti gestiti nello stesso modo, e così i sistemi Linux, eccetera.

Se l'organizzazione ha più sedi, solitamente le procedure di manutenzione degli impianti e di controllo degli accessi sono le medesime.

Vi sono ovviamente numerose eccezioni. Per esempio, i controlli di sicurezza fisica tra il sito principale e le altre sedi di un'organizzazione sono spesso diversi.

Nel paragrafo 7.5.2.1 si era suggerito di iniziare a valutare il rischio solo relativamente all’adeguatezza dei controlli, soprattutto in organizzazioni molto complesse. La valutazione di adeguatezza dovrebbe essere basata anche sull’uniformità dei controlli: se, dove è possibile, i controlli sono attuati in modo non uniforme, allora si ha una vulnerabilità.

Controlli compensativi

Quando si valutano i controlli rispetto a quelli ideali bisogna prestare attenzione se, a fronte di inadeguatezze o non conformità, sono attuati controlli compensativi. Bisogna quindi verificare se e quanto il controllo compensativo garantisca un livello di sicurezza equivalente al controllo ideale.

Quando si utilizza un programma software commerciale per la valutazione del rischio può essere difficile o impossibile valutare i controlli compensativi, in quanto solitamente non previsti.

7.5.3 Chi assegna i valori ai controlli

I valori $p(m,c)$ e $i(m,a,c)$, per i metodi quantitativi, e $g(v)$ per quelli qualitativi, dovrebbero essere assegnati con il supporto di persone competenti nelle diverse tecnologie e coinvolgendo più persone, non necessariamente contemporaneamente: per valutare gli strumenti in uso al personale, è necessario coinvolgere gli utenti stessi; per valutare i processi e le soluzioni tecnologiche in ambito informatico è necessario coinvolgere gli amministratori di sistema; per valutare la sicurezza fisica è necessario coinvolgere il suo responsabile; e così via.

Alcuni raccolgono le informazioni sui controlli di sicurezza attraverso interviste ai manager di livello gerarchico elevato, però essi non sono sovente a conoscenza di molti dettagli operativi e alcuni hanno in mente dei processi non coincidenti con la realtà. Questa non è una critica ai manager, piuttosto una presa d'atto che il loro ruolo non prevede di conoscere tutti i dettagli relativi a vulnerabilità e controlli di sicurezza.

Esempio 7.5.9. In un'organizzazione si è potuto rilevare che gli addetti alla gestione della rete informatica, contrariamente a quanto supposto dal loro responsabile, utilizzavano connessioni insicure per gestire gli apparati di rete. È stato possibile individuare questa vulnerabilità solo attraverso l'osservazione diretta delle attività operative.

Dovrebbero essere intervistati gli operatori presso le proprie postazioni, in modo da poter analizzare direttamente gli strumenti in uso, i processi seguiti e i documenti pertinenti (per esempio gli schemi di rete).

Durante le interviste dirette si ha anche la possibilità di discutere di eventuali controlli di sicurezza ritenuti inefficaci o non conformi e dei possibili miglioramenti da introdurre. Quanto emerso sarà utile in fase di trattamento del rischio.

Esempio 7.5.10. Riprendendo l'esempio 7.5.9: dopo aver visto l'uso di connessioni insicure, una prima indagine ha evidenziato come fosse impossibile attivare i necessari meccanismi di sicurezza a causa dell'obsolescenza delle apparecchiature.

Quando si sono scelte le azioni per ridurre il rischio, erano già disponibili delle informazioni da cui partire e si stabilì di predisporre un piano di migrazione a una nuova tecnologia.

Altro effetto positivo della conduzione delle interviste con il personale operativo e presso le loro postazioni è che questa attività contribuisce all'aumento della loro consapevolezza sull'importanza della sicurezza delle informazioni, sul loro ruolo e sui controlli di sicurezza (paragrafo 12.4.3.3).

Un ulteriore metodo per assegnare i valori $p(m,c)$, $i(m,a,c)$ e $g(v)$ consiste nell'inviare dei questionari ai responsabili delle singole aree di riferimento affinché li compilino con le informazioni pertinenti. Dei problemi collegati a questo metodo si è già discusso in precedenza.

Nel caso di metodologie quantitative, il valore $i(m,a,c)$ dovrebbe essere riesaminato dai referenti per le informazioni coinvolte.

Al termine della valutazione delle vulnerabilità, è necessario riesaminare i risultati finali per renderli tra loro omogenei dove opportuno, visto che le valutazioni di ciascuno in merito allo stesso soggetto potrebbero essere diverse.

7.6 Il livello di rischio

Per calcolare il livello di rischio si possono utilizzare le medesime formule di calcolo del rischio intrinseco, aggiungendo il parametro di vulnerabilità.

Ulteriori considerazioni sono nei paragrafi successivi dedicati alle metodologie quantitative e qualitative.

Al termine dei calcoli, il livello di rischio deve essere riesaminato ed eventualmente modificato per gli effetti di distribuzione, dipendenza e cumulo.

7.6.1 Livello di rischio quantitativo

Per le metodologie quantitative, si parte dalla formula 7.4.2 già vista in precedenza per il rischio intrinseco, ossia:

$$ri(m, a) = \sum p(m) \cdot z(m) \cdot z(a) \text{ per } z=\text{ris,int,dis.} \quad (7.4.2)$$

Per il calcolo del livello di rischio, come visto nel paragrafo 7.5.2, si utilizzano i valori di probabilità e conseguenze modificati dai controlli di sicurezza. Si ottiene così la formula:

$$r(m, a, c) = \sum p(m, c) \cdot z(m) \cdot z(a, c) \text{ per } z = \text{ris, int, dis.} \quad (7.6.1)$$

Esempio 7.6.1. Dall'esempio 7.5.6 relativo alla valutazione delle vulnerabilità con metodi quantitativi, si erano individuati i seguenti valori relativi all'asset CRM, alla minaccia di guasto hardware e alla vulnerabilità di mancanza di backup:

$p(m,c) = 0,5;$
 $(ris(m),int(m),dis(m)) = (0, 1, 1);$
 $ris(a,c) = € 0;$
 $int(a,c) = € 500;$
 $dis(a,c) = € 80.000 .$

A questo punto è possibile calcolare il rischio:

$$r(m, a, c) = p(m, c) \cdot \text{ris}(m) \cdot \text{ris}(a, c) + p(m, c) \cdot \text{int}(m) \cdot \text{int}(a, c) + p(m, c) \cdot \text{dis}(m, a, c)$$

Questa equazione riguarda un singolo asset, una singola minaccia e i controlli di sicurezza a essa associati.

Molti vorrebbero sapere il rischio “complessivo” di un asset rispetto a tutte le minacce m_1, m_2, \dots e sommano i singoli rischi applicando la seguente formula:

$$r(a) = \sum p(m_j, c) \cdot z(m_j) \cdot z(a) \text{ per } z = \text{ris, int, dis} \text{ e per tutti i } j. \quad (7.6.3)$$

Tuttavia questa formula non è di aiuto perché impedisce di capire a quale minaccia è necessario prestare maggiore attenzione. È più utile conoscere il rischio relativo a ogni singola minaccia.

Altri calcolano il “rischio medio” rispetto alle minacce. In altre parole, dividono il rischio complessivo per il numero di minacce, in modo da sapere mediamente qual è il rischio di ciascuna minaccia:

$$r(a) = [\sum p(mj, c) \cdot z(mj) \cdot z(a)] / j \text{ per } z = \text{ris, int, dis.} \quad (7.6.4)$$

Questo metodo è sconsigliato, perché se si ha una minaccia collegata a un rischio elevato e tante minacce collegate a un rischio basso, la minaccia più elevata non viene evidenziata a causa della media.

Questo potrebbe essere chiamato problema delle code statistiche, per cui i casi estremi rischiano di essere ignorati. Nella sicurezza, invece, sono importanti proprio i casi estremi, perché evidenziano dove si corrono i rischi maggiori.

A questo punto, si potrebbe obiettare che a fronte di 10 asset e 30 minacce, si avrebbero 300 rischi da valutare e questo può essere troppo complesso. In realtà, con un semplice foglio di calcolo è possibile ordinare i rischi in modo da evidenziare solo quelli più elevati, sicuramente meno di 300.

7.6.2 Livello di rischio qualitativo

Per questo calcolo del livello di rischio, è sufficiente moltiplicare il valore del rischio intrinseco per il valore della vulnerabilità.

Esempio 7.6.2. Dagli esempi 7.4.3 e 7.5.7 relativi alla valutazione del rischio intrinseco e alla valutazione delle vulnerabilità con metodi qualitativi, si erano individuati i seguenti valori relativi all'asset CRM, alla minaccia di guasto hardware e alla vulnerabilità di mancanza di backup:

$p(m) = 2;$
 $(ris(m), int(m), dis(m)) = (0, 1, 1);$
 $ris(a) = 2;$

```
int ( a ) = 2;  
dis ( a ) = 3;  
g ( v ) = 3 .
```

A questo punto è possibile calcolare il rischio:

$$r(m, a, v) = \max[p(m) \cdot ris(m) \cdot ris(a), p(m) \cdot int(m) \cdot int(a), p(m) \cdot dis(m) \cdot dis(a)]$$

Come già accennato, qui sono state usate delle scale di tre valori per valutare i parametri RID, le minacce e le vulnerabilità, ma se ne possono utilizzare altre.

Come per le analisi quantitative anche qui c'è il problema dell'elevato numero di elementi. In questo caso, oltre ai 10 asset e alle 30 minacce, si dovranno aggiungere i controlli di sicurezza necessari per contrastare le minacce (nelle analisi quantitative, i controlli erano delle variabili per calcolare le conseguenze e la verosimiglianza delle minacce, non dei valori a sé stanti). Se mediamente si contano almeno 10 controlli per minaccia, si hanno la bellezza di 3.000 valori di rischio. Nella realtà il numero di controlli associati a una minaccia è superiore a 10 a causa di quelli complementari e correlati e quindi i valori saranno molti di più.

Anche in questo caso è sufficiente utilizzare la semplice funzione di ordinamento di un foglio di calcolo elettronico per evidenziare i rischi più elevati e quindi concentrarsi su di essi.

Si potrebbero modificare leggermente le argomentazioni sopra esposte distinguendo i controlli di tipo preventivo e quelli di recupero per utilizzare la formula 4.1.6, con i controlli c al posto delle vulnerabilità v, come per le analisi quantitative. Non si approfondisce ulteriormente questo metodo, ma è riportato uno schema in figura 7.6.1.

$p(m, c)$

	Basso	Basso	Medio
Alto	Basso	Medio	Alto
Medio	Basso	Medio	Alto
Basso	Medio	Alto	Alto
	Basso	Medio	Alto

Probabilità $p(m, c)$

Rischio

Alto	Medio	Alto	Alto
Medio	Basso	Medio	Alto
Basso	Basso	Basso	Medio

Probabilità $\alpha(m, c)$

Conseguenza $i(a, c)$

	Basso	Basso	Medio
Alto	Basso	Medio	Alto
Medio	Basso	Medio	Alto
Basso	Medio	Alto	Alto
	Basso	Medio	Alto

Conseguenza $i(a)$

Figura 7.6.1:

Schema per il calcolo del rischio qualitativo



Sulla base di questo metodo, riprendendo quanto già visto in figura 7.4.2, è possibile rappresentare graficamente il risultato come riportato in figura 7.6.2.



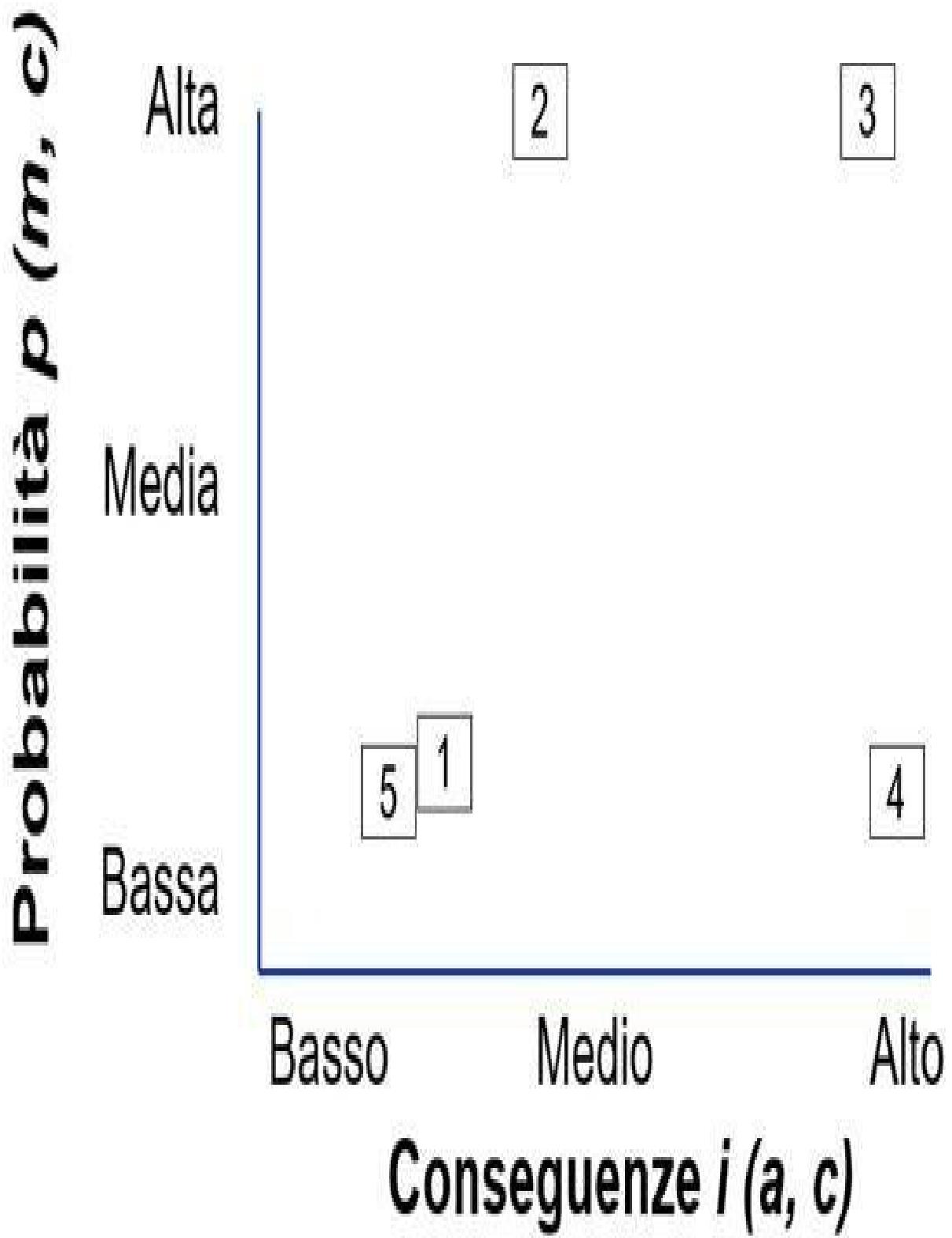


Figura 7.6.2:

Grafico del livello di rischio qualitativo



7.6.3 Conclusioni

Da quanto esposto, è facile vedere come il metodo quantitativo possa presentare in modo molto evidente i risultati. Anticipando quanto si vedrà in seguito, nell'esempio 7.6.1 si apprezza facilmente che la mancanza di un sistema di backup può costare all'organizzazione €202.500 all'anno, mentre la sua presenza porterebbe questo costo a €40.250 all'anno: se si comprasse un sistema di backup di circa €1.500, si ammortizzerebbe l'investimento in meno di un mese.

Purtroppo la raccolta dei dati necessari al metodo quantitativo è molto onerosa e non sempre questi dati sono affidabili.

Esempio 7.6.3. Per l'esempio del CRM dell'azienda casearia e la minaccia di guasto hardware, la valutazione delle conseguenze ha richiesto un calcolo della produttività giornaliera dell'organizzazione e la valutazione della verosimiglianza della minaccia ha richiesto la consultazione delle specifiche del produttore del server.

Il calcolo della mancata produttività, però, non tiene conto dell'impatto dell'accumulo dei ritardi su diverse lavorazioni.

Per minacce di tipo fisico e conseguenze strettamente collegate alla produttività non è difficile reperire dati utili, ma questo non è sempre possibile per altre situazioni. Per esempio: quale potrebbe essere la perdita economica per la mancanza di riservatezza dei dati dei clienti considerando gli impatti sulla competitività? Per la valutazione delle minacce, quale valore attribuire alla probabilità di un’intrusione informatica anche dopo aver attuato dei controlli preventivi?

Per contro, la metodologia qualitativa può apparire più grossolana, ma è molto più efficiente perché non richiede una minuziosa raccolta dati. Inoltre, la valutazione dei controlli di sicurezza, essendo indipendente dalla valutazione degli asset e delle minacce, può essere molto più veloce da realizzare.

L’analisi qualitativa del rischio permette, in tempi brevi, di individuare i rischi più elevati. Limitandosi a questi, è quindi opportuno effettuare delle indagini quantitative più approfondite, in modo da calcolare l’opportunità economica dell’attuazione dei controlli di sicurezza, ossia il ritorno dell’investimento sulla sicurezza delle informazioni (return on security investments, ROSI) [134].

7.7 Ulteriori riflessioni sulle aggregazioni

A questo punto è possibile fare un’ultima considerazione in merito alle aggregazioni necessarie per rendere più veloce, anche se non meno significativa, l’analisi del rischio.

La prima aggregazione riguarda gli asset e si è appena detto che a fronte di 10

asset si possono avere molti dati da analizzare. Nelle organizzazioni piccole o medie si può addirittura avere un unico asset inteso come l'organizzazione nel suo complesso.

Questo potrebbe apparire strano, ma si consideri quanto segue:

le minacce sono rivolte a tutta l'organizzazione, non a una parte di essa; certamente possono sfruttare dei singoli asset, ma le motivazioni dei malintenzionati, la possibilità di fare errori e gli eventi naturali sono comuni a tutta l'organizzazione e non specifici di un singolo asset;

i controlli di sicurezza, se presi dalla ISO/IEC 27001, sono già solitamente pertinenti a una singola categoria di asset; si osservi la tabella 6.6.1: ogni controllo è in relazione solo con un'unica categoria di asset (fa eccezione la protezione contro il malware, associata ai PC e ai server).

Sicuramente ci sono delle eccezioni a quanto detto e sono state segnalate in precedenza e le tabelle 7.5.2 e 7.5.3 lo dimostrano. Rappresentano però delle eccezioni se la lista di riscontro da preparare come indicato nel paragrafo 6.5 è fatta con cura.

Per le grandi organizzazioni, ovviamente, il discorso è diverso. Ma anche in questo caso si può ricorrere a degli accorgimenti, come iniziare dalla valutazione dell'adeguatezza dei controlli in generale e cercando di uniformarli in tutta l'organizzazione. Questa è infatti una strada che molte multinazionali hanno intrapreso o stanno percorrendo.

Note

²⁶<https://www.dailynews.com/2011/02/10/report-hackers-in-china-hit-western-oil-companies/>.

²⁷Per esempio, come valutare le conseguenze della diffusione del database di Babbo Natale? precision-blogging.blogspot.it/2009/12/another-leak-worst-so-far.html

²⁸<https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends>.

²⁹<https://www.ncsc.admin.ch/ncsc/it/home/dokumentation/berichte.html>.

³⁰<https://csirt.gov.it/>.

³¹cert.europa.eu

³²Anche se, in effetti, l'hardware di questo esempio è scadente, visto che 2 anni di MTBF sono pochi.

³³www.worldofcoca-cola.com/explore/explore-inside/explore-vault-secret-formula/.

Capitolo 8

Ponderazione del rischio

'cause nothing compares

nothing compares 2 U.

Prince, Nothing compares 2 U

Di seguito è riportata la definizione di ponderazione del rischio, come al solito dalla ISO/IEC 27000.

Ponderazione del rischio (risk evaluation): processo di comparazione dei risultati dell'analisi del rischio rispetto ai criteri di rischio per determinare se il rischio è accettabile o tollerabile.

È necessario fare ricorso a un'altra definizione dalla ISO/IEC 27000.

Criteri di rischio: valori di riferimento rispetto ai quali è ponderato il rischio.

La ponderazione del rischio, in altre parole, consiste nel giudicare se un rischio è accettabile o non accettabile rispetto a dei criteri prestabiliti.

Standard e metodologie, normalmente, richiedono sempre di individuare i criteri di rischio nella fase iniziale della valutazione del rischio.

Alcune organizzazioni si sforzano indicando: “Tutti i rischi con perdita economica annua maggiore di €100 non sono accettabili” per le analisi quantitative, oppure “Tutti i rischi di livello alto non sono accettabili” per quelle qualitative, oppure “Tutti i rischi nel quadrante in alto a destra non sono accettabili” per quelle qualitative con grafico come in figura 7.6.2. Prima di aver concluso la valutazione del rischio, però, non si hanno parametri di riferimento.

I criteri iniziali possono essere i seguenti:

il livello di sicurezza deve essere almeno quello richiesto dalle clausole contrattuali e dalla normativa vigente;

il rischio accettabile è quello che bilancia il rischio di impresa e la sua sostenibilità in termini economici; in altre parole, se un controllo di sicurezza “costa troppo”, vuol dire che la sua assenza è accettabile;

se per alcuni rischi sono attuati dei controlli compensativi efficaci, essi sono accettabili;

si deve dare priorità ai rischi più elevati;

si deve dare priorità alle minacce per le quali una singola occorrenza può avere conseguenze tali da compromettere la sostenibilità dell’organizzazione.

È quindi necessario ordinare i rischi dal più elevato al meno elevato e cominciare a ponderarli (ossia, giudicarli) uno a uno. I primi rischi potranno essere ritenuti inaccettabili, poi, a un certo punto della lista, ci saranno solo rischi accettabili.

Esempio 8.0.1. Facendo uso di una metodologia qualitativa è possibile associare a ciascun controllo di sicurezza un livello di rischio, qui calcolato come il massimo di tutti i rischi che contrasta.

$$rc = \max r(a, m, c) \text{ per tutte le minacce } m. \quad (8.0.1)$$

È possibile fare questo calcolo per un singolo asset o per un insieme di asset. Ordinando i controlli sulla base del livello di rischio a essi associati si ottiene un risultato come quello presentato in tabella 8.0.1.

Risulta evidente come il primo controllo da migliorare sia quello relativo ai backup.

	<h2>Controllo di sicurezza</h2>
18	<h3>8.13 Backup delle informazioni</h3>
9	<h3>5.14 Trasferimento delle informazioni</h3>
9	<h3>8.15 Logging</h3>
9	<h3>8.5 Autenticazione sicura</h3>
8	<h3>8.7 Protezione contro il malware</h3>
8	<h3>5.16 Gestione delle identità</h3>
8	<h3>5.17.1 Informazioni di autenticazione</h3>

Tabella 8.0.1:

Esempio ordinamento controlli ordinati per livello di rischio

Come già specificato in precedenza, il fatto di accettare un rischio o meno è una questione soggettiva e non è possibile renderla oggettiva (a dimostrazione di ciò, malgrado le statistiche negative, tanta gente continua a fumare e a guidare ubriaca).

In questa fase si effettua uno studio di fattibilità preliminare relativo ai possibili controlli di sicurezza da introdurre o alle modifiche a quelli esistenti, in modo da comprendere se avviare dei progetti di miglioramento. Lo studio di fattibilità andrà approfondito nel processo di trattamento del rischio.

Un ultimo appunto sulla terminologia. Qui si usa l'espressione "accettabilità del rischio" o "tollerabilità del rischio". In molti contesti è utilizzata l'espressione inglese "risk appetite" o una sua traduzione. Poiché questa espressione è orrenda, non è qui usata.

Capitolo 9

Trattamento del rischio

If there's anything that you want

If there's anything I can do

Just call on me and I'll send it along

With love, from me to you.

McCartney/Lennon, From me to you

Cominciamo, come sempre, dalla definizione ufficiale della ISO/IEC 27000 e dalle sue note, con alcune modifiche tra parentesi quadre per renderne più facile la lettura.

Trattamento del rischio: processo per modificare il rischio.

Nota 1: il trattamento può comportare: evitare il rischio decidendo di non iniziare o continuare un'attività; prendere o aumentare il rischio per cogliere un'opportunità; rimuovere la sorgente del rischio [ossia la minaccia]; modificare la probabilità [della minaccia]; modificare le conseguenze; condividere il rischio con altri soggetti (anche attraverso contratti e finanziamenti); mantenere il rischio con una scelta informata.

Nota 2: i trattamenti relativi a conseguenze negative sono spesso indicati con le espressioni “mitigazione del rischio”, “eliminazione del rischio”, “prevenzione del rischio” e “riduzione del rischio”.

Nota 3: il trattamento del rischio può creare nuovi rischi o modificare quelli esistenti.

Nel seguito si approfondiscono le diverse opzioni riportate nella nota 1, per poi introdurre il piano di trattamento del rischio e ulteriori considerazioni in merito.

Il rischio successivo al trattamento è detto rischio residuo.

9.1 Le opzioni di trattamento del rischio

Prima di elencare nel dettaglio le opzioni di trattamento del rischio, è bene fornire una prima conclusione: solitamente si sceglie di attuare o modificare dei controlli di sicurezza per prevenire il successo di una minaccia (paragrafo 9.1.3) o ridurne le conseguenze (paragrafo 9.1.4). Le altre opzioni richiederebbero di modificare processi o attività non strettamente legati alla sicurezza delle informazioni oppure di modificare il valore delle informazioni o delle minacce, che però sono intrinseci del contesto.

Esempio 9.1.1. Per ridurre il rischio relativo all’intrusione di un malintenzionato nei sistemi informatici, è irrealistico pensare di ridurre il valore della minaccia (bisognerebbe convincere i malintenzionati a non attaccare l’organizzazione!) oppure il valore delle informazioni potenzialmente compromesse.

Si possono invece migliorare i controlli di sicurezza e ridurre le vulnerabilità per ridurre la probabilità che l’attacco abbia successo o le sue conseguenze.

Questa conclusione evidenzia quanto sia importante l'identificazione e la valutazione delle vulnerabilità e dei controlli di sicurezza in fase di identificazione e analisi del rischio.

9.1.1 Evitare o eliminare il rischio

Come indicato nella nota alla definizione, un'organizzazione evita il rischio quando decide di non iniziare o di interrompere un'attività.

Questa scelta è di tipo strategico e legata al posizionamento sul mercato dell'organizzazione. Non di rado le cronache riportano grandi imprese che vendono propri rami d'azienda³⁴, a causa di minacce o opportunità di tipo strettamente economico o finanziario. Si tratta quindi di una scelta molto rara da vedere nella pratica se collegata alla sola sicurezza delle informazioni.

Esempio 9.1.2. Un'organizzazione non accetta il rischio connesso alle attività di e-commerce e quindi decide di chiudere questo servizio (oppure, se non ancora attivo, decide di non avviarlo).

Questa scelta, quando è fatta, si basa spesso su considerazioni in merito alle spese di realizzazione o mantenimento dell'attività. Tali spese includono quelle di attuazione o miglioramento dei controlli di sicurezza.

Esempio 9.1.3. Alcune organizzazioni evitano i rischi collegati all’uso di dispositivi portatili impedendone l’uso al proprio personale.

Quando si interrompe un’attività, non sempre si evitano tutti i rischi a essa correlati. Potrebbe essere infatti necessario conservare per un certo periodo di tempo delle informazioni.

Esempio 9.1.4. Un’azienda italiana ha deciso di chiudere il proprio sito di e-commerce per evitare il rischio che venga compromesso da malintenzionati.

Ciò nonostante dovrà conservare per 10 anni i dettagli delle transazioni effettuate con i clienti per rispettare la normativa in materia di contabilità. A queste informazioni dovrà essere assicurato un adeguato livello di sicurezza.

9.1.2 Aumentare il rischio

Questa opzione è l’inversa della precedente.

Esempio 9.1.5. Un’organizzazione accetta di aumentare il rischio connesso alle attività di e-commerce, attivando questo servizio.

Il rischio potrebbe essere aumentato inconsapevolmente e questo è molto pericoloso.

Esempio 9.1.6. I responsabili dell'organizzazione potrebbero:

invitare a non seguire tutte le procedure di sicurezza per rendere più veloci le attività;

decidere di utilizzare dei fornitori senza effettuare gli opportuni controlli preventivi.

Queste pratiche dovrebbero essere rilevate come non conformità. I responsabili avrebbero dovuto continuare a seguire le procedure e segnalarne l'inadeguatezza, in modo che questa fosse valutata rispetto al rischio.

Esempio 9.1.7. Equifax fu vittima di uno dei più importanti incidenti di sicurezza delle informazioni che sfruttò vulnerabilità di sistemi informatici non aggiornati.

La società aveva un gruppo dedicato all'aggiornamento dei sistemi informatici, ma lo considerava come di "B team". Equifax aveva anche coinvolto una società di consulenza specializzata in sicurezza, ma rifiutò i suoi consigli e assunse come responsabile della sicurezza una persona senza le necessarie competenze.

Tutte queste vulnerabilità furono sottovalutate e il rischio crebbe fino all'incidente di sicurezza del settembre 2017³⁵.

Al contrario, si può aumentare consapevolmente il rischio quando si modificano delle procedure, anche a fronte di controlli di sicurezza ritenuti eccessivamente onerosi.

Esempio 9.1.8. Tra i controlli di sicurezza eccessivamente onerosi, identificati in alcune organizzazioni, vi sono:

- il controllo della carta di identità all'ingresso anche per i visitatori già noti;
- la modifica delle password ogni 30 giorni (e non 90 o più);
- il controllo con telecamere in ogni locale;
- la duplicazione esatta e non parziale di tutti i sistemi informatici (incluso l'hardware) in un sito di disaster recovery;
- la richiesta di molteplici autorizzazioni per ogni operazione di cambiamento o configurazione dei sistemi informatici;
- la richiesta di firma autografa per autorizzazioni per le quali basterebbe una conferma via e-mail o altro sistema informatico.

Un controllo di sicurezza ritenuto eccessivamente oneroso dovrebbe essere identificato come vulnerabilità. Infatti nel medio periodo il personale smette di attuarlo come previsto (ingenerando, tra l'altro, un falso senso di sicurezza). Deve essere quindi stabilito se mantenerlo così com'è, eliminarlo o, infine,

modificarlo rendendolo meno robusto ma più efficiente.

9.1.3 Modificare la probabilità della minaccia (Prevenire)

Modificare la probabilità della minaccia, nel contesto del rischio relativo alla sicurezza delle informazioni, è quasi impossibile. Infatti, non possono essere eliminati i fenomeni naturali, né i malintenzionati, né le persone che fanno errori.

È più opportuno parlare di riduzione delle probabilità di riuscita di un attacco. Per esempio: è impossibile evitare i tentativi di intrusione alla propria rete informatica, ma se ne possono ridurre le probabilità di riuscita grazie a dei firewall.

Questa opzione prevede quindi di aggiungere o migliorare i controlli di prevenzione e di rilevazione già trattati nel paragrafo 6.5 e quindi di ridurre le vulnerabilità.

È impossibile eliminare completamente il rischio perché nessun controllo di sicurezza è inattaccabile: è sempre possibile individuare un metodo per aggirarlo o comprometterlo, soprattutto se attuato in modo non corretto. Un controllo è tanto più robusto quante più risorse e competenze richiede per aggirarlo o comprometterlo, non per l'impossibilità di farlo. Inoltre, come si vedrà nel paragrafo 9.3.1.4, l'adozione o la modifica di uno o più controlli di sicurezza possono introdurre nuovi rischi, da valutare bene.

9.1.4 Modificare le conseguenze (Recuperare)

Questa opzione è collegata ai controlli di recupero e, parzialmente, a quelli di rilevazione già trattati nel paragrafo 6.5.

Un esempio molto comune di questo tipo di controlli sono i backup: non prevengono alcuna minaccia, ma permettono di ripristinare i dati se questi dovessero essere danneggiati e quindi ridurre i danni.

Questa opzione non permette di eliminare completamente il rischio: un attacco riuscito, anche se i suoi effetti sono stati ridotti al minimo grazie a controlli di recupero, può sempre comportare un'interruzione, per quanto breve, delle attività o un loro rallentamento e un conseguente danno all'immagine.

Anche in questo caso, l'adozione o la modifica di uno o più controlli di sicurezza possono introdurre nuovi rischi, da valutare attentamente.

9.1.5 Condividere il rischio

Per questa opzione si usa anche l'espressione trasferire il rischio, meno precisa.

La condivisione del rischio si attua attraverso il ricorso a fornitori e a polizze assicurative.

Se un'attività è affidata a fornitori, questi devono predisporre delle misure per prevenire le minacce e recuperare eventuali danni. In questo modo, il cliente non deve preoccuparsi di certi rischi.

Se però un attacco ha successo, anche se è previsto che il fornitore paghi delle penali, il cliente può sperimentare interruzioni o rallentamenti delle attività, danni di immagine o altre conseguenze. Il cliente, quindi, non trasferisce tutti i rischi al fornitore, ma solo una parte di essi.

Un cliente deve prendere atto dei rischi non trasferibili ai fornitori e dei nuovi rischi introdotti dai fornitori stessi. Tra questi ultimi vi sono: perdita di competenze all'interno dell'organizzazione, possibilità che il fornitore fallisca e interrompa la fornitura, accesso di nuove persone alle informazioni dell'organizzazione.

L'assicurazione è un controllo (vedere paragrafo 12.12.6) che rappresenta un'altra forma di condivisione del rischio e permette di ridurre gli impatti economici conseguenti a un incidente di sicurezza delle informazioni. È quindi un controllo di recupero.

Neanche in questo caso un'assicurazione copre tutti i rischi relativi alla sicurezza delle informazioni poiché copre solo alcuni rischi di danneggiamento e di interruzione delle attività e non può eliminare i disagi e i danni all'immagine conseguenti a un incidente.

La sottoscrizione di una polizza introduce nuovi rischi, come lo scoprire troppo tardi che l'evento sperimentato non è contemplato dalla polizza sottoscritta, la compagnia di assicurazioni ha la cessato le attività o sono cambiati elementi di contesto per cui la polizza sottoscritta è meno efficace.

9.1.6 Mantenere il rischio (Accettare)

Quando si decide di non fare nulla, si mantiene il rischio (retain). Ulteriori espressioni utilizzate sono ritenere il rischio o accettare il rischio.

Si mantiene il rischio per diversi motivi:

il rischio è talmente basso per cui ogni azione di riduzione non darebbe benefici apprezzabili;

ci sono controlli compensativi tali da non ritenere necessaria alcuna azione (caso particolare del precedente, per cui ogni ulteriore azione di riduzione non darebbe benefici apprezzabili);

le scelte strategiche non permettono alcuna azione di riduzione;

il costo per nuovi controlli di sicurezza o per il miglioramento di quelli già esistenti sarebbe tanto elevato da non dare benefici apprezzabili;

l'aggiunta o modifica di controlli di sicurezza potrebbe introdurre ulteriori vulnerabilità o inefficienze ritenute inaccettabili.

L'importante, in tutti questi casi, è che tale scelta sia consapevole, in modo da monitorare nel tempo le vulnerabilità.

Esempio 9.1.9. I supermercati sono strutturati affinché i clienti si servano da soli, ma il rischio di furto è elevato; ciò nonostante non ci sono guardie in ogni corridoio, ma telecamere mobili: il rischio rimane elevato ma comunque monitorato.

9.2 Piano di trattamento del rischio

L'insieme di tutte le decisioni prese, rischio per rischio, prende il nome di piano di trattamento del rischio (risk treatment plan).

Il termine è lievemente ambiguo perché il piano di trattamento del rischio non comprende nessuna azione pianificata, ma solo un elenco di scelte fatte. Si sarebbe potuta usare l'espressione documento riportante le scelte di trattamento dei rischi, ma evidentemente sarebbe stata troppo lunga.

In questo piano, normalmente, la gran parte delle scelte sono di accettazione del rischio. Deve essere specificato se il rischio è mantenuto perché basso o per altri motivi.

Le opzioni di trattamento del rischio devono essere scelte dai responsabili dei rischi, eventualmente con l'aiuto di altre persone con competenze tecniche.

Il piano deve essere approvato dalla Direzione che fornisce le risorse per attuarlo e dimostra di essere consapevole dell'intero processo.

9.3 Scelta e attuazione delle azioni di riduzione

Prima di stabilire definitivamente se ridurre un rischio, è necessario sapere quali

azioni sarebbero necessarie.

Per ognuna di esse dovranno essere identificati i benefici attesi. Inoltre l'elenco delle azioni deve essere riesaminato per accertarsi che queste siano tra loro coerenti, fattibili e non introducano nuovi rischi inaccettabili. Infine, le azioni vanno pianificate in dettaglio e monitorate fino alla loro conclusione e alla valutazione della loro efficacia.

9.3.1 Riesaminare il piano delle azioni

Prima di approvare il piano delle azioni, vanno accertarti i loro benefici, la loro reciproca coerenza, la loro fattibilità e che non introducano nuovi rischi inaccettabili.

9.3.1.1 I benefici attesi (gli obiettivi)

Per valutare se un'azione possa portare a una riduzione del rischio, si può effettuare una what-if analysis, vale a dire la determinazione dei valori previsti per asset, minacce e vulnerabilità a seguito della conclusione dell'azione, in modo da calcolare il livello di rischio che si otterrebbe.

Esempio 9.3.1. Nell'esempio 7.4.1 sul rischio calcolato con metodi quantitativi, si era visto che, in assenza di un sistema di backup, il rischio relativo a un guasto hardware del server era di €202.500.

Nell'esempio 7.6.1 era stata fatta una what-if analysis, riportando il livello di rischio nel caso in cui fosse presente un sistema di backup. Tale livello di rischio era pari a €40.250 all'anno.

Il beneficio atteso da un sistema di backup è quindi pari a €162.250 annui. Si può dunque decidere di acquistarlo valutando il ritorno dell'investimento.

Esempio 9.3.2. Riprendendo l'esempio 7.6.2 sul rischio calcolato con metodi qualitativi, si era visto che il rischio relativo a un guasto hardware del server era pari a 18 in assenza di un sistema di backup.

In quel caso, la vulnerabilità aveva valore pari a 3. Se si introducesse un sistema di backup, una what-if analysis potrebbe portare la gravità della vulnerabilità a 1, che renderebbe il livello di rischio pari a 6.

Un'analisi economica non sempre conduce i responsabili del rischio a promuovere azioni di riduzione. Infatti molte resistenze sono dovute alla difficoltà di comprensione delle conseguenze su beni intangibili come le informazioni e alla paura del cambiamento. Non è compito di questo libro affrontare il change management organizzativo e quindi questo aspetto non è approfondito.

Gli obiettivi di rischio misurabili

Per quanto riguarda i benefici, è opportuno prestare attenzione al mito del miglioramento continuo e della necessità di perseguire degli obiettivi misurabili sempre più elevati. Questo non può applicarsi alla sicurezza delle informazioni in senso stretto.

Esempio 9.3.3. Nel caso di un’organizzazione commerciale, il livello di rischio di furto degli strumenti informatici fu inizialmente calcolato come alto. Si avviò un progetto di controllo degli accessi alla sede e di installazione degli allarmi perimetrali. La what-if-analysis riportava come obiettivo un livello di rischio basso.

Passato un anno, dopo aver terminato i lavori e in occasione della rivalutazione del rischio, il livello di rischio di furto degli strumenti informatici fu nuovamente calcolato come alto, contrariamente a quanto previsto l’anno precedente: si osservò infatti che molti addetti dell’organizzazione utilizzavano computer portatili e tablet, per i quali non erano state attuate opportune misure di sicurezza.

Secondo il mito del miglioramento continuo questo risultato sarebbe da ritenere inaccettabile. Alcuni, addirittura, falsificano i risultati dell’analisi del rischio per riportare solo miglioramenti. Questo è un atteggiamento ovviamente sbagliato perché l’accettazione inconsapevole dei rischi è molto pericolosa.

Al contrario, si dovrebbe valutare positivamente la corretta conclusione dell’azione stabilita l’anno precedente e l’aumento di consapevolezza dei responsabili dell’organizzazione che hanno evidenziato dei rischi inizialmente trascurati.

Ulteriori considerazioni sono nel paragrafo 15.6.5.

Il miglioramento continuo deve essere interpretato come una costante capacità di analisi del contesto, in modo da individuare i rischi e controllarli in modo che siano accettabili, e di completamento delle azioni pianificate.

9.3.1.2 Coerenza delle azioni

Le azioni sono tra loro incoerenti se introducono disomogeneità inutili. Per esempio, se in una sede è prevista una vigilanza armata, anche nelle altre sedi simili si dovrebbe prevedere la medesima misura.

Esempio 9.3.4. In un'organizzazione con due service desk dedicati a due clienti diversi furono attivate due azioni distinte per avere un sistema di registrazione e gestione delle chiamate degli utenti. Questo avrebbe generato un problema per il personale specialistico, addetto a entrambi i clienti, perché avrebbe dovuto usare due strumenti distinti per interfacciarsi con i due service desk.

Fortunatamente il caso fu individuato per tempo e i progetti furono fusi.

Esempio 9.3.5. In un'organizzazione, in un'area era consentito l'uso di dispositivi personali per accedere alla rete, in un'altra si era deciso di vietarlo completamente.

Il personale della seconda area, grazie agli strumenti messi a disposizione dalla prima, riusciva comunque a collegare i propri dispositivi alla rete.

Le azioni dovrebbero essere coerenti con quanto già presente nell’ambiente di riferimento. Per esempio, se è già in uso una certa tecnologia per la gestione dei backup di alcuni server, si potrebbe utilizzarla anche per i nuovi server senza acquisire nuove tecnologie; per le organizzazioni appartenenti a un gruppo, è opportuno, se possibile, che tutte utilizzino le stesse soluzioni tecnologiche.

9.3.1.3 Fattibilità delle azioni

Per la fattibilità, sono da valutare molti aspetti. Il primo è sicuramente economico ed è già stato discusso in precedenza.

Il secondo è tecnico: quando si introduce un nuovo controllo di sicurezza è necessario istruire convenientemente gli utenti e gli operatori sul suo corretto utilizzo e configurazione: l’uso scorretto o l’inadeguata configurazione di un meccanismo di sicurezza sono molto pericolosi perché, oltre a non migliorare il livello di sicurezza, potrebbero indurre un falso senso di sicurezza e quindi ridurne il livello. Sono molto diffuse le storie relative a meccanismi di sicurezza acquistati e mai installati o installati e mai tenuti aggiornati a causa della mancanza di competenza del personale.

9.3.1.4 Nuovi rischi introdotti dalle azioni

Ultimo punto da valutare sono i rischi che potrebbero essere introdotti dai nuovi controlli di sicurezza. Per esempio, le UPS possono esplodere; i programmi software di sicurezza informatica possono a loro volta essere difettosi e vulnerabili e potrebbero essere configurati in modo insicuro. Gli strumenti devono essere quindi preventivamente analizzati come ogni altro prodotto da introdurre nell'ambito di riferimento (paragrafo 12.11).

Esempio 9.3.6. CCleaner è un software molto noto che permette di eliminare file inutili da un computer e migliorarne le prestazioni.

La versione pubblicata nell'agosto 2017 conteneva del malware³⁶.

Potrebbero essere introdotti rischi dalla modifica dei processi e delle procedure. Il personale, una volta aggiornate le procedure, non modifica automaticamente il proprio comportamento, a causa delle abitudini acquisite: ogni cambiamento richiede tempo per essere recepito e attuato sistematicamente. Ciò dovrebbe essere noto grazie all'esperienza di ciascuno (per esempio, a molti è capitato di sbagliare strada perché diretti verso la propria precedente abitazione). In alcuni casi il personale deve essere formato e affiancato fino a quando il cambiamento sia correttamente compreso e tutti lo attuino in modo omogeneo.

Uno dei rischi più comuni è quello di introdurre controlli inutili e inefficienti, per esempio pratiche burocratiche eccessive. È importante ricordare che i controlli inefficienti diventano, dopo poco, anche inefficaci. Questo non vuol dire che tutte le pratiche burocratiche siano inutili, ma è sempre necessario prestare attenzione affinché siano correttamente dimensionate, anche con il supporto di programmi informatici.

9.3.2 Il piano delle azioni

Dopo aver scelto le azioni da intraprendere, vanno pianificate, coinvolgendo le parti interessate, riportando:

il responsabile dell’azione;

la data prevista di chiusura dell’azione;

le risorse necessarie per attuare l’azione;

le modalità di verifica dell’efficacia dell’azione.

La pianificazione dovrebbe anche includere le attività di formazione per il personale che dovrà installare, configurare e amministrare i controlli e per il personale che li dovrà utilizzare o che dovrà seguire le nuove procedure.

L’elenco delle azioni, o piano delle azioni, deve essere approvato dai responsabili dei rischi affinché forniscano le risorse necessarie al suo completamento.

Quando un’azione richiede l’avvio di un progetto lungo e complesso, lo si potrebbe ripartire in più fasi. In questo caso andrebbero indicati i benefici previsti al termine di ogni singola fase, come si può intuitivamente dedurre dalla figura 9.3.1.

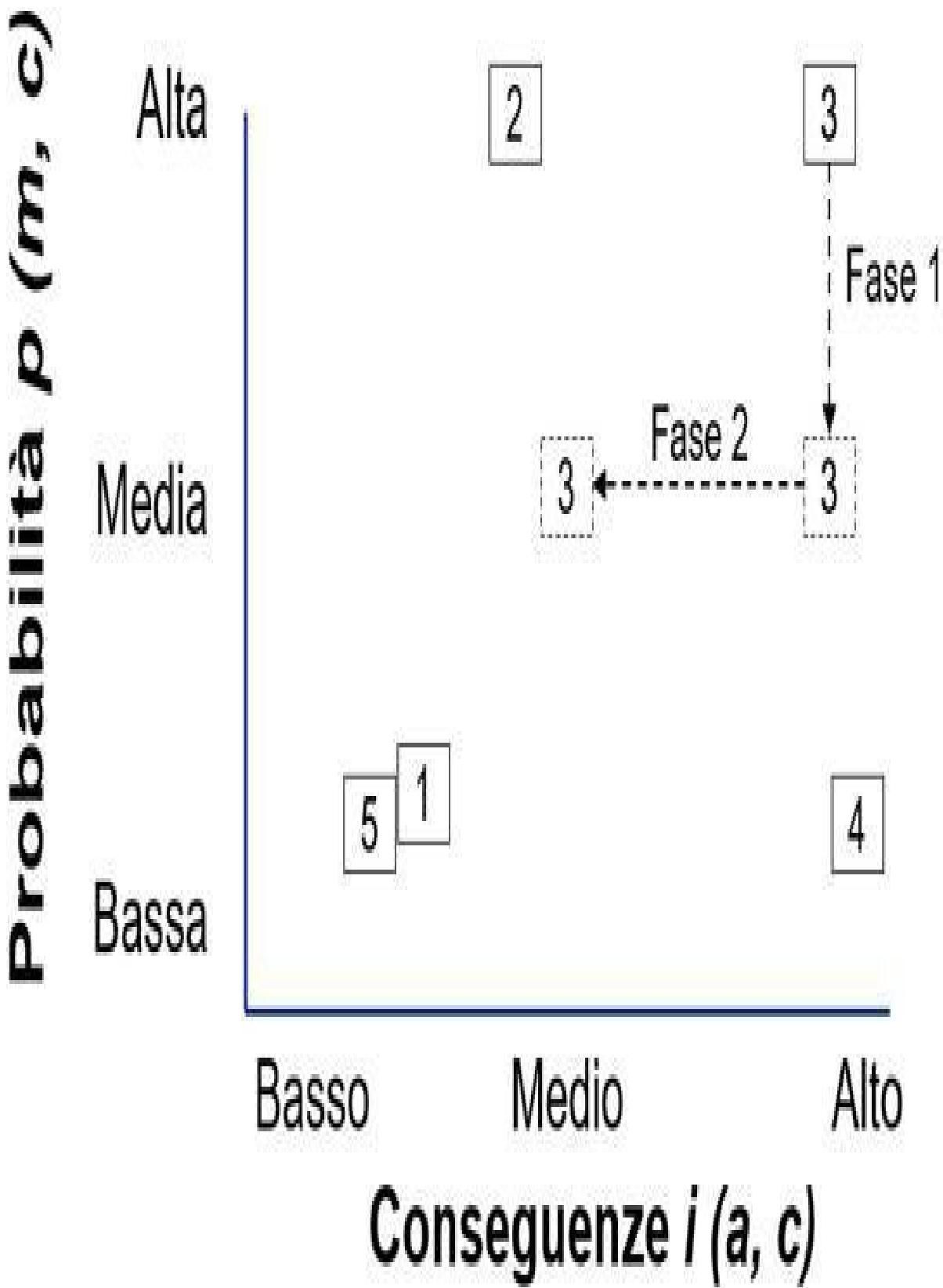


Figura 9.3.1:

Analisi dei benefici di un’azione in più fasi

Per un progetto suddiviso in più fasi potrebbe non essere possibile indicare una data precisa di ultimazione. In questi casi, è comunque necessario indicare: una data indicativa per l’ultimazione del progetto (per esempio un trimestre di un anno specifico) e le date precise di ultimazione delle fasi avviate.

9.3.3 Efficacia delle azioni

Dopo aver concluso l’azione, è necessario verificare se è stata realizzata correttamente e ha avuto gli effetti desiderati. In altre parole, è necessario verificarne e valutarne l’efficacia.

La valutazione dell’efficacia dovrebbe avvenire dopo un certo tempo dalla chiusura dell’azione, quando i risultati sono stati integrati nelle normali attività e alcuni benefici dovrebbero essere tangibili. Questo argomento è approfondito nel paragrafo 15.6.4.1.

9.3.4 Tenuta sotto controllo del piano di azioni

Nel tempo dovrebbero essere analizzati gli avanzamenti delle azioni da parte dei responsabili dei rischi, in modo che eventuali ritardi o altri problemi siano gestiti.

Alcuni istituiscono un comitato (paragrafo 12.3.1.5) al quale partecipano i responsabili dei rischi, dei sistemi informatici e della sicurezza fisica, in modo da analizzare l'avanzamento e gli impatti di ciascuna azione in tutte le aree coinvolte.

Note

³⁴Questa è solo una delle tante: www.ilsole24ore.com/art/impresa-e-territori/2013-04-23/trony-negozi-fnac-154148.shtml.

³⁵www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros.

³⁶www.bleepingcomputer.com/news/security/ccleaner-compromised-to-distribute-malware-for-almost-a-month/.

Capitolo 10

Monitoraggio e riesame del rischio

Chissà chissà domani

su che cosa metteremo le mani.

Lucio Dalla, Futura

Gli asset e le informazioni e il loro valore, le minacce e la loro verosimiglianza e le vulnerabilità e la loro gravità cambiano nel tempo oppure sono percepite diversamente nel tempo.

Bisogna quindi tenere sotto controllo il contesto di riferimento affinché i cambiamenti siano identificati.

È anche necessario che siano mantenuti aperti dei canali di comunicazione con le parti interessate coinvolte nel corso della valutazione e del trattamento del rischio, in modo che possano segnalare tempestivamente le novità rilevanti. Andrebbero anche monitorate le segnalazioni provenienti da newsletter, articoli di cronaca o specialistici, report e conferenze; alcune di queste fonti sono riportate in bibliografia.

Tutte le segnalazioni andrebbero registrate, dopo averne valutato la pertinenza per la sicurezza delle informazioni. Per questo alcune organizzazioni indicano una persona addetta alla loro raccolta e sintesi da utilizzare per il successivo riesame della valutazione del rischio.

Alcune segnalazioni possono richiedere interventi immediati e possono essere trattate nell’ambito di processi ben stabiliti, come quello di gestione degli incidenti (paragrafo 12.13), delle vulnerabilità, delle non conformità e del miglioramento (paragrafo 15.10).

Bisogna effettuare nuovamente la valutazione del rischio a intervalli periodici oppure a seguito di cambiamenti rilevanti, come è meglio indicato nel paragrafo 15.6.2.

10.1 Analisi del rischio operativo

La valutazione del rischio illustrata dei capitoli precedenti, come già detto, è di tipo tattico o strategico, permette di identificare aree di miglioramento a livello di processo o di tecnologie e spesso porta ad avviare progetti di lunga durata. È utile per impostare un budget annuale e per una relazione a livello della Direzione.

Nel corso delle attività, però, il rischio va costantemente monitorato: nuove vulnerabilità ai sistemi in uso (che possono anche richiedere significativi interventi per essere mitigate), nuove modalità con cui si presentano vecchie minacce (come si è visto con il social engineering, che si è evoluto con l’aumento dello smart work, o con il supporto dell’intelligenza artificiale). Questo avviene attraverso il monitoraggio di molti canali di informazione (inclusi frequenti scansioni della rete informatica per identificare vulnerabilità), l’analisi della pertinenza delle segnalazioni per la propria organizzazione (e quindi un inventario degli asset aggiornato e completo) e decisioni rapide e di tipo operativo. Spesso le segnalazioni pertinenti riguardano vulnerabilità inaccettabili da rimuovere immediatamente, per cui i criteri di accettabilità non sono dettati dalla Direzione, ma dai tecnici.

Le analisi delle segnalazioni vanno accompagnate da una valutazione dei possibili impatti di un evento o dello sfruttamento di una vulnerabilità e della probabilità con cui questo evento potrebbe manifestarsi o la vulnerabilità sfruttata.

Si tratta quindi di una valutazione del rischio, ma di tipo operativo (anzi, parte del normale esercizio, business as usual) ed è solitamente ignorata da chi si occupa di valutazione del rischio relativo alla sicurezza delle informazioni, anche se ne è una sua parte.

Ulteriore valutazione del rischio relativa alla sicurezza delle informazioni di tipo operativo è quella che riguarda i singoli progetti. Essi potrebbero avere impatti sulle informazioni. Si pensi alla ristrutturazione degli uffici, che, nel periodo dei lavori, risultano accessibili da numerosi estranei che potrebbero rubare o danneggiare, anche inavvertitamente, archivi cartacei o strumenti informatici. Si pensi anche all'introduzione o aggiornamento dei sistemi informatici. Di questo argomento si discute nei paragrafi 12.3.3 sul controllo sui progetti e 12.9.3 sul controllo sui cambiamenti.

Sarà necessario, nel futuro, riflettere su come queste valutazioni del rischio, tattiche e operative, devono convivere.

Sarà necessario riflettere sul reale significato della valutazione del rischio di tipo tattico, in modo da non usarla in modo improprio e non appesantirla con questioni puramente operative. Anzi, è possibile usarla come occasione di incontro tra le diverse funzioni e competenze, affinché si confrontino su strategie, progetti, eventi dell'ultimo anno. Di certo il budget è un obiettivo di questo esercizio, ma non ne dovrebbe essere il fine. Il fine dovrebbe essere portare visibilità alla Direzione.

10.2 L'integrazione delle analisi del rischio

Da molti anni si parla di Enterprise risk management (ERM), ossia di gestione del rischio complessivo per tutta un'organizzazione e relativo a tutte le aree. Questo approccio ha l'ambizione di promuovere una gestione dell'organizzazione basata sui rischi, anche quelli con possibile esito positivo (le cosiddette opportunità, di cui si tratterà più diffusamente nel paragrafo 15.6.1) e quindi basata su una loro visione complessiva, in modo da distribuire risorse e priorità nel modo più efficace.

Questo libro non ha certo l'ambizione di trattare questo argomento, ma sempre più si assiste a tentativi di unire la valutazione del rischio relativo alla sicurezza delle informazioni con altre, incluse quelle relative ai potenziali reati (paragrafo 12.15.1.4), alla sicurezza delle persone e alla corruzione.

Alcuni ambiti sono apparentemente facilmente integrabili, come quelli relativi alla sicurezza delle informazioni, al trattamento dei dati personali e alla continuità operativa. È opportuno osservare che ambiti diversi richiedono sensibilità e competenze diverse e anche persone diverse. Cercare di unire le valutazioni del rischio può essere controproducente.

Sicuramente è necessario riflettere su come impostare la valutazione del rischio relativo alla sicurezza delle informazioni in modo che i suoi risultati possano essere integrati con gli altri. Può essere opportuno cercare una visualizzazione comune di tutti i rischi più elevati, come presentato dalla tabella in figura figure 10.2.1 da [129].

Figura 10.2.1:

Registro dei rischi



Parte III

Minacce e controlli di sicurezza delle informazioni

Capitolo 11

Tecniche di minaccia

*S'i fosse fuoco, arderei 'l mondo;
s'i fosse vento, lo tempestarei;
s'i fosse acqua, i' l'annegherei;
s'i fosse Dio, mandereil' en profondo.*

Cocco Angiolieri

Nel seguito sono illustrate minacce normalmente pertinenti a tutte le organizzazioni.

La suddivisione che segue non è basata su alcuna tassonomia condivisa. Esistono diverse proposte su pubblicazioni [16, 91] o sul web³⁷, ma nessuna sembra aver raccolto un consenso molto vasto. Inoltre esse sono più pertinenti alla classificazione degli incidenti informatici che non alla valutazione del rischio relativo alla sicurezza delle informazioni.

Alcune delle proposte possono essere discutibili, come l'inserimento dello sciopero come caso particolare dell'esaurimento o riduzione di risorse. Quando si identifica il rischio non si devono usare esattamente le tecniche qui riportate, ma queste possono costituire un punto di partenza per predisporre elenchi aderenti al contesto in cui si opera.

Si inizia con quattro minacce generali, non dirette alle informazioni, ma propedeutiche per attaccare le informazioni stesse. Si conclude con minacce relative a tecnologie specifiche, ossia IoT, OT, IIoT e intelligenza artificiale.

11.1 Intrusione nella sede o nei locali da parte di malintenzionati

Agenti di questa minaccia sono:

persone esterne malintenzionate;

persone interne malintenzionate.

Un esterno malintenzionato potrebbe voler accedere alla sede dell’organizzazione senza permesso. Per questo può adottare diverse tecniche, tra cui: entrare violentemente nella sede rompendo porte o finestre, clonare chiavi fisiche o tessere magnetiche, utilizzare un PIN per aprire una porta dopo aver osservato una persona autorizzata, approfittare di cantieri, convincere qualcuno di avere il permesso per accedere (molte volte basta presentarsi in giacca e cravatta all’ingresso), confondersi in mezzo al personale quando entra la mattina, accodarsi a qualcuno quando supera i tornelli di ingresso (piggy backing o tailgating), saltare i tornelli di ingresso, ricattare qualcuno. Le tecniche sono tantissime e molti spettacoli di intrattenimento (film, telefilm, libri e racconti) e casi di cronaca ne suggeriscono sempre di nuovi.

Ci sono anche casi divertenti o macabri: per accedere nei locali dove l’accesso è controllato con le impronte digitali, è possibile duplicare quelle di qualcuno con la gomma da masticare³⁸; purtroppo, si racconta anche che qualcuno abbia tagliato la mano a una persona allo stesso scopo³⁹.

Le stesse tecniche possono essere utilizzate per accedere ai locali interni della sede, agli archivi, alle sale server, agli uffici, eccetera: una persona che ha accesso all'edificio, sia perché autorizzata sia perché entrata abusivamente, potrebbe cercare di entrare in singoli locali senza autorizzazione.

11.2 Intrusione nei sistemi informatici da parte di malintenzionati

Agenti di questa minaccia sono:

persone esterne malintenzionate;

persone interne malintenzionate;

amministratori di sistema (interni o fornitori) malintenzionati;

utenti del sistema informatico, interni ed esterni, inclusi clienti, fornitori e partner, quando cercano di ampliare le proprie autorizzazioni senza permesso.

La minaccia riguarda tutti i sistemi informatici, tra cui: server, apparati di rete, applicazioni, PC, dispositivi portatili come cellulari, smartphone e tablet. Può anche riguardare impianti industriali o dispositivi non associati al trattamento delle informazioni, come lavatrici, frigoriferi e altri impianti di casa.

Un esterno può attaccare i sistemi informatici per effettuare altri attacchi presentati nei paragrafi successivi (lettura e copia non autorizzate di informazioni, uso non autorizzato dei sistemi informatici, eccetera).

Alcune volte un sistema può essere utilizzato per attaccare ulteriori sistemi (in

questo caso, i computer utilizzati senza autorizzazione sono anche chiamati zombie).

Esempio 11.2.1. Nel 2016, molti servizi Internet risultarono indisponibili a causa di un attacco che sfruttò dispositivi precedentemente compromessi⁴⁰. Con un malware, dei malintenzionati presero il controllo di dispositivi e poi lanciarono un attacco di Distributed denial of service a Dyn, uno dei nodi Internet più importanti.

Oggi, con la diffusione di dispositivi eterogenei collegati a Internet (che costituiscono il cosiddetto Internet of things o IoT), spesso progettati e sviluppati senza attenzione alla sicurezza, è sempre più facile per un attaccante iniziare un attacco di questo tipo. Questi strumenti non vanno sottovalutati: sono già stati utilizzati per condurre attacchi e come punti di accesso alle reti aziendali.

In modo simile, non sono da sottovalutare gli impianti industriali, anch'essi connessi a Internet.

L'intrusione nei sistemi di un'organizzazione può avvenire sfruttando vulnerabilità presenti nei sistemi dei fornitori, potenzialmente più insicuri, e poi usando questi come ponte. Questo prende il nome di supply chain attack.

Esempio 11.2.2. Il supply chain attack ebbe molta notorietà a fine 2020 e poi a metà 2021, quando una sua variante ebbe impatti molto significativi: le vittime iniziali, infatti, furono produttori di software (SolarWinds e Kaseya⁴¹) e il software stesso fu usato per diffondere del ransomware.

Questa minaccia si collega alla precedente, perché alcune tecniche richiedono un accesso fisico alla rete informatica, ottenibile anche a seguito di intrusione alla sede o ai locali.

Le tecniche per accedere in modo non autorizzato ai sistemi informatici comprendono il ricatto, l’osservazione di qualcuno che inserisce le proprie credenziali e altre illustrate nel seguito.

Il meccanismo più diffuso per controllare gli accessi a un sistema informatico prevede l’uso di una password. Esso non è affatto il più sicuro: troppi utenti hanno la pessima abitudine di comunicarla ad altri (soprattutto familiari o colleghi), sceglierla facilmente indovinabile da persone non autorizzate⁴², scriverla su fogli di carta in bella vista, inserirla in modo che chiunque possa vedere i tasti premuti (è anche successo di vedere una persona che la inseriva ripetendola a voce alta). Casi di cronaca lo confermano: il principe William fotografato con alle spalle un foglio con user-id e password di un qualche sistema di sicurezza⁴³, coniugi che si scambiano le password per l’accesso ai servizi utilizzati per lavoro⁴⁴, utenti che comunicano la propria password a un perfetto sconosciuto solo perché questo gli ha telefonato presentandosi come un responsabile dei sistemi informatici [110].

I malintenzionati possono individuare le password di qualcuno verificando con dei software tutte le password possibili con un attacco detto brute force, spesso iniziando con le parole più comuni con un attacco a dizionario.

Poiché gli utenti di un sistema informatico tendono a utilizzare la medesima password per tutti i sistemi a cui hanno accesso (rete dell’organizzazione per cui lavorano, email personale e di lavoro, social network, siti di e-commerce, eccetera), un malintenzionato può attaccare un sistema vulnerabile su Internet,

scoprire le password dei suoi utenti e poi cercare di utilizzarle per accedere ad altri sistemi.

Le tecniche di intrusione con soli programmi software sono generalmente dette tecniche di hacking e prevedono le fasi qui riassunte:

investigazione: si cerca di comprendere come sono fatti i sistemi da attaccare, anche attraverso ricerche sul web (molti, imprudentemente, rendono disponibili dettagli sull'architettura informatica della propria organizzazione); un interno ha accesso a maggiori informazioni di un esterno; fanno parte di questa fase anche le analisi tecniche (fingerprinting) e la ricerca delle vulnerabilità (enumeration);

intrusione: l'aggressore individua delle vulnerabilità e applica degli exploit per sfruttarle e accedere ai sistemi, cercando di ottenere autorizzazioni sempre più estese;

attacco: l'aggressore raccoglie i dati dal sistema compromesso o attiva delle funzionalità;

uscita: l'aggressore lascia i sistemi dopo aver cancellato le proprie tracce; prima di uscire può installare dei programmi (rootkit) per accedere nuovamente al sistema attraverso una backdoor e svolgere ulteriori attività.

Un malintenzionato può individuare una vulnerabilità e inserire dati non corretti in un sistema informatico per indurlo in errore e permettergli così di accedere (i due attacchi di questo tipo più diffusi sono noti come buffer overflow e SQL Injection).

Altre tecniche (per esempio il cross-site scripting) prevedono di inserire nei siti web e nei forum di discussione dei dati tali da permettere l'intrusione ai computer di coloro che vi accedono.

11.3 Social engineering e frodi

Agenzi di questa minaccia sono:

persone esterne malintenzionate;

persone interne malintenzionate.

Si preferisce utilizzare l'espressione inglese al posto dell'italiano ingegneria sociale. I termini inganno, frode e raggiro sono usati in contesti più generali, mentre si parla di tecniche di social engineering quando usate per intrusioni fisiche o informatiche. Alcuni esempi:

presentarsi in giacca e cravatta all'ingresso di un'organizzazione e spacciarsi per un cliente;

telefonare a un utente dei sistemi informatici e spacciarsi per un tecnico informatico che ha bisogno della sua password⁴⁵;

inviare una email a un utente affinché acceda con la propria password a un sito apparentemente legittimo ma fasullo (phishing, per ricordare l'espressione “pescare password”)⁴⁶;

inviare email di phishing, ma con un contenuto personalizzato a seconda del ricevente (spear phishing);

contattare un amministratore di sistema spacciandosi per un dirigente dell'organizzazione e raccogliere informazioni sui sistemi informatici (un fingerprinting non tecnologico);

richiedere alla contabilità, spacciandosi per un dirigente dell’organizzazione, un pagamento urgente a un nuovo fornitore (evidentemente finto)⁴⁷; questo tipo di attacco ha successo se la persona contattata preferisce non disturbare un dirigente per chiedere conferma o in caso di lavoro da remoto (ancora più diffuso durante l’emergenza COVID del 2020) perché la persona non ha l’occasione di chiedere conferma di persona.

Per quanto riguarda l’ultimo esempio, se le richieste avvengono via email, usando domini simili a quelli noti o le funzionalità di molti client di posta che nascondono l’indirizzo completo del mittente o account compromessi in precedenza, questo attacco prende il nome di BEC (business email compromise).

Queste tecniche sono ben descritte nel libro di uno dei più famosi hacker [110] o nel film “Prova a prendermi” anch’esso basato sulla vita di un famoso truffatore.

Esempio 11.3.1. Un consulente fu ammesso senza ulteriori controlli nella sede di un cliente, presidiata da una guardia, solo perché si era avvicinato all’accesso con un’aria convinta del proprio diritto a entrare.

Il consulente immaginava di doversi identificare dopo essere entrato e non aveva intenzione di accedere alla sede senza autorizzazione. Questo è un caso di social engineering involontario.

L’FBI ha anche redatto una lista delle frodi più comuni⁴⁸ e tra di esse molte sfruttano servizi informatici.

Il numero di persone che cade nel tranello è molto elevato. Le cause sono spesso da ricercare nella volontà di aiutare e nei modelli educativi, nella paura di essere accusati di non aver fatto bene il proprio lavoro e nella prospettiva di guadagno materiale o di riconoscenza.

11.4 Furto d'identità

Agenti di questa minaccia sono:

persone esterne malintenzionate;

persone interne malintenzionate.

Quando si parla di furto d'identità si può intendere il solo furto della user-id e password (credenziali) di una persona per accedere abusivamente a dei sistemi oppure un insieme molto vasto di attività svolte con il nome di un'altra persona: acquisti di beni e servizi su Internet o nel mondo reale, apertura di conti bancari, richiesta di carte di credito, partecipazione alle attività di un gruppo di persone, eccetera.

Chi ruba l'identità di un'altra persona potrebbe avere intenti criminali oppure voler cambiare vita nascondendosi dietro il nome di un altro.

Questa minaccia può essere attuata in molti modi, anche attraverso normali tecniche di social engineering, come quella di presentarsi dal commercialista per avere le credenziali del titolare di un'impresa temporaneamente assente⁴⁹.

11.5 Danneggiamento di apparecchiature fisiche

Agenti di questa minaccia sono:

persone esterne, malintenzionate o non malintenzionate;

persone interne, malintenzionate o non malintenzionate;

amministratori di sistema (interni o fornitori);

strumenti tecnici;

natura.

Le apparecchiature possono essere:

apparecchiature nella sede come PC, server, impianti, fotocopiatrici;

apparecchiature fuori sede, come sportelli ATM (in Italia detti Bancomat), biglietterie automatiche, pannelli informativi e antenne;

dispositivi portatili, come PC, cellulari, smartphone, tablet, chiavi USB;

linee di telecomunicazione, interne alla sede o esterne.

Si possono anche considerare le apparecchiature in senso lato:

documenti;

la sede dell'organizzazione.

I danneggiamenti potrebbero avvenire da parte di malintenzionati, anche con tecniche potenzialmente disastrose, come incendi, allagamenti, bombe ed esplosivi. Gli atti di guerra rientrano in questo caso.

I malintenzionati, per accedere a informazioni riservate, potrebbero manomettere apparecchiature, smart card, lettori di tessere, ATM, terminali POS e cavi di trasmissione. Questo attacco è molto diffuso ed è spesso indicato con il termine inglese *tampering* [157].

Per quanto riguarda i danneggiamenti da parte di persone non malintenzionate, è bene ricordare quanto sia facile inciampare in cavi mal disposti, urtare server o scaffali. Sono anche molto comuni i danneggiamenti dovuti a cantieri, come per esempio quelli stradali che spesso interrompono le linee di comunicazione.

Alcuni incidenti potrebbero fare sorridere, come il rovesciamento del caffè sulla tastiera o la caduta di un cellulare in una piscina. Alcune persone, per contro, non solo commettono errori, ma sono proprio incuranti delle apparecchiature affidate loro e, per esempio, ci lasciano giocare i bambini.

Quando si consente di portare fuori dalla sede del materiale, inclusi i numerosi dispositivi portatili affidati al personale, le possibilità di avere danneggiamenti, perdite o furti sono elevate.

I danneggiamenti possono essere causati da strumenti tecnici perché possono causare:

incendi a causa di avarie agli impianti o alle apparecchiature;

allagamenti dovuti a rotture delle tubature;

eccesso di calore dovuto ad avarie degli impianti di aria condizionata o ventilazione;

blackout elettrici o sbalzi di tensione.

Gli strumenti tecnici possono degradarsi o rompersi autonomamente a causa di obsolescenza o non corretta progettazione o produzione.

La natura può arrecare danni a causa di:

polvere, corrosione, eccesso di calore o congelamento;

fenomeni climatici quali uragani, tornado o nevicate;

fenomeni disastrosi quali terremoti o eruzioni vulcaniche;

fulmini;

incendi;

allagamenti dovuti a esondazioni di corsi d'acqua o simili.

Alcune di queste minacce potrebbero non avere impatti diretti sulle informazioni, ma sulle misure di sicurezza, come per esempio un guasto dei tornelli all'ingresso di un edificio.

11.6 Danneggiamenti dei programmi informatici

Agenti di questa minaccia sono:

persone esterne, malintenzionate o non malintenzionate;

persone interne, malintenzionate o non malintenzionate;

amministratori di sistema (interni e fornitori);

strumenti tecnici.

Se l'attacco è perpetrato da malintenzionati, l'obiettivo potrebbe essere l'esaurimento di risorse (paragrafo 11.19), oppure l'accesso non autorizzato ai sistemi informatici.

Gli utenti non malintenzionati potrebbero utilizzare male dei programmi informatici e, anche perché mal progettati, questi potrebbero assumere un comportamento anomalo.

Esempio 11.6.1. Nel 2020, la sanità inglese consolidava i dati dei test COVID-19 su un foglio Excel. Però Excel può trattare un massimo di un milione circa di righe (65mila nelle vecchie versioni) e i dati erano più numerosi. Il risultato è che molte righe furono perse dal foglio usato.⁵⁰.

Gli amministratori di sistema e i programmati, anche se non malintenzionati,

potrebbero danneggiare i programmi configurandoli o modificandoli non correttamente. Questi casi sono molto numerosi⁵¹.

Alcuni fornitori di sviluppo software potrebbero introdurre vulnerabilità o inefficienze nel codice per poi farsi affidare i lavori di correzione o ottimizzazione⁵².

Si osservi che questa minaccia ha sicuramente impatti sull'integrità e sulla disponibilità delle informazioni. Potrebbe avere impatti anche sulla riservatezza se il danneggiamento riguarda i meccanismi di sicurezza, il cui funzionamento scorretto potrebbe rendere disponibili le informazioni a persone non autorizzate.

11.7 Furto di apparecchiature informatiche o di impianti fisici

Agenzi di questa minaccia sono:

persone esterne malintenzionate;

persone interne malintenzionate.

Le apparecchiature e gli strumenti che potrebbero avere impatti da questa minaccia sono quelli riportati nel paragrafo 11.5. Per il furto finalizzato alle sole informazioni, vedere il paragrafo 11.8.

Per attuare questa minaccia non sempre è necessaria un'intrusione fisica: un esterno può approfittare della disattenzione di qualcuno per rubargli PC,

cellulare, smartphone o tablet, con violenza o destrezza. A molti hanno rubato il PC lasciato nella macchina parcheggiata in un'area di servizio in autostrada; a qualcuno hanno anche rubato l'automobile, con dentro molti documenti e il PC, mentre era sceso a citofonare lasciando la chiave inserita.

In questi anni, a causa dell'aumento del costo del rame, sono stati rubati i cavi di telefonia, telecomunicazione e alimentazione elettrica con la conseguente interruzione dei servizi correlati.

Casi particolari relativi al personale interno sono costituiti dai dimissionari che hanno “subito” il furto di PC, cellulare o smartphone pochi giorni prima della conclusione del rapporto di lavoro. In altri casi la persona uscente ha reso all’organizzazione il PC con RAM o hard disk meno potenti di quelli inizialmente assegnati.

L’obiettivo, nella maggior parte dei casi, è l’apparecchiatura fisica per il suo valore come oggetto. Ciò non esclude che i ladri potrebbero essere delle spie oppure possano diffondere le informazioni trovate nel dispositivo rubato.

11.8 Lettura, furto, copia o alterazione di documenti in formato fisico

Agenti di questa minaccia sono:

persone esterne malintenzionate;

persone interne malintenzionate.

I documenti cartacei o su altro supporto possono essere rubati a seguito di un’intrusione in una sede, un ufficio, un armadio o una cassaforte. Se i documenti sono già all’esterno della sede, dei malintenzionati possono rubare la valigia o il contenitore dove sono riposti, oppure intercettare la posta.

Le spie copiano i documenti evitando di rubarli. In questo modo la vittima non si accorge di quanto avvenuto.

È successo a molti di poter leggere dei documenti perché si sono trovati in un ufficio senza che nessuno controllasse, per esempio perché la persona con cui avevano appuntamento si era dovuta assentare un momento oppure era in ritardo. Succede spesso di invitare i consulenti a usare come punto d’appoggio un ufficio il cui responsabile è assente, ma con i documenti in bella vista.

Altri casi sono costituiti dai documenti non ritirati da fax, scanner, stampanti e fotocopiatrici, disponibili per chiunque li voglia rubare o copiare, anche mentalmente o con una foto scattata con il cellulare.

Nei luoghi pubblici è comune vedere persone che leggono documenti in formato cartaceo o al computer in modo da renderli visibili anche a estranei (per esempio in treno o in sale d’aspetto).

Possiamo includere in questo gruppo anche la perdita involontaria di documenti.

Esempio 11.8.1. Nel 2020, una folata di vento fece volare dalla finestra di una società alcuni documenti cartacei con dati personali e appena digitalizzati con scanner.

Questo era un caso non previsto in precedenza, ha avuto impatti sulla riservatezza e non sulla disponibilità (perché già passati allo scanner) e non è attribuibile a malintenzionati. Alcune minacce, quindi, non sono facilmente classificabili.

11.9 Intercettazioni di emissioni elettromagnetiche

Agenti di questa minaccia sono persone malintenzionate.

Tutti gli strumenti informatici emettono emissioni elettromagnetiche, in particolare i monitor dei computer e i cavi di collegamento.

Un malintenzionato può intercettare le emissioni per ricostruire quanto visualizzato dall'utente. Si tratta di una tecnica complessa, che richiede vicinanza fisica alla vittima.

In passato si utilizzavano anche altre tecniche per ottenere risultati simili. Per esempio, alcune spie riuscivano a ricostruire quanto scritto sulle telescriventi grazie all'analisi audio della tastiera [160].

Una ricerca recente ha dimostrato che è possibile identificare i caratteri attraverso l'analisi termica della tastiera⁵³.

11.10 Interferenze da emissioni elettromagnetiche

Agenti di questa minaccia sono:

persone esterne malintenzionate e non malintenzionate;

persone interne malintenzionate e non malintenzionate;

apparecchiature.

Collegata alla minaccia precedente, questa riguarda invece emissioni che interferiscono con altre apparecchiature. Esse possono alterare l'integrità o la disponibilità delle informazioni quando trasmesse o memorizzate su un supporto magnetico.

Questo caso è spesso ben visibile dalle interferenze su alcuni schermi quando vi si lascia il cellulare vicino.

Non di rado, per errori delle persone addette, i cavi utilizzati per le trasmissioni informatiche sono posti vicini a quelli per la distribuzione dell'energia e creano interferenze reciproche.

11.11 Lettura e copia non autorizzata di documenti informatici

Agenti di questa minaccia sono:

persone esterne malintenzionate, anche a seguito di intrusione; persone interne malintenzionate, anche a seguito di intrusione a sistemi per i quali non sono autorizzati ad accedere.

La lettura e copia non autorizzata di documenti informatici, rispetto a quelli cartacei, è spesso più facile da attuare e difficile da rilevare: per quelli cartacei, la lettura può essere facilmente notata e la copia richiede l'uso di una fotocopiatrice o di una macchina fotografica, anch'esse potenzialmente rilevabili. Per un documento informatico, soprattutto se si hanno già le autorizzazioni per accedervi, è necessario solo un computer (solitamente con una chiave USB o l'accesso a un sistema di file sharing⁵⁴) ed è difficile che qualcuno si accorga dell'azione. Molti, quindi, effettuano questo attacco, anche per rivendere le informazioni o fare concorrenza alla propria organizzazione⁵⁵, sentendosi psicologicamente meno colpevoli che se lo ripetessero sui documenti cartacei.

Esempio 11.11.1. A fine 2020 fu scoperto un malware installato sui sistemi di Leonardo S.p.A., società coinvolta in molti progetti innovativi e strategici nell'ambito della difesa, usato per copiare e, quindi, rubare dati e documenti. Si ipotizza che il malware fosse stato installato da un dipendente e da un consulente dell'azienda⁵⁶.

Se il malintenzionato non dispone delle necessarie autorizzazioni, può applicare delle tecniche di intrusione ai sistemi (paragrafo 11.2).

Esempio 11.11.2. Un modo con cui può essere attuata questa minaccia e che

ne dimostra la facilità, è l'iPod slurping: un malintenzionato chiede a una persona di collegare il proprio dispositivo portatile al suo computer, per esempio per poterlo caricare. Il dispositivo, però, fa partire un programma per copiare tutti i dati del PC nella propria memoria senza che il malcapitato se ne accorga.

Se l'intrusione è reiterata per lungo tempo senza essere identificata, prende il nome di Advanced persistent threat o APT. Essa si basa solitamente su una combinazione di tecniche sofisticate (include lo spear phishing, il social engineering, lo sfruttamento di vulnerabilità non ancora note e l'aggiornamento del malware installato affinché continui a non essere individuato) e richiede molto tempo. Per questo le minacce APT hanno solitamente come obiettivo le grandi imprese multinazionali o infrastrutture collegate alla sicurezza nazionale di Paesi importanti e sono condotte da gruppi di persone anche finanziate da grandi concorrenti o agenzie di spionaggio.

Molto particolare è quanto si racconta sul dossier Mitrokhin: non potendo portare al di fuori delle sedi del KGB alcun documento, né effettuare trasmissioni informatiche, l'agente sovietico Vasili Mitrokhin memorizzò le informazioni visualizzate sul computer nel proprio ufficio per riscriverle a mano a casa e preparare il famoso dossier.

11.12 Modifica non autorizzata di documenti informatici

Agenti di questa minaccia sono:

persone esterne malintenzionate e non malintenzionate, anche a seguito di intrusione;

persone interne malintenzionate e non malintenzionate, anche a seguito di intrusione a sistemi per i quali non sono autorizzati ad accedere; apparecchiature.

La modifica comprende anche la cancellazione di un documento.

La modifica di un documento cartaceo è facilmente rilevabile, mentre quella di un documento informatico, se si hanno o si ottengono abusivamente le opportune autorizzazioni, può essere difficilmente individuabile.

Per quanto riguarda i malintenzionati, le modifiche potrebbero essere fatte per frode o per nascondere eventuali errori.

Relativamente ai non malintenzionati, basti pensare a quanti errori si possono commettere per distrazione. Per esempio, si possono fare errori di digitazione (inserendo una “a” al posto di una “s”⁵⁷), oppure aprire un documento, modificarlo per errore, chiuderlo e accettare di salvare le modifiche per automatismo, senza pensare che tali modifiche non erano previste. Molti sistemi non sono a prova di errore (error-proof) e sono propensi agli errori (error-prone). Le prime versione di Windows 10 ne furono un esempio perché non chiedevano conferma della cancellazione di un file.

Gli errori potrebbero non essere causati dagli utenti ma dai programmi software, se mal sviluppati o danneggiati, e da guasti nelle apparecchiature informatiche (inclusi gli sbalzi di tensione), che possono modificare delle informazioni, spesso rendendole illeggibili.

File Conversion - 02-20081210-Questions ISMAS.EN CG7-11.doc



Select the encoding that makes your document readable.

Text encoding:

Windows (Default) MS-DOS Other encoding:

Document direction:

Right-to-left Left-to-right

- Wang Taiwan
- Western European (DOS)
- Western European (IA5)
- Western European (ISO)
- Western European (Mac)
- Western European (Windows)

Preview:

QÇ‰i0{9uÊbôÄ.
..... Column Break

ch#PoMCú}¶, '1Cf\ZÍ97TiÇSR|
P^éÍpÑ'LftSNôæ»)œniPAÿþúu-ÐÐ-ß ñ9 ä·r:Ø-R; Ý+=Ë«,ëç%é
..... Page Break

q Zæ"»¶‰0þT" ï¶[š+?ý:+^

°@Mq• _÷=OÀl§-³-k(8I‰„ae•¶Óå³H-)þý4)ý¶VÀ JÁHå/zÃ% k~, -
j¤äY+1ó [E]Äèü06Ý...ð¹+d¤¤ä Ú9iiò' 6)Ýo? x0i«VeÅEÜ]Óe-ýå\Z)SB¶-
S>ù¹fsóéÜtvK,,y %f" x\&

..... Page Break

.....

OK

Cancel

Figura 11.12.1:

Il computer cerca di riconoscere un file corrotto

11.13 Trattamento scorretto delle informazioni rispetto alla normativa

Agenzi di questa minaccia sono:

persone interne malintenzionate;

persone interne non malintenzionate;

fornitori.

Questa minaccia riguarda:

dati in formato elettronico;

dati in formato non elettronico (fax, stampe, lettere, eccetera).

I dati riferibili a una persona, detta interessato, sono definiti dati personali. Questi dati possono essere utilizzati solo su basi legali previste dalla normativa vigente.

Un esempio di trattamento scorretto e illecito dei dati personali è l'uso degli elenchi telefonici per attività di marketing senza il permesso degli interessati, oppure la pubblicazione di foto o video personali senza il permesso delle persone ritratte.

In molti casi le comunicazioni commerciali indesiderate sono fatte consapevolmente da chi vuole attuare tecniche aggressive di marketing. Forse alcuni sono inconsapevoli del disturbo che arrecano e dell'illegalità delle proprie azioni, soprattutto quando dicono “Qual è il problema? Stiamo offrendo un’occasione!” (alcuni dicono che la base legale è il proprio “legittimo interesse”).

Se i contatti avvengono attraverso l’invio di email non richieste, allora si parla di spamming.

I fornitori, se sono loro affidati dei dati, potrebbero utilizzarli per scopi non coerenti con il contratto stipulato (dal 2017, dopo il caso Cambridge Analytica, sono stati segnalati molti esempi di questa minaccia⁵⁸⁾.

Questa minaccia riguarda anche trattamenti scorretti, ma non consapevolmente da parte degli attaccanti.

Esempio 11.13.1. In una scuola italiana, a fine 2020, un bambino segnalò la propria positività al COVID. Allora la scuola fece una comunicazione in bacheca raccomandando a tutti i suoi compagni di classe di fare il tampone e fornendo indicazioni su dove andare.

La circolare in bacheca, però, riportava i destinatari: tutti gli alunni della classe, tranne il positivo, che risultò così facilmente identificabile.

Bisogna prestare attenzione ai sistemi di intelligenza artificiale perché possono fornire risultati non facilmente giustificabili, anche quando corretti, o essere estremamente invasivi. Questo pone problemi etici e quindi il trattamento dei dati con questi strumenti non sempre è ammissibile [63].

L'uso scorretto delle informazioni può comportare il coinvolgimento dell'organizzazione in cause penali o civili, con conseguente perdita di denaro e di immagine.

11.14 Malware

Agenti di questa minaccia sono:

persone esterne malintenzionate;

persone interne malintenzionate;

persone interne non malintenzionate, anche grazie ad azioni di malintenzionati; utenti.

Il termine malware indica tutti i programmi software dannosi per computer e

comprende virus, worm, trojan horse e spyware. Alcuni software permettono agli utenti di creare macro, che possono essere utilizzate anche per diffondere malware. Il malware può colpire ogni genere di computer, inclusi tablet e smartphone.

Questi programmi possono: danneggiare altri programmi e servizi informatici e bloccarli anche per giorni⁵⁹, permettere a un malintenzionato di usare un computer all’insaputa del suo legittimo utilizzatore, inviare a un malintenzionato informazioni presenti sul computer, eccetera.

Un tipo di malware è quello rappresentato dalle backdoor, meccanismi che permettono di accedere al sistema aggirando le normali misure di sicurezza. Esso può essere installato da malintenzionati, oppure da operatori autorizzati a svolgere alcune attività straordinarie. Alcuni operatori autorizzati non chiudono la backdoor al termine dei lavori, lasciando aperte delle vulnerabilità.

Un utente interno può installare del malware volontariamente (per esempio per vendetta nei confronti della propria organizzazione) o involontariamente se apre un file, anche apparentemente innocuo, ricevuto per email o scaricato da Internet.

Quando una spia riesce a installare un software di intercettazione con tecniche tali per cui l’azione non è individuata per lungo tempo, si parla di Advanced persistent threat o APT.

Il malware detto ransomware modifica (solitamente cifrando) i dati di un dispositivo e poi chiede di inviare soldi per poter ripristinare i dati corretti. I ransomware sfruttano anche l’elevata interconnessione dei sistemi, spinta anche dai promotori della cosiddetta convergenza, che permette loro di propagarsi di sistema in sistema.

Una forma particolare di malware è lo spamming.

11.15 Copia e uso illegale di software

Agenti di questa minaccia sono:

persone interne malintenzionate;

persone interne non malintenzionate.

Un interno malintenzionato potrebbe copiare i software e le licenze dell’organizzazione per utilizzarli personalmente, rivenderli o metterli a disposizione del pubblico attraverso sistemi di condivisione dei file.

Un malintenzionato potrebbe installare software non adeguatamente coperto da licenza sui computer e sui dispositivi dell’organizzazione per poter svolgere “meglio” il proprio lavoro, con il risultato che l’organizzazione stessa potrebbe essere ritenuta responsabile del reato e pagare elevate penali.

Nella nostra cultura, grazie al fatto che si tratta di un reato “virtuale”, l’installazione illegale di software è ritenuta poco grave, rendendo questa minaccia molto diffusa.

Il software acquisito attraverso canali non ufficiali può anche essere stato

modificato e introdurre malware o vulnerabilità nei sistemi.

Una persona non malintenzionata potrebbe essere un amministratore di sistema che non tiene il conto di quante installazioni di un certo programma software sono attive, anche a causa delle diversissime tipologie di licenze sul mercato. Alcuni programmi, anche attraverso connessioni con il produttore, bloccano le installazioni ulteriori a quelle previste e l'organizzazione potrebbe avere problemi di operatività fino a quando non ha aggiornato le proprie licenze.

Persone non competenti potrebbero installare e configurare software non autorizzato e in modo non appropriato e aprire vulnerabilità nella rete informatica dell'organizzazione.

Questa minaccia comprende la proliferazione di programmi non previsti dalle procedure dell'organizzazione, anche se free. Non è raro il caso di persone con compiti uguali che utilizzano programmi diversi per svolgerli. Il risultato è che ciascuno perde tempo a installare i propri prodotti, le comunicazioni tra gli utenti sono più complesse (ancora oggi i programmi di videoscrittura non garantiscono la completa interoperabilità) e il passaggio di consegne a una nuova persona può risultare quasi impossibile.

Esempio 11.15.1. A un'organizzazione è successo di dover reinstallare tutti i propri server a seguito delle dimissioni di un operatore perché risultò impossibile capire come venivano gestiti i programmi installati.

11.16 Uso non autorizzato di sistemi e servizi informatici esterni

Agenti di questa minaccia sono gli utenti interni malintenzionati che utilizzano servizi Internet, in particolare quelli di condivisione di file, i social network e il gioco on-line, proibiti dalle regole dell’organizzazione o in modo inappropriato. Le conseguenze di questa minaccia possono essere: perdita di tempo e rallentamenti della rete e dei sistemi.

Alcuni di questi servizi sono utilizzati per attività come l’invio di documenti a persone non autorizzate, l’invio di copie illegali di software e lo scambio di file contrari all’etica dell’organizzazione (pornografici, pedo-pornografici, di terroristi, razzisti, eccetera) o contenenti malware.

11.17 Uso non autorizzato di sistemi e servizi informatici offerti dall’organizzazione

Agenti di questa minaccia sono:

persone esterne malintenzionate;

utenti esterni malintenzionati, inclusi clienti, fornitori e partner.

Il personale interno può utilizzare i servizi dell’organizzazione per attività non lavorative. In particolare l’email per comunicare con gli amici e la connessione Internet per sfruttarne alcuni servizi (vedere anche paragrafo 11.16).

Oggi molte organizzazioni non reputano gravi queste prassi, ma potrebbero subire rallentamenti della rete e riduzione della produttività. Alcuni servizi sono

anche utilizzati per lo scambio illegale di file.

Esempio 11.17.1. In un'organizzazione, dopo aver individuato un file server con la memoria in esaurimento, si scoprì che veniva utilizzato per la condivisione di film, telefilm e file musicali.

Attraverso l'uso scorretto di servizi informatici è possibile rendere disponibili canali utilizzabili da malintenzionati per attaccare l'organizzazione.

Se l'organizzazione mette a disposizione servizi al pubblico, a clienti, a fornitori o a partner, essi potrebbero usarli in modo scorretto e non autorizzato, per esempio come canali per condurre attacchi (vedere, tra gli altri, i paragrafi 11.2, 11.20 e 11.21).

11.18 Recupero di informazioni

Agenti di questa minaccia sono persone malintenzionate.

Questa minaccia riguarda:

dati in formato elettronico;

dati in formato non elettronico (documenti cartacei come fax, stampe e lettere, foto, eccetera).

La normale cancellazione dei dati informatici non li rende irrecuperabili, anche se eliminati da eventuali “cestini” previsti dal sistema operativo: rende solo disponibile lo spazio di memoria occupato; finché non sono memorizzati altri dati nello stesso spazio, quelli precedenti sono ancora facilmente reperibili con semplici programmi software.

Possono essere oggetto di attacco tutte le memorie, inclusi hard disk, chiavi USB, fotocopiatrici e fax.

I malintenzionati potrebbero cercare documenti cartacei riservati anche tra i rifiuti. Questa attività prende il nome di thrashing. Il film Argo del 2013 ha mostrato come i rivoluzionari khomenisti ricostruirono informazioni riservate dell’ambasciata USA in Iran da documenti distrutti.

11.19 Esaurimento o riduzione delle risorse

Agenti di questa minaccia sono:

persone esterne malintenzionate;

utenti dei servizi, interni ed esterni, malintenzionati o non malintenzionati;

apparecchiature;

natura.

La minaccia può avere come effetto il blocco dei servizi informatici o non informatici di un'organizzazione.

Esterini malintenzionati, spesso attivisti, possono voler bloccare i servizi informatici di un'organizzazione per danneggiarla; questo attacco è detto Denial of service (DoS). Esso può essere efficacemente realizzato da poche persone con scarsi mezzi. Nella sua forma più semplice, l'attacco consiste nell'inviare un gran numero di richieste opportunamente progettate al server attaccato, in modo che questo non riesca più a soddisfarle tutte.

Una forma ancora più nociva di DoS, oggi utilizzata per condurre questi attacchi, consiste nell'utilizzare un elevato numero di computer zombie affinché attacchino contemporaneamente uno stesso sistema; questo attacco è detto distributed denial of service (dDoS).

Un Dos o un dDoS, visto che sono facilmente rilevabili, anche se non facilmente contrastabili, possono essere usati per distrarre il personale dell'organizzazione mentre si conducono altri attacchi ai sistemi informatici.

Il web defacement, ossia l'alterazione del sito web di un'organizzazione⁶⁰, è un esempio particolare di Denial of Service.

L'esaurimento di risorse può essere causato da personale interno non malintenzionato quando usa in modo inappropriato i servizi messi a disposizione, per esempio scambiando file molto pesanti e non attinenti l'attività lavorativa (come certi auguri di buone feste e filmati pornografici) o Catene di S. Antonio.

Lo spamming è una forma lieve di riduzione di servizio perché le email non richieste rallentano, anche se di poco, i sistemi informatici e fanno perdere tempo alle persone. Alcune statistiche⁶¹ dicono che almeno il 70% delle email è spam.

L'esaurimento di risorse può essere causato da guasti o danneggiamenti di apparecchiature, già descritti in precedenza.

Per quanto riguarda l'esaurimento di risorse non informatiche, è possibile ricordare alcune forme di protesta negli anni '80 e '90 per cui gli attivisti mandavano continuamente fax allo stesso numero per bloccarlo (si trattava di una forma di protesta abbastanza costosa, a differenza del DoS informatico).

Uno sciopero può essere visto come attacco di esaurimento delle risorse condotto da malintenzionati, nel senso che il suo obiettivo esplicito è bloccare le attività per qualche tempo.

Relativamente all'esaurimento di risorse non informatiche con agenti non malintenzionati, si devono ricordare le dimissioni e le malattie (cause dalla natura), che rendono indisponibili persone e competenze.

Alcuni esaurimenti di risorse possono essere causati anche indirettamente dai fornitori. Il primo caso riguarda il loro fallimento, perché in questo caso non possono più erogare i servizi previsti. Il secondo caso riguarda la perdita di competenze all'interno dell'organizzazione perché completamente trasferite ai fornitori. Il terzo caso viene denominato vendor lock-in e riguarda l'impossibilità di poter sostituire un fornitore con uno equivalente e, quindi, di poter avere un servizio migliore o più adeguato alle esigenze dell'organizzazione; questo potrebbe succedere se il fornitore utilizza tecnologie o applicazioni proprietarie o non diffuse per le comunicazioni, la

memorizzazione e la trasmissione dei dati.

Esempio 11.19.1. La perdita di un fornitore può essere improvvisa e devastante. Un fornitore di apparati di rete e relativa assistenza specialistica chiuse i battenti da un giorno all'altro a inizio 2020 e senza avvisare i propri clienti.

Pochissimi giorni dopo, un cliente ebbe un incidente che poteva essere risolto solo con una correzione al firmware dei firewall, ma questa non poteva più essere apportata. Il tutto fu risolto con alcune soluzioni temporanee e la successiva acquisizione di nuovi strumenti, ma a costi che misero in pericolo l'azienda stessa.

Oggi molte organizzazioni usano servizi cloud e non dispongono più di tecnici informatici competenti; questo è un errore, come dimostrato da molti incidenti⁶².

Un caso decisamente particolare di esaurimento di risorse si ha quando cambiamenti organizzativi, come l'introduzione di nuove procedure o l'assegnazione di nuove responsabilità o un picco di lavoro mal gestito, causano rallentamenti alle attività.

11.20 Intercettazione delle comunicazioni

Agenti di questa minaccia sono:

persone esterne malintenzionate e non malintenzionate,
persone interne malintenzionate e non malintenzionate.

Questa minaccia riguarda:

dati in formato elettronico;
dati in formato non elettronico (si è già accennato all’intercettazione della posta nel paragrafo 11.8);
dati comunicati in forma orale.

Questi attacchi possono essere utilizzati per conoscere informazioni riservate o alterare le comunicazioni tra gli interlocutori legittimi e persuaderli a compiere azioni utili all’attaccante.

L’intercettazione delle comunicazioni elettroniche può avvenire in molti modi. Il più semplice consiste nel collegare un’apparecchiatura alla rete, anche a seguito di intrusione fisica o informatica, e analizzare quanto vi transita.

Più sofisticato è un tipo di attacco noto come man in the middle. Se gli interlocutori, inclusi sistemi informatici tra loro connessi, non utilizzano meccanismi affidabili per riconoscersi, un malintenzionato può intromettersi convincendoli reciprocamente di essere l’altro e facendo da “passacarte”, leggendo o modificando il contenuto delle comunicazioni. Altro tipo di attacco viene condotto quando un utente di un servizio informatico non si disconnette come previsto e un malintenzionato riesce a utilizzare la sua connessione per usarla a proprio piacimento (session hijacking). Questo attacco può comportare il furto d’identità.

A seguito di un’intrusione informatica potrebbero essere manipolate le configurazioni degli apparati di rete in modo che le connessioni siano indirizzate verso un altro servizio, anche di aspetto molto simile a quello legittimo. In questo modo il malintenzionato può raccogliere le informazioni fornite dall’utente a questo servizio fasullo, tra cui password e numeri di carta di credito.

Si stanno sempre più diffondendo i servizi disponibili su Internet di file sharing (tra i più famosi vi sono Dropbox e Google Drive). Alcuni fornitori di questi servizi, come i casi più recenti lo dimostrano⁶³, potrebbero accedere ai dati dei clienti per le più disparate finalità, inclusa l’intercettazione.

Per quanto riguarda le comunicazioni verbali, molte persone parlano a voce alta al telefono o tra di loro in luoghi pubblici, permettendo a estranei di ascoltare. Questo è il motivo per cui tra gli agenti di questa minaccia ci sono anche persone non malintenzionate.

11.21 Invio di dati a persone non autorizzate

Agenti di questa minaccia sono:

persone malintenzionate;

persone non malintenzionate.

Questa minaccia riguarda:

dati in formato elettronico;

dati in formato non elettronico (fax, stampe, lettere, eccetera);

dati comunicati via orale.

Per quanto riguarda i malintenzionati, l'invio di dati a persone non autorizzate è assimilabile alla copia di documenti in formato fisico o informatico.

Personale interno insoddisfatto potrebbe rendere pubblici documenti compromettenti per vendetta. Oggi è sempre più diffusa la diffamazione: diverse persone sono state condannate per aver diffamato la propria organizzazione su Internet pubblicando anche informazioni riservate⁶⁴.

Quando si parla di non malintenzionati, si possono distinguere due casi: errore personale e errore indotto da malintenzionato.

Un errore classico è l'invio di una email alla persona sbagliata (per esempio, la funzionalità di auto-completamento degli indirizzi di email dei programmi di posta elettronica potrebbe indurre un utente a inviare una email a Mario Rossi al posto di Mario Rossini). Il medesimo errore può avvenire anche con fax o posta tradizionale.

Tra gli esempi di questa minaccia, vi è il rapporto sul caso Calipari: esso presentava degli omissis ma, se opportunamente analizzato, diventavano visibili⁶⁵.

Altro esempio è fornito dagli inoltri di email da parte di chi non presta attenzione a tutto il testo che inoltra.

Esempio 11.21.1. Un cliente, chiedendo una dilazione del pagamento al proprio fornitore, ha inoltrato per errore un'email con i suggerimenti del proprio avvocato per evitare di pagare.

La dilazione non è poi stata accettata.

I file potrebbero essere condivisi con persone o programmi software sbagliati. È noto il caso di un consulente che aveva per errore condiviso una cartella di lavoro su un sistema pubblico di file sharing⁶⁶.

Molti mantengono attivi sistemi di messaggistica sul proprio computer quando stanno condividendo un documento o il proprio schermo con altri. Succede che l'altro, pur non volontariamente, a causa dei pop-up sullo schermo, venga a conoscenza di tutte le email e i messaggi ricevuti.

Alcuni dati sono diffusi per errore perché memorizzati come metadati, ossia nelle “proprietà” di un file o in altre aree di memoria non immediatamente visibili all’utilizzatore; spesso questi dati permettono di sapere quali sono altri clienti e fornitori della persona che ha inviato il documento. Anche le funzionalità di “revisione” dei documenti, per cui è possibile vederne le versioni precedenti, possono rivelare informazioni non previste.

Come già visto in precedenza, nel paragrafo 11.3, dei malintenzionati potrebbero

convincere una persona, con tecniche di social engineering, a fornire dei dati.

11.22 Invio e ricezione di dati non accurati

Agenti di questa minaccia sono:

persone malintenzionate;

persone non malintenzionate;

sistemi informatici.

Questa minaccia riguarda dati in formato elettronico e non elettronico.

Una persona potrebbe inserire per errore o deliberatamente dei dati o dei caratteri che interferiscono con i processi interni di un sistema (per esempio, un nome di un file con punti interrogativi può bloccare un sistema Windows).

I sistemi informatici possono essere progettati o sviluppati male e commettere errori di trasmissione e inviare a un sistema o utente dati scorretti e indurlo a sua volta in errore.

Esempio 11.22.1. I sistemi informatici possono essere progettati male anche volontariamente, come dimostrato dallo scandalo delle emissioni delle auto Volkswagen. Il software dei motori diesel modificava i dati in modo da

passare i test⁶⁷.

Questo attacco può anche essere innocuo, come quando le persone dichiarano un'età diversa da quella reale (qualche anno in più quando sono giovani, qualche anno in meno più tardi) oppure inventano nomi fasulli per registrarsi a servizi disponibili su Internet e mantenere l'anonimato.

In altri casi i dati scorretti possono richiedere rettifiche onerose, come nel caso delle “cartelle pazze”.

Questa minaccia è applicabile ai sistemi basati su intelligenza artificiale [21], sia involontariamente quando si usano dati non ottimali per l’addestramento, creando i cosiddetti pregiudizi o bias, sia volontariamente con gli attacchi oggi indicati come adversarial machine learning usando dati nocivi per l’addestramento o durante l’utilizzo del sistema.

Esempio 11.22.2. Nel 2016, Microsoft avviò su Twitter il profilo Tay: un programma di intelligenza artificiale che rispondeva gentilmente agli utenti. Fu chiuso dopo meno di 24 perché gli attaccanti riuscirono a insegnargli a rispondere con messaggi razzisti e sessisti⁶⁸.

11.23 Ripudio di invio di messaggi e documenti da parte del mittente

Agenti di questa minaccia sono persone malintenzionate.

Questa minaccia è facilmente comprensibile e può avere diverse ragioni: una persona che si pente dell'acquisto effettuato via web oppure un tentativo di frode di chi effettua l'acquisto di un servizio e, dopo averne usufruito, lo nega.

L'email non fornisce al mittente la certezza del recapito (il protocollo è inaffidabile) a meno che il destinatario non fornisca una ricevuta. Se si usano dei servizi non affidabili (inclusa la posta tradizionale), il ripudio di ricezione può anche essere fondato.

11.24 IoT, OT, IIOT

Gli oggetti digitali, anche se non usati prevalentemente per il trattamento di informazioni, possono essere comunque soggetti a minacce di tipo informatico.

Alcune di queste sono le medesime già trattate in precedenza:

intrusione nei sistemi informatici: in questo caso, l'attacco è facilitato dal fatto che i dispositivi non sono stati progettati con attenzione alla sicurezza (per esempio impongono l'uso di password semplici e non modificabili), non hanno incorporati strumenti per prevenire gli attacchi e anche il patching, in caso di vulnerabilità, è solitamente complicato;

danneggiamento di apparecchiature fisiche;

furto di apparecchiature informatiche o di impianti fisici: reso ancora più semplice dalla scarsa attenzione che si pone su questi oggetti;

lettura e copia non autorizzata di documenti informatici, ossia le informazioni

raccolte dal dispositivo; si pensi a una telecamera;

modifica di documenti informatici: in questo caso, la modifica riguarderebbe le configurazioni; nel caso di infrastrutture critiche, la conseguenza può essere il blocco dell'erogazione di energia elettrica, gas, acqua e riscaldamento;

malware;

recupero di informazioni;

esaurimento o riduzione delle risorse, anche attraverso attacchi DoS;

intercettazione delle comunicazioni, resa ancora più semplice da una progettazione inadeguata, che potrebbe non aver previsto l'attivazione di canali cifrati per le comunicazioni.

Ulteriori minacce a cui prestare attenzione, specifiche per questi dispositivi:

disconnessione dalla rete, che potrebbe portare al malfunzionamento del dispositivo (per esempio, succede spesso che gli allarmi antintrusione suonino dopo un certo periodo di assenza di connettività);

assenza di energia elettrica, per cui il dispositivo può non funzionare e quindi arrecare danni o inconvenienti (per esempio, in caso di blackout, l'accesso controllato da tastierino elettronico o badge non può funzionare e questo può avere pesanti impatti; altro esempio sono le tapparelle controllate da un sistema elettronico che, in assenza di alimentazione elettrica, non può più essere utilizzato per alzarle);

spegnimento o azzeramento manuale, deliberato o involontario, anche da parte di persone non autorizzate, se i pulsanti di spegnimento o di azzeramento sono facilmente accessibili;

ripristino e uso non autorizzato, spesso facilitato dal pulsante di ripristino della connessione di rete, fisicamente accessibile.

Si raccomanda, per approfondire i casi sopra generalizzati, la lettura di testi dedicati come, per esempio, [22].

11.25 Intelligenza artificiale

I sistemi di intelligenza artificiale sono soggetti a specifiche minacce relative a:

progettazione e addestramento;

utilizzo.

I sistemi di intelligenza artificiale, essendo essi stessi sistemi informatici, sono oggetto delle medesime minacce descritte precedentemente in questo capitolo e quindi non saranno qui trattate.

Per quanto riguarda la progettazione e addestramento, le minacce sono le seguenti:

presentazione di risultati non affidabili, a causa dei cosiddetti pregiudizi o bias, originati da sistemi di addestramento non ben bilanciati; questa minaccia è tanto più complessa, quanto è difficile ricostruire, in molti casi, l'esatto comportamento del sistema di intelligenza artificiale;

comportamenti inattesi, a causa dell'assenza di limiti al sistema; questi si manifestano in casi limite (per esempio, il mancato riconoscimento di banconote false o di cartelli stradali).

Durante l'utilizzo, invece, un sistema di intelligenza artificiale può essere avvelenato (poisoned) con dati scorretti da parte degli utilizzatori. L'effetto è sempre la presentazione di risultati non affidabili o inattesi. Solitamente l'attacco avviene da parte di malintenzionati, che costruiscono dati scorretti per alimentare e quindi compromettere il sistema.

Si raccomanda, per approfondire i casi sopra generalizzati, la lettura di testi dedicati come, per esempio, [21].

Note

³⁷www.veriscommunity.net.

³⁸cryptome.org/gummy.htm.

³⁹Speriamo sia una leggenda metropolitana.

⁴⁰www.ilpost.it/2016/10/24/attacco-informatico-venerdi-21-ottobre-mirai-dyn/.

⁴¹Per l'attacco a Solarwinds, vedere <https://arstechnica.com/information-technology/2020/12/russian-hackers-hit-us-government-using-widespread-supply-chain-attack/> e <https://www.schneier.com/blog/archives/2020/12/russias-solarwinds-attack.html>. Per l'attacco a Kaseya, vedere <https://www.wired.com/story/revil-ransomware-supply-chain-technique/>.

⁴²Le 50 peggiori password (in inglese) del 2019 si trovano alla pagina <https://teampassword.com/blog/top-50-worst-passwords-of-2019>.

⁴³nakedsecurity.sophos.com/2012/11/21/prince-william-photos-password; un caso simile è accaduto qualche tempo dopo, nel 2015: arstechnica.com/security/2015/04/hacked-french-network-exposed-its-own-passwords-during-tv-interview/.

⁴⁴Se poi il matrimonio va in crisi, si rischia di coinvolgere i tribunali: <https://notiziario.uspi.it/accede-con-la-password-al-profilo-facebook-della-moglie-la-cassazione-conferma-la-condanna-penale/>.

⁴⁵Purtroppo sono molti gli amministratori di sistema che abituano male gli utenti, come dimostrano alcune ricerche: www.achab.it/blog/index.cfm/2014/4/chiedere-la-password-in-modo-sicuro.htm.

⁴⁶Il phishing può avere impatti anche sull’impresa che offre il servizio web legittimo, come stabilito da una sentenza italiana: <http://www.altalex.com/documents/news/2014/08/19/phishing-poste-condannate-per-misure-di-sicurezza-non-adeguate>.

⁴⁷<https://www.ncsc.admin.ch/ncsc/it/home/cyberbedrohungen/ceo-betrug.html>.

⁴⁸<https://www.fbi.gov/scams-and-safety/common-scams-and-crimes>.

⁴⁹In questo caso, i malintenzionati sono riusciti addirittura a ottenere la firma digitale del malcapitato: www.ilsole24ore.com/art/notizie/2012-03-26/rubano-firma-digitale-intestano-181133.shtml.

⁵⁰<https://www.theguardian.com/politics/2020/oct/05/how-excel-may-have-caused-loss-of-16000-covid-tests-in-england>.

⁵¹I casi più noti riguardano i patch di Windows; questo è uno dei tanti: <https://threatpost.com/microsoft-windows-update-patch-tuesday/163981/>.

⁵²www.theregister.co.uk/2010/06/25/spanish_logic_bomb_probe.

⁵³<https://www.bleepingcomputer.com/news/security/thermanator-attack-steals-passwords-by-reading-thermal-residue-on-keyboards/>.

⁵⁴<https://www.bleepingcomputer.com/news/legal/engineer-found-guilty-of-stealing-navy-secrets-via-dropbox-account/>.

⁵⁵<https://www.altalex.com/documents/news/2011/01/05/non-commette-furto-chi-copia-i-files>.

⁵⁶www.startmag.it/innovazione/neuron-ecco-il-vero-bersaglio-dellattacco-hacker-a-leonardo/

⁵⁷Un programmatore scrisse “googleaspis” al posto di “googleapis” e creò non

pochi problemi: www.bbc.com/news/technology-26016802.

⁵⁸www.theregister.co.uk/2018/03/19/boom_cambidge_analytica_explodes_follow_extraordinary_tv_expose/.

⁵⁹<https://edition.cnn.com/2022/01/13/politics/cyberattacks-schools-new-mexico-ransomware/index.html>.

⁶⁰wwwansa.it/web/notizie/rubriche/cronaca/2013/02/16/Attacco-hacker-sito-tribunale-Milano_8259442.html.

⁶¹www.economist.com/news/business/21570754-read-and-win-million.

⁶²www.cyberscoop.com/verizon-wireless-s3-bucket-public-access-kromtech/;
www.darkreading.com/application-security/git-some-security-locking-down-github-hygiene/d/d-id/1330511.

⁶³Il caso PRISM e NSA del 2013 sul Washington Post: tinyurl.com/mm3ttqt.

⁶⁴<http://www.mirror.co.uk/news/uk-news/exclusive-marks-spencer-staff-370491>.

⁶⁵La notizia poteva essere divertente, non fosse stata collegata a un episodio tragico: punto-informatico.it/1209009/PI/News/rapporto-calipari-un-pdf-rivela-omissis.aspx.

⁶⁶www.techdirt.com/articles/20050623/0251255.shtml.

⁶⁷www.bbc.com/news/business-34324772.

⁶⁸<https://knowyourmeme.com/memes/sites/tay-ai>.

Capitolo 12

I controlli di sicurezza

*Bisogna saper scegliere in tempo,
non arrivarsi per contrarietà.*

Francesco Guccini, Eskimo

I controlli di sicurezza delle informazioni sono spesso indicati come misure di sicurezza delle informazioni o, più brevemente, misure o contromisure. Il termine meccanismo di sicurezza è talvolta qui usato per indicare i controlli tecnologici.

È opportuno leggere la definizione fornita dalla ISO/IEC 27000.

Controllo: misura che modifica il rischio.

Nota 1: I controlli includono processi, politiche, dispositivi, pratiche o altre azioni che modificano il rischio.

Nota 2: I controlli non sempre potrebbero ottenere l'effetto atteso o previsto di modifica del rischio.

Considerazioni in merito alle diverse tipologie di controlli (preventivi, di

recupero e di rilevazione) e alle loro relazioni (alternativi, compensativi, complementari e correlati) si trovano nel paragrafo 6.7.

Lo standard internazionale che descrive i controlli di sicurezza è la ISO/IEC 27002. I suoi controlli sono riportati anche nell'Appendice A della ISO/IEC 27001. L'edizione del 2022 dello standard categorizza i controlli in 4 temi:

- organizzativi (Organizational controls);
- relativi alle singole persone (People controls);
- di sicurezza fisica (Physical controls);
- tecnologici (Technological controls).

Una notevole novità dell'edizione del 2022 della ISO/IEC 27002 è rappresentata dagli attributi, che possono essere usati per etichettare i controlli. L'idea è quella di permettere agli utilizzatori di riordinare e raggruppare i controlli secondo viste, in accordo alle proprie specifiche esigenze. Se controlli ed etichette sono riportati su fogli di calcolo o database, come sempre più spesso succede, queste viste permettono di personalizzare il raggruppamento dei controlli.

Lo standard presenta alcuni esempi di attributi, tra cui quelli basati su:

- tipologia di controllo: preventivo, di rilevazione, correttivo;
- proprietà di sicurezza: riservatezza, integrità, disponibilità;
- concetti di sicurezza cyber: identificare, proteggere, rilevare, rispondere, ripristinare.

Un altro esempio ripropone un raggruppamento simile a quello dell’edizione del 2013 della ISO/IEC 27002 [85]: governo, gestione degli asset, sicurezza del personale, sicurezza fisica, eccetera.

In questo libro i controlli sono suddivisi proprio secondo questo schema, anche se con alcune eccezioni, come per esempio il paragrafo 12.1 sulla documentazione. Le relazioni tra i controlli della ISO/IEC 27002:2022 e i paragrafi di questo libro sono riportati in appendice G.

Per ovvi motivi di diritti di autore, non sono copiati i contenuti della norma, di cui si raccomanda la lettura.

12.1 Documenti

Per garantire la sicurezza delle informazioni vanno fornite al personale regole e istruzioni su come comportarsi, come trattare le informazioni e come gestire gli strumenti in uso.

Questo è importante soprattutto quando le attività:

sono svolte da più persone;

sono svolte raramente e, pertanto, il modo di procedere potrebbe essere dimenticato;

sono nuove e il personale necessita supporto per svolgerle in modo corretto.

Tali regole e istruzioni potrebbero essere date in forma orale. Questo però non ne garantirebbe la corretta comprensione, l'omogenea attuazione e il sistematico riesame periodico; è quindi necessario prevedere alcuni documenti scritti.

12.1.1 Tipi di documenti

Sono previsti tre tipi di documenti:

politiche, che danno le regole generali, oggetto del paragrafo 12.2;

procedure, a cui è dedicato il paragrafo 12.1.1.1;

registrazioni, a cui è dedicato il paragrafo 12.1.1.2.

Nel seguito, ogni volta che ricorre il termine “procedura” o “politica”, si sottintende il termine “documentata”.

12.1.1.1 Procedure

Molti controlli di sicurezza richiedono di seguire delle procedure. La definizione dalla ISO 27002 è la seguente.

Procedura: un modo specifico per effettuare un’attività o un processo.

Nota [dalla ISO 9000:2015]: Una procedura può essere documentata o no.

Nota [dalla ISO 9000:2005]: Quando una procedura è documentata, si usa frequentemente il termine procedura scritta o procedura documentata.

Le procedure documentate hanno la finalità di descrivere processi e attività in modo che il personale ne garantisca la ripetibilità seguendo le indicazioni riportate.

Le normative e gli standard riportano requisiti generali e quindi il personale non può essere chiamato a rispettarli così come sono; è compito dell'organizzazione stabilire come applicarli e descriverlo in politiche e procedure interne a cui il personale deve attenersi.

Esempio 12.1.1. Secondo alcune normative e standard, i supporti di memorizzazione contenenti dati di elevata riservatezza dovrebbero essere cancellati in modo sicuro. L'organizzazione deve quindi stabilire quale strumento utilizzare a questo scopo e come deve essere configurato e riportarlo per iscritto in una procedura.

Un altro esempio riguarda il processo di assegnazione delle autorizzazioni agli accessi alle informazioni. Come indicato nel paragrafo 12.6.3.1, sono molte le alternative percorribili e la normativa e gli standard non ne impongono alcuna. Per questo è necessario stabilire un processo e, tranne che nelle organizzazioni molto piccole, è preferibile documentarlo riportando i canali di comunicazione tra le varie funzioni, chi può chiedere di modificare le autorizzazioni e chi può modificarle tecnicamente.

Purtroppo le procedure sono spesso ritenute astratte, inefficienti, inefficaci, incomprensibili e, in definitiva, inutili. Questo perché sono viste come imposizione degli standard ISO e di altre normative, predisposte con l'obiettivo di dimostrare la conformità a qualche norma senza preoccuparsi della loro applicabilità e leggibilità, scritte e verificate da operatori, consulenti e auditor più attenti alla forma che alla sostanza.

Per questo, per indicare dei documenti più operativi (e più utili), alcuni usano i termini istruzioni o standard interni. In questo libro si preferisce usare il termine procedura anche per questi documenti.

In molti accusano la cultura italiana quando il personale non segue le procedure. Questo non è vero: ci sono organizzazioni anglosassoni dove avviene lo stesso. L'accusare una generica "cultura italiana" è una scusa per non ammettere di avere procedure complicate, lacunose e la cui attuazione non interessa né al personale né alla Direzione.

Un errore comune è quello di realizzare la documentazione per il solo sistema di gestione per la sicurezza delle informazioni, indipendente dalle altre necessità dell'organizzazione. Per esempio si realizzano più procedure per la gestione degli acquisti, ciascuna relativa a un sistema di gestione (qualità, sicurezza delle informazioni, ambiente, eccetera) o normativa applicabile (privacy, diritto d'autore, eccetera). Questo comporta spreco di risorse, confusione nel personale e disallineamenti tra i diversi requisiti. È quindi più opportuno avere un'unica procedura relativa a un determinato processo che riporti tutti i requisiti pertinenti.

Le procedure devono specificare quali attività registrare e come registrarle, indicando quali moduli o programmi software utilizzare.

Esempio 12.1.2. Il processo di gestione degli acquisti prevede la registrazione delle richieste di acquisto, delle offerte ricevute dai potenziali fornitori, degli ordini emessi, delle fatture ricevute e dei pagamenti.

Quando una procedura non è documentata, si usa anche il termine prassi.

Il termine linee guida fa riferimento a documenti le cui indicazioni, a differenza delle procedure, non sono da attuare obbligatoriamente.

12.1.1.2 Registrazioni

Ulteriori documenti importanti per un'organizzazione sono le registrazioni, la cui definizione dalla ISO 9000:2015 è la seguente.

Registrazione: documento che riporta i risultati ottenuti o fornisce evidenza delle attività svolte.

Le registrazioni possono essere di due tipi:

registrazioni con approvazione;

registrazioni senza approvazione.

Esempio 12.1.3. Sono registrazioni con approvazione:

il verbale di una riunione, perché approvato dei suoi partecipanti;
un rapporto di audit, perché, prima della sua distribuzione, approvato dal suo esecutore e dal suo committente;
i documenti dove sono definiti i requisiti di un determinato sistema informatico perché approvato dai partecipanti all’analisi.

Sono registrazioni senza approvazione: il registro delle entrate e delle uscite da un edificio, i log informatici e le registrazioni di videosorveglianza.

Alcune registrazioni, come i verbali o i documenti di specifiche tecniche, riportano attività da fare o requisiti da rispettare e assumono quindi una funzione simile a quella delle procedure.

Le registrazioni sono utili per:

l’organizzazione in caso di contestazioni da parte di clienti o fornitori;
il coordinamento tra le varie persone coinvolte nelle attività;
il passaggio di consegne tra diverse persone o funzioni dell’organizzazione (per esempio, quando un software passa in gestione dagli sviluppatori a chi lo gestisce negli ambienti di produzione) o tra le varie parti interessate (organizzazione, clienti, fornitori e partner);
l’elaborazione di report utili per l’analisi delle tendenze;

una migliore pianificazione delle attività.

Alcuni richiedono molte registrazioni su moduli estremamente complessi perché “richiesto dalla norma”, ma non è sempre vero. Occorre ricordare che troppe registrazioni e moduli complessi sono dannosi perché non vengono correttamente utilizzati dalle persone.

12.1.2 Come scrivere i documenti

L’organizzazione deve stabilire quali documenti (politiche, procedure e registrazioni) sono necessari. Essi devono:

essere identificabili, per esempio con un titolo o un codice;

riportare, quando opportuno, chi li ha scritti e chi li ha approvati;

riportare la data o la versione in modo che sia chiara la versione in vigore di una politica o procedura e la data di aggiornamento di una registrazione;

essere scritti in una lingua e forma comprensibili ai loro destinatari;

essere in formato cartaceo o digitale e, nel caso siano in formato digitale, essere accessibili e modificabili con programmi software disponibili a chi deve accedervi.

Le procedure e le politiche documentate devono essere chiare, precise, sintetiche e semplici. Non devono essere prodotti di alta letteratura, nonostante alcuni redattori abbiano velleità artistiche: le istruzioni di IKEA, anche se costituite soprattutto da disegni, e alcuni libri di ricette sono ottimi esempi di come scrivere procedure.

Suggerimenti per la scrittura di politiche e procedure sono disponibili in diverse pubblicazioni [125, 126, 132]. I più comuni sono:

impostare uno stile grafico semplice, economico (nel senso di utilizzare pochi tipi di caratteri, colori ed effetti) e uniforme;

usare parole semplici e periodi brevi, senza scadere nella neo-lingua di Orwell o sue varianti, purtroppo molto diffuse e basate su termini inglesi o gergali usati a sproposito⁶⁹;

prediligere la forma attiva dei verbi e frasi positive;

ripetere i termini senza paura;

usare preferibilmente le lettere minuscole perché più leggibili e meno aggressive;

dare più importanza alle regole che alle loro giustificazioni (ossia, iniziare un documento riportando le regole da seguire e poi, in sintesi, le giustificazioni; non l'inverso, come spesso avviene).

Per ogni attività descritta in una procedura vanno chiaramente indicati:

quando o per quali ragioni va iniziata;

i ruoli che la devono svolgere;

a chi vanno indirizzati i risultati delle attività e le comunicazioni significative.

Le politiche e le procedure, anche per non appesantirne la lettura, non devono riportare necessariamente i riferimenti alla normativa o agli standard di

riferimento come la ISO/IEC 27001 e tantomeno ai loro singoli requisiti. Si consiglia l'inverso: indicare su un documento a parte, per ciascuna normativa o standard, e solo quando è utile, le procedure che riportano come vengono soddisfatti i requisiti.

12.1.3 Approvazione e distribuzione

Bisogna stabilire chi può approvare le politiche, le procedure e le registrazioni e chi le può pubblicare.

L'approvazione non deve essere necessariamente fatta con firma autografa sulla copertina del documento. In molti casi, la pubblicazione di un documento ne sottintende l'approvazione.

È importante osservare che i documenti possono essere approvati da diverse funzioni dell'organizzazione.

Esempio 12.1.4. La politica per la sicurezza delle informazioni (paragrafo 12.2) deve essere approvata dalla Direzione, mentre alcune procedure possono essere approvate da altri livelli gerarchici.

In alcune organizzazioni, determinate procedure applicabili a più aree devono essere approvate dal responsabile della sicurezza delle informazioni, oppure da tutti i responsabili di funzione coinvolti dalla procedura stessa. Viceversa, le procedure applicabili a una singola area dell'organizzazione possono essere approvate dal solo responsabile di quell'area.

Le modalità di pubblicazione delle politiche e procedure possono riflettere queste scelte e, per esempio, le procedure con impatto su più aree sono pubblicate su un sistema accessibile a tutto il personale dell’organizzazione, mentre quelle specifiche per un’area sono pubblicate su sistemi ad accesso più limitato.

Le regole di approvazione e pubblicazione dei documenti vanno a loro volta riportate in una politica o procedura, fondamentale per evitare una proliferazione incontrollata di regole e procedure, con possibili conflitti tra loro e pubblicate da persone non autorizzate.

Le politiche e le procedure vanno comunicate a tutto il personale interno, incluso quello temporaneo, secondo le loro mansioni; alcune ai fornitori, ai clienti e agli altri partner, quando pertinenti alle attività commissionate e agli accordi e contratti stipulati.

Vanno stabilite le modalità con cui il personale e le altre parti interessate devono essere avvise degli aggiornamenti, per esempio via email.

In molte organizzazioni, le politiche e le procedure sono pubblicate con l’ausilio di sistemi informatici. Nei casi più semplici si usano siti web o partizioni di un file server accessibili solo da personale autorizzato e modificabili da alcune specifiche persone; in casi più complessi si usano sistemi di document management che permettono a ciascuno di redigere un documento, di classificarlo, di chiederne l’approvazione e quindi di pubblicarlo.

Bisogna prestare attenzione alle versioni obsolete di procedure e moduli: molti

usano delle versioni archiviate sul proprio PC e non le aggiornano con le nuove versioni, oppure copiano e incollano moduli compilati in precedenza senza verificare se sono ancora in vigore.

12.1.4 Archiviazione delle registrazioni

L'organizzazione deve stabilire le modalità di archiviazione delle registrazioni. È infatti importante che siano conservate in archivi condivisi da più persone, per evitare difficoltà in caso di assenze o uscite. Vanno quindi stabilite regole che indichino quali archivi fisici o informatici usare.

L'archiviazione deve assicurare un adeguato livello di sicurezza delle registrazioni. Per esempio, le registrazioni relative alla valutazione del rischio vanno tenute riservate, in quanto riportano vulnerabilità o carenze di sicurezza. Vanno quindi applicati opportuni controlli di sicurezza, soprattutto di controllo degli accessi (paragrafo 12.6 e sugli scambi di informazioni (paragrafo 12.10.4).

Sono frequenti i casi in cui le registrazioni sono archiviate nelle caselle personali di email. Questa pratica va scoraggiata perché le caselle di email non sono sistemi di archiviazione e conservazione di documenti, né permettono ad altri di accedervi.

È peraltro interessante notare che, nei tempi passati, ogni documento importante veniva depositato ordinatamente in faldoni e archivi, mentre l'uso dell'email sembra aver reso obsoleto questo sistema, anche se facilmente attuabile in ambito informatico.

Esempio 12.1.5. Un consulente aveva concordato con il cliente modifiche al progetto rispetto a quanto stabilito nell'offerta. Dopo un certo tempo, sia il consulente sia il referente del cliente diedero le dimissioni.

Il nuovo referente del cliente, non trovando corrispondenza tra quanto riportato nell'ordine di lavoro e quanto consegnato dalla società di consulenza, chiese spiegazioni al nuovo consulente, incaricato dalla medesima società di consulenza del primo.

Ovviamente non fu trovato alcun documento che potesse aiutare i due interlocutori a capire cosa fosse successo e la società di consulenza dovette riprendere il lavoro da capo, rimettendoci soldi e credibilità presso il cliente.

Il primo consulente, contattato tempo dopo, disse: “Forse ci eravamo scambiati qualche email da cui si poteva capire quanto deciso, ma credo sia molto difficile da reperire dopo tutto questo tempo”.

Oggi, dopo alcune esperienze spiacevoli, alcune organizzazioni hanno introdotto metodi di archiviazione basati su sistemi di document management, anche se non sempre efficienti. In alcuni casi è sufficiente un attento uso di un file server, accompagnato da regole precise di archiviazione e di denominazione di file.

Per la documentazione con valore legale, in Italia si dovrebbero considerare i sistemi di conservazione a norma regolamentati dal Codice dell'amministrazione digitale (paragrafo 12.15.1.8).

12.1.5 Tempo di conservazione

Bisogna fissare i tempi di conservazione di ciascuna politica, procedura e registrazione.

Per le politiche e le procedure, al fine di giustificare azioni intraprese in passato, può essere utile conservare le versioni precedenti per almeno due anni.

Per la conservazione dei documenti, vedere anche il paragrafo 12.5.1.8.

12.1.6 Verifica e manutenzione dei documenti

Per verificarne l'adeguatezza e, se il caso, aggiornarle, le politiche e le procedure vanno riesaminate periodicamente (almeno una volta all'anno) e ogni volta che si attuano modifiche organizzative o tecnologiche rilevanti.

12.1.7 Documenti di origine esterna

Caso particolare di documenti sono quelli di origine esterna come, per esempio, le specifiche dei clienti o la normativa vigente (paragrafo 12.15.1).

Queste informazioni devono essere opportunamente riconosciute come pertinenti e conservate e gestite secondo principi simili a quelli sopra riportati e deve essere verificato periodicamente se sono aggiornate rispetto alle ultime versioni pubblicate.

12.2 Politiche di sicurezza delle informazioni

Per la formulazione dei principi di sicurezza, si usa il termine politica, di cui segue la definizione della ISO/IEC 27000.

Politica: intenzioni e indirizzi di un’organizzazione espressi formalmente da parte della Direzione.

Il termine “politica” (in inglese policy) può creare confusione con la politica (politics) fatta di elezioni, dibattiti parlamentari e prime pagine dei giornali. Fortunatamente, quest’ultima non è oggetto di questo libro. In alcuni casi, al posto di politiche, si usano i termini regole, principi o norme, sicuramente più intuitivi e corretti.

Vi sono due tipi di politiche: quelle generali (per esempio, la “politica per la sicurezza delle informazioni”) e quelle specifiche per un determinato argomento, dette politiche specifiche (topic-specific policies).

La politica generale è un documento fondamentale per la sicurezza delle informazioni e deve riportare:

cosa si intende per “sicurezza delle informazioni”, perché è importante per l’organizzazione, cosa è più e cosa è meno importante;

quali sono i principi generali da seguire, incluso l’impegno a rispettare i requisiti legali e quelli dei clienti in materia di sicurezza delle informazioni e l’impegno a migliorare continuamente la sicurezza delle informazioni;

come sono state assegnate le responsabilità a più alto livello.

Essa deve essere approvata ed emessa dalla Direzione dell'organizzazione e riesaminata regolarmente.

Esempio 12.2.1. Un semplice esempio è riportato di seguito:

Politica per la sicurezza delle informazioni - Azienda x

La nostra azienda offre servizi informatici ai propri clienti, appartenenti a tutti i settori di mercato, pubblico e privato. Trattiamo quindi dati pubblici e riservati, dati anonimi, personali comuni o sensibili, dati anche ad alta criticità.

Data la potenziale criticità dei dati trattati, in qualunque formato essi siano (informatico e non), è fondamentale che sia loro garantita la massima sicurezza. Questo si traduce nella salvaguardia della loro riservatezza in particolare e anche della loro integrità e disponibilità.

I livelli di sicurezza da garantire devono essere tali da rispettare le clausole contrattuali e la normativa vigente, nonché da garantire la coerenza e il bilanciamento tra: rischio di impresa, sostenibilità economica, risultati delle analisi e valutazioni del rischio, politiche e strategie aziendali, politiche e strategie dei fornitori e dei clienti, necessità di costante adeguamento al contesto in cui operiamo e di miglioramento dell'efficacia ed efficienza dei nostri processi e controlli di sicurezza.

I principi cardine a cui attenersi sono:

le informazioni devono essere accessibili solo a coloro che ne hanno necessità (principio need to know) e nei tempi stabiliti;

il personale deve essere opportunamente formato in materia di sicurezza delle informazioni e deve seguire i principi etici e comportamentali prescritti;

i fornitori devono essere opportunamente tenuti sotto controllo attraverso misure da stabilire a seconda dei casi;

i partner devono essere selezionati anche per la loro capacità e disponibilità a conformarsi alle nostre regole di sicurezza;

per i servizi erogati, è necessario considerare i requisiti di sicurezza sin dalla contrattazione con il cliente.

La responsabilità finale della sicurezza delle informazioni ricade sulla Direzione che ha delegato i responsabili delle divisioni interne ad attuare quanto necessario, in accordo con il responsabile dei sistemi IT, il responsabile della logistica e il direttore del personale.

Questa politica è comunicata a tutto il personale attraverso l'affissione in bacheca e la intranet e alle parti interessate attraverso la pubblicazione sul nostro sito web.

Un documento di questo tipo, come è facile intuire, può essere contenuto in una pagina. È compito della Direzione approvarlo e riesaminarlo almeno annualmente per stabilire se aggiornarlo a causa dei cambiamenti del contesto in cui opera l'organizzazione o delle sue strategie.

Le politiche specifiche possono essere espresse in poche righe e devono riportare le responsabilità corrispondenti.

Esempio 12.2.2. Una politica sull'antivirus è la seguente.

Politica relativa all'uso dell'antivirus

Su ogni PC e server collegato alla rete aziendale e su ogni dispositivo informatico utilizzato per accedere ai dati dell'azienda deve essere installato un antivirus tenuto aggiornato in modo automatico. Ogni eccezione deve essere documentata e approvata dal Responsabile per la sicurezza informatica.

Ogni trasmissione di dati, dove pertinente, deve essere controllata per verificare l'assenza di virus. È responsabilità dell'IT configurare opportunamente i PC e i server; è responsabilità di ogni utente non modificare le configurazioni predefinite e avvisare il service desk in caso di anomalie.

Quando l'antivirus rileva del malware, gli utenti devono richiederne la rimozione e, se ciò non fosse possibile, avvisare il Security operation center al numero interno 634.5789.

Alcune organizzazioni hanno raccolto la politica generale e tutte le politiche specifiche in un unico documento di meno di 20 pagine, rimandando, dove opportuno, a procedure di maggior dettaglio (qualcuno ha paragonato questo

documento alla Costituzione da cui poi devono discendere le leggi). Altre hanno pubblicato la politica generale in un documento a sé stante e le politiche specifiche nell'introduzione delle procedure pertinenti.

I destinatari devono confermare la ricezione delle politiche. Per esempio attraverso una ricevuta di ritorno all'email con cui i documenti sono stati inviati, i log di accesso alla cartella condivisa, la partecipazione a una sessione di presentazione delle politiche o anche una conferma verbale. Queste sono però soluzioni formali e spesso inefficaci. Buone sessioni di sensibilizzazione e l'impegno visibile da parte della Direzione e dei primi riporti sono un approccio migliore per comunicare le politiche e i loro aggiornamenti.

12.3 Organizzazione per la sicurezza delle informazioni

Uno dei principi di organizzazione aziendale richiede di assegnare esplicitamente le responsabilità per ciascuna attività e processo. Le responsabilità possono essere assegnate a singole persone o a funzioni dell'organizzazione.

Le responsabilità di livello strategico e tattico devono essere riportate nella politica generale per la sicurezza delle informazioni e rese evidenti nell'organigramma. Le responsabilità operative possono essere riportate nelle procedure pertinenti o in un mansionario.

12.3.1 Organizzazione

In questo paragrafo sono descritti i ruoli più importanti per la sicurezza delle informazioni e da prevedere in ogni organizzazione.

12.3.1.1 La Direzione

Come sempre, è opportuno riportare la definizione della ISO/IEC 27000.

Direzione [con la “D” maiuscola, o alta direzione o top management]: persona o gruppo di persone che dirigono e tengono sotto controllo un’organizzazione al più alto livello.

Nota 1: La Direzione ha il potere di delegare parte della sua autorità e fornire risorse all’interno dell’organizzazione.

Nota 2: Se l’ambito di applicazione del sistema di gestione riguarda solo una parte di un’organizzazione, allora si intende con Direzione coloro che dirigono e tengono sotto controllo quella parte dell’organizzazione.

La Direzione ha la responsabilità ultima della sicurezza delle informazioni, così come di tutto il resto. Essa deve stabilire le politiche di sicurezza delle informazioni, assegnare le responsabilità di primo livello alle persone più adeguate, effettuare o far effettuare verifiche sulla corretta attuazione delle disposizioni date, dare l’esempio e fornire le risorse necessarie a garantire l’efficacia del sistema di gestione per la sicurezza delle informazioni.

Purtroppo ci sono molti casi in cui la Direzione si disinteressa della sicurezza delle informazioni e delega tutto a consulenti o funzionari di medio livello. A volte, addirittura, la Direzione non si preoccupa neanche di dare il buon esempio, pretendendo di derogare dalle procedure per ogni attività in cui è coinvolta.

Esempio 12.3.1. Il responsabile della sicurezza di un grande gruppo italiano, pochi giorni dopo la nomina, decise di visitare una sede e si presentò all'ingresso del parcheggio con la propria macchina. La guardia, non riconoscendolo a causa della recente nomina, gli chiese un documento di identità prima di consentirgli l'accesso.

Raccontano che il dirigente si arrabbiò, malgrado la guardia abbia svolto correttamente il proprio dovere secondo le istruzioni ricevute.

La continua richiesta di deroghe da parte della Direzione e dei dirigenti ha come risultato l'aumento della disattenzione nei confronti delle misure di sicurezza visto che i primi a non ritenerle utili sono proprio coloro che le hanno stabilite.

Governance e management

Molti testi distinguono tra governance e management, dove la governance si occupa di attività direzionali e di fornire politiche e linee guida, mentre il management si occupa di garantire operativamente il loro rispetto. La Direzione è la prima responsabile della governance e deve stabilire i ruoli e le responsabilità per le attività di management.

In molti casi, chi si occupa di governance fornisce politiche e linee guida senza curarsi del loro impatto sull'organizzazione. Dovrebbe invece coinvolgere i livelli operativi prima di pubblicarle, in modo da valutarne l'impatto sulle loro attività, e presidiarne l'attuazione in modo da raccogliere informazioni utili per migliorarle e renderle più efficaci. Da tenere presente che alcuni potrebbero

approfittare di questo approccio più prudente per sollevare costantemente eccezioni e quindi rallentare le decisioni ed evitare la pubblicazione di regole non apprezzate.

In molte realtà, la governance è delegata a diverse funzioni. Ciò non esime la Direzione dalle proprie responsabilità di dare indirizzi strategici, essere di esempio e fornire le risorse necessarie. Anche i messaggi di sensibilizzazione o le comunicazioni al personale, seppure inviati operativamente da altre funzioni (per esempio, l’Ufficio del personale), devono essere promossi e approvati dalla Direzione.

12.3.1.2 Il responsabile della sicurezza e il DPO

La norma ISO/IEC 27001 non richiede la presenza di un Responsabile per la sicurezza delle informazioni, dato che la responsabilità ultima per la sicurezza delle informazioni è della Direzione.

Molti promuovono la presenza di questo ruolo, soprattutto in organizzazioni complesse, dove è necessario avere una figura dedicata alla sicurezza delle informazioni, in staff all’Amministratore delegato o al Direttore generale e con adeguato potere e risorse in modo da poter coordinare efficacemente le funzioni coinvolte nella sicurezza delle informazioni (informatica, sicurezza fisica, gestione del personale, eccetera).

In alcune organizzazioni è presente un Responsabile della sicurezza, spesso con esperienza nelle forze dell’ordine, il cui compito non riguarda solo la sicurezza delle informazioni, ma anche quello delle persone e dell’immagine. Affinché non sottovaluti la sicurezza delle informazioni, dovrebbe avere in staff una persona dedicata a questo argomento.

Considerando quanto previsto dal Regolamento europeo in materia di privacy (paragrafo 12.15.1.9), ulteriore figura da prevedere è il Data protection officer o DPO o, in italiano, Responsabile della protezione dei dati personali. Questa figura, non sempre obbligatoria, può coincidere con il Responsabile per la sicurezza delle informazioni.

Questo approccio è comunque sconsigliato perché i due ruoli hanno obiettivi diversi e potenzialmente in conflitto tra loro: il DPO dovrebbe occuparsi primariamente dei diritti degli interessati, mentre il Responsabile per la sicurezza delle informazioni della protezione dell'organizzazione. Inoltre per il Responsabile per la sicurezza delle informazioni, a differenza che per il DPO, non è richiesta l'indipendenza dalla Direzione.

12.3.1.3 Gli amministratori di sistema

Gli amministratori di sistema sono le persone addette alla configurazione e manutenzione dei sistemi informatici e dei meccanismi tecnologici di sicurezza fisica, inclusi quelli di monitoraggio della rete informatica, di esecuzione dei backup, di rilevazione dei virus informatici, di controllo degli accessi informatici, di controllo degli accessi fisici (per esempio, bussole e badge) e di segnalazione delle intrusioni informatiche e fisiche.

Questi soggetti sono particolarmente critici perché possono attaccare in modo molto efficace l'organizzazione e possono commettere errori involontari con impatti considerevoli. Per questo motivo è necessario identificarli in modo chiaro per ciascun ambito (vedere il paragrafo 12.6.3.4).

12.3.1.4 Altri ruoli e responsabilità

Alcuni ruoli di primo livello, importanti per la sicurezza delle informazioni e da avere chiaramente visibili sull'organigramma, riguardano i responsabili di: sistemi e reti IT (infrastruttura informatica), sviluppo dei programmi informatici, gestione del personale, acquisti, logistica e sicurezza fisica, audit interni.

Esempio 12.3.2. Un reparto IT può essere diviso in diverse sotto-aree:

rete, responsabile degli apparati di rete, del cablaggio di rete e delle connessioni a Internet;

sistemi, responsabile dell'hardware e dei sistemi operativi dei server;

database e storage;

desktop, responsabile dei PC fissi e portatili utilizzati dal personale, delle stampanti, dei fax, della telefonia VOIP, dei dispositivi portatili, eccetera;

applicazioni, responsabile dello sviluppo e della manutenzione delle applicazioni utilizzate dal personale non del reparto IT e dei software a loro supporto.

12.3.1.5 Coordinamento

I vari ruoli devono coordinarsi tra loro e a tal fine vanno istituite commissioni da riunire periodicamente per: analizzare eventi o incidenti occorsi dopo la riunione precedente, riesaminare l'avanzamento delle attività concordate in precedenza e stabilire come recepire le variazioni normative e migliorare i processi, le procedure e le misure di sicurezza con impatto su più funzioni. Ciascun partecipante deve informare gli altri su iniziative e progetti programmati dalla

propria funzione e che potrebbero avere impatti sulle altre.

Gli incontri di coordinamento possono essere molto brevi se non ci sono casi particolari all'ordine del giorno.

Alcune di queste commissioni possono essere:

quella composta dai responsabili dell'infrastruttura informatica e degli sviluppi applicativi per discutere sugli incidenti e sui cambiamenti infrastrutturali o applicativi previsti e in corso;

quella composta dai responsabili dell'infrastruttura informatica e della sicurezza fisica per discutere sugli incidenti e sui cambiamenti futuri o in corso relativi agli impianti e all'hardware.

Una commissione composta dai dirigenti di più alto livello è anche chiamata forum per la sicurezza delle informazioni. È importante osservare che, se questo non include tra i suoi membri la Direzione, non può assumerne le responsabilità.

Al termine di ogni incontro deve essere scritto e condiviso un breve resoconto di quanto discusso, in modo da confermare e non dimenticare le cose dette. Purtroppo, molti lo ritengono inutile, anche se tutti hanno sperimentato malumori e incomprensioni perché qualcuno si è dimenticato, o ha fatto finta di dimenticare, gli impegni presi verbalmente in riunione.

12.3.2 Separazione dei ruoli

Quando si assegnano ruoli e responsabilità, a qualunque livello, bisogna evitare i possibili abusi, volontari o involontari, dei poteri: a questo mira la separazione dei compiti.

Una prima regola: se sono istituiti dei controlli, la persona controllata non può assumere il ruolo di controllore delle proprie attività. Esempi sono:

nelle agenzie bancarie, alcune operazioni devono essere approvate dal direttore, purché non siano state avviate da lui stesso;

nei cinema, il biglietto venduto dal cassiere deve essere verificato dalla maschera in modo che il primo non incassi senza emettere il biglietto;

nei supermercati, gli errori di battitura alle casse possono essere corretti solo dai supervisori, i quali non possono ricoprire il ruolo di cassiere;

gli auditor devono essere indipendenti dalle attività verificate.

Un'altra regola prevede l'autorizzazione di operazioni molto critiche da parte di almeno due persone distinte e identificate chiaramente. Alcuni esempi:

nelle banche, per l'apertura delle cassette di sicurezza, è richiesta la presenza del titolare e di un rappresentante della banca, ciascuno con la propria chiave;

per alcuni sistemi crittografici (per esempio, gli HSM delle PKI), la configurazione può essere avviata solo in presenza di due referenti, ciascuno con la propria smart card e la propria password per accedere al sistema.

Per autorizzazioni ancora più critiche è necessario prevedere l'autorizzazione di almeno tre persone.

Un’ultima regola prevede di separare delle funzioni, in modo che alcuni obiettivi non siano ignorati in favore di altri. Nell’ambito della sicurezza delle informazioni, separazioni suggerite sono le seguenti, da attuare se le dimensioni dell’organizzazione sono adeguate:

le funzioni dedicate all’identificazione, progettazione e attuazione delle misure di sicurezza (informatiche e non informatiche) devono essere indipendenti dalle altre funzioni; questo per evitare che le scelte siano basate solo sul parametro dell’efficienza; idealmente, i responsabili della sicurezza e i responsabili della privacy dipendono direttamente dalla Direzione;

l’IT non deve dipendere da altre funzioni dell’organizzazione utilizzatrici dei sistemi informatici, perché queste tendono a privilegiare le funzionalità rispetto alla sicurezza;

gli amministratori dei database devono essere indipendenti dal restante personale dell’IT, per evitare che troppe persone abbiano accesso diretto ai dati e che la loro sicurezza non sia secondaria rispetto alle necessità di efficienza;

chi richiede e chi configura le autorizzazioni sui sistemi informatici devono essere persone distinte, in modo da prevenire errori e azioni illecite;

chi sviluppa le applicazioni deve essere indipendente da chi le mantiene e da chi le verifica perché, se tutto è in mano alle stesse persone, queste perdono l’abitudine di documentare quanto fatto e di effettuare i controlli e le verifiche previste;

chi sviluppa e mantiene le applicazioni deve essere indipendente da chi conduce i sistemi, per evitare che siano introdotti negli ambienti di produzione dei software non adeguatamente verificati.

Quando il personale è poco numeroso e non si possono assegnare ruoli distinti a persone diverse, devono essere attuate misure compensative. Per esempio, quasi tutti i sistemi informatici tracciano le operazioni effettuate dagli utenti (paragrafo

12.9.6.1); essi vanno quindi configurati affinché lo facciano per le attività più critiche e per le quali non vi è un’adeguata separazione dei ruoli.

Alcuni sistemi informatici prevedono di assegnare utenze distinte per ciascun ruolo. In questo modo, se una persona ricopre più ruoli, quando vuole cambiarlo deve sconnettersi e riconnettersi al sistema. Questo permette di evitare, tra gli altri, abusi involontari.

Da segnalare che il data protection officer (DPO) deve essere completamente indipendente dalla altre funzioni.

12.3.3 Gestione dei progetti

Il termine progetto indica un insieme di attività con termini di tempo e obiettivi definiti. Sono progetti: l’introduzione di un nuovo sistema informatico o servizio non informatico, l’apertura di una nuova sede, l’acquisizione di un ramo d’azienda, una riorganizzazione, un cambio di procedura e l’introduzione di una misura di sicurezza, come anche la modifica e la rimozione di sistemi informatici, servizi, sedi, rami d’azienda, procedure e misure di sicurezza. Il risultato di un progetto è spesso indicato con il termine prodotto, anche se si tratta di un servizio o di un’organizzazione.

La gestione dei progetti è una materia a sé stante [60, 105, 114] e quindi non è qui approfondita. Nel paragrafo 12.9.3 si parla della gestione dei cambiamenti ai sistemi informatici, i cui principi sono da applicare a tutti i progetti.

Ogni progetto prevede le seguenti fasi, importanti per la sicurezza delle informazioni:

pianificazione: all'avvio del progetto le attività sono pianificate e le responsabilità assegnate; i piani devono garantire la disponibilità di tempo e di risorse necessari alla determinazione dei requisiti del prodotto (inclusi quelli di sicurezza), al corretto sviluppo e alla verifica del prodotto;

definizione dei requisiti del prodotto: tutti i requisiti relativi alla sicurezza delle informazioni vanno considerati fin dall'inizio del progetto, anche a seguito di una valutazione del rischio del prodotto; è noto che in questo modo i prodotti sono realizzati più correttamente ed economicamente di quanto succede quando i requisiti di sicurezza sono stabiliti in un secondo tempo [14];

momenti di incontro (joint review) tra le parti interessate, anche nell'ambito dei coordinamenti periodici: per verificare che quanto realizzato sia in linea con i requisiti iniziali e le aspettative e i vincoli di ciascuno e per concordare eventuali ripianificazioni e modifiche dei requisiti con coloro che ne potrebbero subire gli impatti;

attività di verifica e test, inclusi quelli relativi alla sicurezza delle informazioni, come i vulnerability assessment e i penetration test (paragrafo 12.15.4).

Tra i requisiti di sicurezza da prevedere anche per i progetti non informatici sono descritti in questo capitolo e includono:

controllo degli accessi;

informare del cambiamento con un adeguato anticipo gli utilizzatori e le parti interessate;

tracciamento delle azioni, anche valutandone gli impatti con la privacy;

requisiti legali applicabili;

rapporti con le terze parti, inclusi clienti, fornitori e partner (contratti, monitoraggio).

12.3.4 Rapporti con le autorità

È necessario, soprattutto per organizzazioni di grandi dimensioni, costruire una rete di contatti con le forze dell'ordine e con le autorità. Questo non per ottenere trattamenti di favore, ma per meglio coordinare le attività quando necessario: cosa fare se i sistemi informatici sono attaccati, chi contattare in caso di intrusioni fisiche, mantenere gli aggiornamenti su normativa e standard pertinenti e gestire le crisi (paragrafo 12.13.5).

Per alcuni settori, come banche, assicurazioni, certificatori di firma digitale, fornitori di servizi di telecomunicazione, gestori di giochi d'azzardo e prestatori di servizi fiduciari, sono istituite autorità di vigilanza nazionale o sovranazionale, con le quali è opportuno mantenere buone relazioni.

La normativa sugli operatori di servizi essenziali, sui fornitori di servizi digitali e sul “perimetro di sicurezza nazionale cibernetica” (vedere 12.15.1.10) prevede che alcune organizzazioni (per esempio nel settore dei trasporti, dell'energia, della sanità, dei servizi digitali o dell'amministrazione pubblica) siano indicate da specifiche autorità (attualmente l'Agenzia per la cybersicurezza nazionale) come significative per la sicurezza informatica. Le autorità devono indicare le misure di sicurezza da attuare e ricevere notifiche sugli incidenti e pertanto è necessario che i soggetti “significativi” mantengano i rapporti con tali autorità.

Per le piccole organizzazioni è possibile limitarsi all'iscrizione a newsletter o alla consultazione periodica di siti web al fine di essere costantemente aggiornati in merito alla normativa applicabile e altri eventi pertinenti, previa valutazione dell'attendibilità della fonte.

Tutte le imprese dovrebbero avere dimestichezza con il sito web dell'autorità competente per la protezione dei dati personali⁷⁰ anche perché devono comunicarle le violazioni di dati personali trattati (vedere anche 12.15.1.9).

12.3.5 Monitoraggio delle minacce

Il monitoraggio delle minacce (threat intelligence) permette di raccogliere informazioni per prevenire, rilevare o affrontare minacce e attacchi.

È necessario identificare i canali di informazione da monitorare tra cui newsletter⁷¹, riviste, giornali e altri mezzi di comunicazione, oltre ai centri di risposta agli incidenti di sicurezza (si segnala in particolare il CSIRT italiano⁷²). Anche i casi di cronaca come quelli presentati all'inizio del capitolo 2 possono aiutare a identificare delle minacce precedentemente non identificate.

Esempio 12.3.3. Nell'aprile 2011, alcuni servizi informatici di Aruba rimasero indisponibili per un incendio originato dal sistema UPS⁷³.

A seguito di questo evento, molte organizzazioni avviarono programmi di verifica per evitare di incorrere nello stesso problema.

Le informazioni vanno poi incrociate con gli inventari degli asset per verificare, in ambito informatico, se la segnalazione è applicabile ai sistemi gestiti e il loro livello di criticità ed esposizione (se per esempio si tratta di sistemi di produzione o esposti su Internet).

Vanno quindi stabilite le responsabilità e i processi per poter utilizzare in modo efficace le informazioni quando si valuta il rischio, si configurano i meccanismi di sicurezza (come, per esempio, i firewall) e si eseguono test di sicurezza (vedere paragrafo 12.15.4).

12.4 Gestione del personale

Il termine risorse umane è ormai molto diffuso per indicare il personale, ma in questo libro, come anche nella ISO/IEC 27002, si preferisce parlare di persone e non di risorse.

Quando si parla di sicurezza delle informazioni, bisogna includere nel “personale”: dipendenti, consulenti, collaboratori temporanei e stagisti.

12.4.1 Inserimento del personale

12.4.1.1 Selezione del personale

Prima di inserire qualcuno nell’organizzazione bisogna verificare se le competenze dichiarate dal candidato corrispondano a quelle effettive richiedendo copie dei certificati di studio e professionali.

Molte volte le persone scelte non hanno tutte le competenze auspicate. In questi casi, bisogna pianificare la formazione necessaria.

In Italia, tranne in alcuni settori regolamentati da leggi specifiche (telecomunicazioni, banche, militari, eccetera) o casi speciali (per esempio per la partecipazione a gare della pubblica amministrazione), è vietato fare verifiche non strettamente collegate alla professionalità della persona: non vanno quindi chiesti casellari giudiziari o cose simili.

12.4.1.2 Contratto con il personale

Una volta selezionata la persona, si redige il contratto. Esso deve includere:

un accordo di riservatezza;

l'obbligo di rispettare le politiche e le procedure dell'organizzazione;

le sanzioni disciplinari.

Al momento della firma, devono essere effettuate le opportune comunicazioni previste dalla normativa vigente, tra cui l'informativa sul trattamento dei dati personali.

Dopo aver inserito una persona, le si assegnano adeguate credenziali e autorizzazioni per accedere alle sedi, ai locali e ai sistemi informatici, come descritto nel paragrafo 12.6.

12.4.1.3 Accordo di riservatezza con il personale

Con un accordo di riservatezza, una persona si impegna a non comunicare informazioni dell’organizzazione a persone non autorizzate o a farne uso senza autorizzazione. Questo accordo deve rimanere valido anche dopo la conclusione del rapporto di lavoro.

Nell’accordo è opportuno indicare precisamente quali sono le informazioni da tutelare. Esse sono le informazioni raccolte, a disposizione o create dall’organizzazione, che non siano pubbliche o di pubblico dominio. Per esempio, esse includono:

i dati personali di clienti, dipendenti, fornitori e partner, compresi gli indirizzi di posta elettronica;

le informazioni di natura commerciale, finanziaria o di strategia di business;

i dati e le informazioni relative ai processi aziendali, inclusa la realizzazione di marchi, brevetti e diritti di proprietà industriale.

12.4.1.4 Sanzioni disciplinari

In Italia le modalità con cui sanzionare il dipendente che non segue le politiche e le procedure sono comprese nel CCNL applicabile e devono essere facilmente disponibili alle persone. Per i consulenti è invece opportuno includere questo aspetto nel contratto, indicando le previsioni per la rescissione anticipata ed eventuali penali in caso di mancato rispetto dei requisiti di sicurezza.

12.4.2 Uscita del personale e cambiamenti di posizione

Al momento dell'uscita può essere opportuno ricordare le responsabilità e gli impegni che rimangono validi anche dopo la conclusione del rapporto di lavoro, in particolare per quanto riguarda la riservatezza.

Importante è pianificare per tempo il passaggio di responsabilità e di consegne a un'altra persona, in modo da assicurare la continuità delle attività.

Ulteriore accorgimento è quello di comunicare alle parti interessate (clienti, fornitori, partner e colleghi) l'uscita della persona, in modo da evitare che continuino a condividere con lei informazioni riservate, cerchino di contattarla convinti che faccia ancora parte dell'organizzazione o, nei casi più gravi, possano essere indotti a compiere azioni non previste (per esempio sottoscrivere un contratto con un'altra organizzazione senza l'adeguata consapevolezza). Vanno quindi comunicati i nuovi riferimenti da usare e per questo è fondamentale assicurare un tempestivo passaggio di consegne.

In caso di cambiamento di posizione, vanno previste azioni simili a quelle sopra descritte.

Per quanto riguarda il processo di cambio o disabilitazione delle autorizzazioni, vedere il paragrafo 12.6.3.1.

12.4.3 Competenze e sensibilizzazione

12.4.3.1 Competenze

Le competenze possono riguardare istruzione (ossia titoli di studio), formazione, addestramento ed esperienza.

Il personale va educato, formato e sensibilizzato. In questo paragrafo si discute delle competenze tecniche, nel 12.4.3.3 di quelle relative alle politiche e procedure da applicare.

Molte organizzazioni dispongono di processi di censimento delle competenze tecniche dei singoli e di valutazione individuali.

La valutazione va condotta anche a seguito di esternalizzazioni o transizioni sul cloud, senza ritenere, erroneamente, di poter fare a meno di certe competenze.

Esempio 12.4.1. Un metodo molto semplice per censire le competenze consiste nella predisposizione di una tabella in cui elencare quelle necessarie, le persone che le hanno e a quale livello.

Si possono prevedere 4 livelli, a cui associare un punteggio:

non competente;

competente ma non autonomo;

competente e autonomo;

competente e capace di insegnare agli altri e aiutare chi è competente ma non autonomo.

Uno schema di questo genere può essere utile per evidenziare se alcune competenze sono in possesso di un numero insufficiente di persone, se il resto del personale può portare avanti il lavoro di una o più persone quando assenti e quali competenze sono da reperire a seguito dell'uscita di una persona dall'organizzazione.

Va osservato che, ai fini della sicurezza delle informazioni, è importante identificare e valutare le competenze presenti nel complesso dell'organizzazione, non solo quelle di una singola persona.

Le competenze tecniche, dove opportuno, vanno dimostrate con certificati professionali riconosciuti a livello internazionale [54].

Sono da pianificare azioni per disporre delle competenze mancanti. Alcuni esempi: formazione attraverso la partecipazione a corsi, affiancamento da parte di personale esperto o di consulenti (training on the job), rotazione del personale in modo che segua diverse attività, assunzione di personale già competente o inserimento di consulenti, studio individuale, partecipazione a gruppi di interesse.

È importante non ridurre questa misura alla “pianificazione annuale della formazione” perché a inizio anno non si possono prevedere tutte le esigenze.

Le azioni intraprese vanno valutate. Per esempio: se il corso di formazione era valido, se i partecipanti erano adatti a parteciparvi, se eventuali esami finali sono stati superati con successo, se l'affiancamento si è concluso positivamente, se il nuovo personale è adeguato. Eventuali interventi di miglioramento devono, se

necessario, essere avviati.

In molti si accontentano, interpretando in modo limitativo il requisito della ISO/IEC 27001, di valutare solo l'efficacia della formazione, ma è evidente come sia insufficiente: le azioni non si riducono alla sola formazione. Bisogna verificare soprattutto se nel complesso si sono ottenute le competenze desiderate.

12.4.3.2 Gruppi di interesse

Il personale tecnico deve mantenersi aggiornato anche per iniziativa personale e partecipando ad associazioni e gruppi di interesse, che mettono a disposizione newsletter, riviste e siti web e organizzano convegni ed eventi finalizzati all'aggiornamento tecnico e professionale. L'organizzazione dovrebbe incentivare queste iniziative, provvedendo direttamente al pagamento degli esami per ottenere i certificati, degli abbonamenti, delle iscrizioni ai corsi di formazione e alle associazioni professionali e degli eventuali viaggi.

12.4.3.3 Consapevolezza e sensibilizzazione

Le attività di sensibilizzazione e consapevolezza hanno l'obiettivo di rendere consapevole il personale delle proprie responsabilità, della politica di sicurezza delle informazioni, dell'importanza del loro contributo per la sicurezza delle informazioni, dei suoi benefici e delle conseguenze del mancato rispetto delle regole stabilite.

Predisporre un programma di sensibilizzazione non è semplice. Richiede la conoscenza della cultura dell'organizzazione e un ottimo supporto da parte della Direzione. Molte organizzazioni hanno predisposto manifesti da diffondere,

gadget basati su un personaggio che richiama la sicurezza, email periodiche da diffondere, filmati da proiettare nelle più diverse occasioni⁷⁴.

Ognuno deve essere formato sulle caratteristiche del proprio lavoro e sulle regole e procedure da rispettare: mai dare per scontata la lettura della documentazione e, pertanto, prevedere degli affiancamenti o dei brevi incontri in aula o teleconferenza.

Si consigliano brevi sessioni periodiche di formazione per ricordare a tutti come reagire a tentativi di social engineering o a fronte di particolari emergenze. Queste sessioni devono essere abbinate a test pratici, per esempio di continuità operativa (paragrafo 12.14) o simulazioni di attacchi (paragrafo 12.15.4). Alcuni eventi sono molto rari e, se non si ribadiscono le regole da seguire, è facile che, quando si presentano, le persone non si ricordino cosa fare o siano prese dal panico.

Alcuni verificano in modo molto fantasioso la consapevolezza del personale, per esempio distribuendo memorie USB in omaggio e senza indicazione della provenienza per osservare quanti le collegano al PC di lavoro, inviando email molto simili a quelle utilizzate per il phishing per osservare quanti sono tratti in inganno oppure inviando file da mittenti anonimi per osservare quanti li eseguono, malgrado possano contenere dei virus.

Più di tutto, però, è necessario che la sicurezza si “respiri nell’aria”, grazie all’esempio della Direzione.

Quando si ricordano al personale le regole da seguire, piuttosto di ripetere le sanzioni a cui potrebbero essere soggetti, è opportuno sottolineare come la sicurezza sia importante per garantire la sostenibilità dell’organizzazione, visto che i danni all’immagine possono comprometterla.

Se si introducono nuovi strumenti o modificano procedure, se le novità sono di scarso impatto, può essere necessario inviare una comunicazione per segnalarle, altrimenti si possono prevedere corsi, anche brevi, in aula o a distanza con strumenti web, o affiancamenti.

Non è scontata la competenza sugli strumenti informatici e la capacità di utilizzarli in modo sicuro, neanche quando si parla di persone giovani, nate nell'era digitale (nativi digitali) [146]. Parecchi casi di cronaca dimostrano che sono proprio i più giovani a essere accusati di diffamazione sui social network (vedere il paragrafo 11.21) o di diffusione di informazioni riservate. Molti sono stati cresciuti o educati al principio che non si ha niente da nascondere (anche a causa dei genitori che pubblicano loro fotografie sui social network senza chiedere il permesso) e devono riconsiderare alcuni loro comportamenti quando iniziano a lavorare per organizzazioni dove la protezione dell'immagine e dei segreti industriali è fondamentale.

È preferibile, quando possibile, mettere a disposizione del personale degli strumenti che li obblighino a rispettare le misure di sicurezza, piuttosto che avere fiducia nella sola efficacia delle iniziative di formazione e sensibilizzazione (allo stesso modo in cui su molti modelli di automobile è presente un allarme se le cinture di sicurezza non sono allacciate).

Esempio 12.4.2. Alcuni controlli di sicurezza per i quali sono disponibili soluzioni tecnologiche che obbligano il personale a tenere un comportamento adeguato:

piuttosto che chiedere di tenere aggiornato l'antivirus sul proprio PC, consegnare un PC con l'antivirus già installato e configurato affinché si aggiorni automaticamente e non sia possibile disinstallarlo;

per fare in modo che siano scelte password complesse, oltre a pubblicare regole scritte, configurare gli strumenti informatici affinché verifichino in automatico la complessità delle password scelte dagli utenti;

per evitare che il personale installi software illegale sui propri PC, configurarli affinché blocchino questa operazione in modo automatico.

12.4.4 Lavoro fuori sede

Il lavoro fuori sede comprende quello temporaneo presso i clienti o altre organizzazioni e quello da casa o in reperibilità.

Le persone, quando lavorano fuori sede, possono fare uso di dispositivi informatici portatili, di cui si discute nei paragrafi 12.9.2 e 12.9.8, e che pertanto devono essere configurati con firewall, antimalware, controllo accessi, software di connessione sicura ai sistemi dell'organizzazione e una soluzione per la cancellazione da remoto.

Per quanto riguarda le informazioni in formato cartaceo o in altri formati portati fuori dalla sede, oltre a quanto indicato nel paragrafo 12.10.4 in merito al loro trasferimento, è necessario prevedere archivi ad accesso limitato.

Vanno fornite regole da seguire relativamente alla sicurezza fisica dei locali dove si lavora.

Vanno anche studiate le opportune misure di backup e continuità nel caso in cui i sistemi informatici usati o il sito fisico non siano più disponibili. Per i backup è

necessario verificare la disponibilità di sufficiente banda di rete se fatto sui server aziendali o, in caso contrario, vanno identificate altre soluzioni anche in locale. Per i siti alternativi se ne deve verificare l'effettiva disponibilità e la connettività.

La formazione specifica per i lavoratori fuori sede è importante sia perché devono attuare le misure previste senza il supporto diretto del personale normalmente addetto a questo, sia perché possono essere oggetto di attacchi come si è visto durante la pandemia COVID-19, quando sono state condotte numerose campagne di phishing mirate⁷⁵.

Un particolare caso di lavoro fuori sede è il telelavoro. In Italia questo tipo di soluzione è regolamentato nel settore privato da accordi interconfederali tra associazioni di imprese e sindacati. Essi prevedono che il datore di lavoro fornisca al telelavoratore procedure scritte sulle attività da svolgere e gli strumenti necessari anche per garantire la sicurezza delle informazioni: archivi sicuri, memorie informatiche e computer adeguatamente configurati.

Ulteriori indicazioni sono riportate dalle sempre utili guide del NIST [139].

12.5 Gestione degli asset

Il termine asset è già stato definito nel paragrafo 6.1. In questo paragrafo si discute di identificazione, censimento, classificazione, etichettatura e trattamento.

12.5.1 Informazioni

Le informazioni devono essere identificate, classificate, etichettate e quindi trattate a seconda della loro classificazione.

12.5.1.1 Identificazione e censimento delle informazioni

L'identificazione e il censimento delle informazioni sono descritti nell'ambito della valutazione del rischio (paragrafo 6.1), dove il livello di dettaglio può essere ridotto.

In alcuni contesti è richiesto di censire con maggiore dettaglio le informazioni, in modo anche di stabilire a priori la loro classificazione. Bisogna dire che solitamente questi censimenti non sono mai perfetti, anche a causa dei frequenti cambiamenti dei processi e delle attività, e bisogna pertanto esserne consapevoli per evitare falsi sensi di sicurezza.

12.5.1.2 Responsabile delle informazioni

Per ogni informazione bisogna identificare un responsabile o proprietario. Può essere una persona o una funzione (per esempio l'Ufficio del personale o quello delle vendite) ed è responsabile della sua classificazione e protezione.

12.5.1.3 Classificazione delle informazioni

Le informazioni vanno classificate, attribuendo loro i pertinenti livelli di riservatezza. È opportuno non confondere la classificazione con la valutazione

necessaria all’analisi del rischio (paragrafo 7.2.1): la classificazione ha il fine di stabilire chi è autorizzato ad accedere alle singole informazioni e modificarle.

In ambiente civile, i livelli di classificazione possono essere: informazione pubblica, informazione a uso interno dell’organizzazione (o general business) e informazione a uso ristretto. Altri livelli possono basarsi sulla normativa privacy (paragrafo 12.15.1.9) e quindi essere: informazioni anonime, informazioni personali non appartenenti a categorie particolari, informazioni personali appartenenti a categorie particolari e informazioni personali e giudiziarie. È necessario stabilire linee guida scritte per evitare disallineamenti nelle classificazioni fatte da persone diverse.

In Italia, la normativa sul segreto di Stato prevede quattro livelli crescenti: riservato, riservatissimo, segreto e segretissimo. Purtroppo, tranne un Regio Decreto del 1941⁷⁶, non sono disponibili linee guida per l’assegnazione di tali valori.

La normativa relativa alla proprietà industriale richiede di specificare cosa si intende per segreto industriale e quindi anche questo è un elemento da considerare quando si stabiliscono i livelli di classificazione.

Un altro tipo di classificazione richiede la designazione delle aree o degli uffici il cui personale può accedere alle informazioni.

Esempio 12.5.1. Le informazioni relative al personale devono essere accessibili solo all’ufficio dedicato all’amministrazione del personale e ai suoi eventuali fornitori (consulenti del lavoro, commercialisti e studi legali).

In organizzazioni molto grandi le informazioni sui progetti potrebbero essere accessibili solo ad alcuni settori di produzione; le offerte e gli ordini solo all'ufficio commerciale.

La classificazione può variare nel tempo. Per esempio, le strategie di un'azienda vanno tenute riservate fino a quando la Direzione non decide di renderle pubbliche. Per questo motivo vanno stabilite le modalità e le responsabilità per modificare la classificazione assegnata.

12.5.1.4 Etichettatura

Una volta classificate, le informazioni possono essere etichettate. Questo termine ricorda le etichette apposte sui documenti cartacei, come quella top secret nota grazie a film e telefilm.

Su supporto fisico è possibile prevedere una scritta in copertina e in ogni piè di pagina o intestazione del documento. La scritta deve riportare il livello di classificazione e le aree il cui personale è autorizzato ad accedervi.

Anche per i documenti in formato elettronico possono essere previste etichette. Sono in commercio alcuni programmi che obbligano gli utenti a classificare ogni documento e ogni email inviata; alcuni di essi possono stabilire in automatico il livello di classificazione da assegnare. Il meccanismo è spesso un po' complicato e per questo molti hanno dismesso questi sistemi.

Per alcune applicazioni informatiche, nella schermata iniziale si potrebbe evidenziare il livello di classificazione delle informazioni a cui si ha accesso.

Le etichette possono essere poste nei metadati dei file, in modo che siano automaticamente gestite dalle applicazioni. Questo, seppure promosso da alcuni, oggi non è però supportato dalle applicazioni più diffuse, se non con alcuni software aggiuntivi. Questo vuol dire che il meccanismo non è più valido quando le informazioni sono trasferite da un'organizzazione all'altra, a meno di rare eccezioni.

Bisogna dire che è quasi impossibile, per le organizzazioni non militari, attuare un sistema di etichettatura per tutte le informazioni: troppa attenzione è demandata alle singole persone. Per questo motivo si suggerisce di ridurre le richieste di etichette ai soli documenti molto critici anche osservando che le etichette potrebbero a loro volta costituire un rischio: quello di attirare l'attenzione di estranei.

12.5.1.5 Trattamento

A seconda del livello di classificazione, vanno previste diverse modalità di trattamento. Esse riguardano:

la conservazione delle informazioni a seconda del loro supporto (per esempio, quelle riservate in formato cartaceo devono essere sempre custodite in armadi chiusi a chiave; quelle in formato elettronico salvate in partizioni cifrate);

la copia totale o parziale delle informazioni, in alcuni casi da vietare;

la trasmissione delle informazioni (per esempio attraverso email cifrate se in formato elettronico e corrieri qualificati se in formato cartaceo; la trasmissione può essere tracciata con una catena di custodia) maggiori dettagli sugli scambi di informazioni sono al punto 12.10.4;

la distruzione delle informazioni (vedere il paragrafo 12.8.2.7);

lo scambio delle informazioni con entità esterne come fornitori, clienti, partner, auditor o forze dell'ordine.

Le regole di trattamento vanno rese note mediante istruzioni scritte che specifichino, coerentemente con le competenze del personale, come utilizzare gli strumenti per classificare, cifrare o distruggere le informazioni.

Esempio 12.5.2. In molte organizzazioni sono distribuite regole che richiedono la cifratura delle informazioni critiche, senza che sia fornito uno strumento per farlo.

Questo è un esempio di misura inefficace, spesso prevista sui documenti perché richiesto da qualche normativa, ma non applicata nella pratica.

Anche per le informazioni non classificate è opportuno fornire istruzioni. Per esempio, tutte le informazioni in formato elettronico devono essere archiviate in specifiche aree della intranet dell'organizzazione, in modo da garantirne il backup.

12.5.1.6 Data loss prevention

Per le informazioni in formato elettronico, alcuni programmi di data loss prevention o DLP, da affiancare a quelli di classificazione, controllano automaticamente il rispetto delle regole stabilite (ma utenti motivati possono

facilmente aggirarli).

Questo programmi possono identificare e classificare le informazioni in automatico anche grazie a parole chiave, monitorare i canali di trasmissione (per esempio email, programmi di file transfer, dispositivi mobili e di memorizzazione), reagire quando sono rilevate attività sospette (per esempio mettendo in quarantena le email e bloccare la copia dei file), richiedere autorizzazioni per azioni specifiche (per esempio richiedere l'autorizzazione a un responsabile quando un utente vuole trasferire un file critico).

Questo specifico argomento può anche essere indicato come “prevenzione della perdita (leakage) di dati”. Esso include le tecniche di reverse social engineering e gli honeypot: queste sostituiscono informazioni autentiche con falsi per confondere un attaccante o rallentare le azioni.

12.5.1.7 Mascheramento e anonimizzazione

Le informazioni, in alcuni casi, possono essere mascherate, anonimizzate o pseudonimizzate, a seconda del loro livello di classificazione. Queste tecniche sono usate, per esempio, nei settori delle ricerche di mercato (quando i dati degli intervistati sono disgiunti da quelli delle risposte), della sanità (quando i risultati di esami critici, per esempio relativi a certe malattie o alla gravidanza, sono nascosti o oscurati, per volontà del paziente, agli stessi operatori sanitari, fino a nascondere lo stesso oscuramento con tecniche di oscuramento dell'oscuramento), farmaceutico (nel corso delle sperimentazioni) e informatico (dove, per i test, sono usati copie anonimizzate dei dati di produzione).

Le tecniche di mascheramento includono il cambiamento casuale o la sostituzione di alcuni valori (per esempio le date di nascita) e la cancellazione di parte dei dati (per esempio gli indirizzi).

Quelle di anonimizzazione prevedono la cancellazione dei riferimenti delle persone (fisiche o giuridiche) a cui si riferiscono i dati o la loro sostituzione con altri caratteri casuali in modo da non poter più risalire al dato originale. Queste tecniche vanno usate con molta attenzione, verificando se, anche con i dati rimanenti, si può risalire alle persone stesse [81].

La pseudonimizzazione consiste nel togliere i riferimenti personali ai dati, ma comunque in modo da poter ricostruire l'associazione.

Esempio 12.5.3. Le società di ricerche di mercato raccolgono i dati degli intervistati (tra cui nome e cognome) e quelli relativi alle risposte alle interviste applicando una tecnica di pseudonimizzazione detta disgiunzione:

a ogni intervista è associato un identificativo dell'intervistato (esiste quindi una tabella che mette in relazione l'identificativo con i dati necessari per identificare l'intervistato);

se i dati sono in formato cartaceo, i dati delle interviste e degli intervistati sono su fogli separati, raccolti in archivi separati;

se i dati sono in formato elettronico, i dati sono in tabelle separate.

In questo modo chi elabora i dati non ha accesso ai nominativi degli intervistati, ma se qualcuno deve intervistare una seconda volta le persone (per controlli qualità o perché l'indagine prevede l'analisi dell'evolversi delle risposte nel tempo), può avere accesso ai dati completi.

Al termine del periodo di conservazione, possono essere cancellati i soli dati personali e non i risultati delle interviste.

La cifratura dei dati è una forma particolare di pseudonimizzazione, visto che è possibile ricostruirli se si è in possesso della chiave di cifratura.

12.5.1.8 Tempi di conservazione

Per ogni informazione va stabilito un tempo di conservazione retention time.

Alcune informazioni devono essere conservate per un periodo minimo di tempo, dipendente spesso dalla normativa vigente e non solo ??. Per esempio, il Codice Civile stabilisce che le scritture contabili devono essere conservate per almeno 10 anni; altre leggi trattano dei fascicoli tecnici di determinati prodotti. La normativa sulla privacy stabilisce invece i tempi massimi di conservazione dei dati personali e quindi di molti documenti e delle videoregistrazioni.

È importante mantenere la leggibilità dei documenti per tutto il tempo in cui devono essere conservati. Se le informazioni sono su supporti deperibili come la carta, è necessario siano conservate in archivi con le opportune misure di sicurezza e di controllo della temperatura e dell'umidità.

Se le informazioni sono in formato digitale, bisogna garantire la disponibilità dei programmi software per leggerle e, se questi non sono più disponibili, stabilire regole per convertirle in altri formati. Un'altra opzione prevede di creare i documenti e le registrazioni direttamente in formati progettati per la conservazione a lungo termine, come il PDF/A descritto dalla ISO 19005.

Alcune questioni da considerare, per i documenti in formato digitale e non digitale:

il possibile deterioramento dei supporti digitali, cartacei, fotografici, eccetera;

l'obsolescenza dei formati digitali e dei software usati per accedervi (in questo caso, una copia del “vecchio” software potrebbe essere mantenuta o i file potrebbero essere tutti convertiti ai nuovi formati);

la scadenza delle chiavi usate per firmare o cifrare i documenti digitali (le chiavi quindi potrebbero essere conservate a loro volta, ma su supporti e archivi distinti, oppure i documenti potrebbero essere cifrati o firmati nuovamente, seguendo specifici processi);

il tempo necessario per reperire i “vecchi” documenti, parametro da considerare quando si sceglie come archiviare i documenti e quali software usare e mantenere;

le modalità per cancellarli nei tempi previsti e in modo sicuro (come anche indicato al paragrafo 12.5.1.5).

12.5.2 Identificazione, censimento e proprietà degli asset

12.5.2.1 Identificazione e censimento degli asset

Nell’ambito della sicurezza delle informazioni, è necessario identificare gli asset al corretto livello di dettaglio.

Esempio 12.5.4. Nella maggioranza delle organizzazioni, ogni PC portatile è inventariato come un tutto unico.

Organizzazioni operanti in settori particolarmente critici, dove è necessario un livello di dettaglio superiore, censiscono anche i numeri di serie dei singoli hard disk e dei moduli RAM.

Per effettuare la valutazione del rischio relativo alla sicurezza delle informazioni non è necessario identificare gli asset a un elevato livello di dettaglio (paragrafo 6.1).

Per finalità operative, è invece necessario disporre di informazioni più dettagliate. Per esempio occorre sapere:

quali computer, inclusi gli ambienti virtuali, sono utilizzati per trattare le informazioni, in modo da valutare gli impatti quando devono essere spenti o disconnessi per manutenzioni;

quali programmi software e in quale versione sono installati, in modo da monitorare le licenze disponibili, stabilire se le segnalazioni di vulnerabilità sono applicabili e se è necessario installare le patch pubblicate;

quali cellulari, smartphone, SIM e chiavi Internet sono assegnati al personale, in modo da provvedere al loro ritiro in caso di dimissioni o licenziamento;

quali impianti (aria condizionata, generatori, batterie, estintori, rilevatori di fumi, rilevatori di intrusioni, eccetera) sono necessari per la sicurezza delle informazioni, in modo da programmarne la manutenzione.

Risulta evidente che si tratta di tipi di asset diversi. Pertanto i loro inventari possono essere gestiti da uffici diversi e con strumenti distinti (per esempio, tabelle o database complessi), da scegliere a seconda di quante persone devono accedervi e degli attributi da registrare, come, per esempio: il numero di versione per un software oppure, per i cellulari e smartphone, la marca, il modello, il numero di serie e l'IMEI.

Nell'ambito della gestione dei servizi informatici, l'inventario è spesso denominato configuration management database (CMDB) o configuration management system (CMS).

In molte organizzazioni l'inventario degli asset informatici è effettuato con l'aiuto di strumenti di discovery che rilevano automaticamente gli apparati collegati alla rete e i programmi installati sui sistemi. I dati raccolti sono poi confrontati con quelli registrati sul CMDB in modo da evidenziare eventuali disallineamenti dovuti ad azioni non autorizzate o dimenticanze.

Progettare, realizzare e mantenere un CMDB è complesso e oneroso; richiede la definizione di un processo ben preciso, collegato al processo di gestione dei cambiamenti (paragrafo 12.9.3), affinché ogni modifica sia registrata in modo tempestivo e accurato [95].

12.5.2.2 Proprietà degli asset

A ciascun asset va assegnato un proprietario, ossia la funzione organizzativa o la persona con la responsabilità della sua corretta gestione e manutenzione. Per esempio, proprietario dell'impianto dell'aria condizionata potrebbe essere l'ufficio addetto ai servizi generali, mentre proprietario di un computer portatile potrebbe essere la persona a cui è stato assegnato.

Più complesso è stabilire il proprietario di un sistema o sottosistema informatico: normalmente è il reparto IT o una sua sotto area. In altri casi, il proprietario di un sistema informatico è l'area dell'organizzazione con la responsabilità di stabilire gli investimenti per la sua conduzione e manutenzione, oppure chi può decidere sulle autorizzazioni di accesso.

12.6 Controllo degli accessi

A ciascuna persona sono assegnate autorizzazioni per accedere alle informazioni, inclusi dati personali, o agli strumenti utilizzati per trattarle o archiviarle: sedi, locali, archivi fisici, applicazioni informatiche, PC, server, reti e apparati di rete, cellulari, smartphone, tablet, eccetera.

Politica di controllo degli accessi

Registrazione e de-registrazione utenti

Autorizzazioni

Sistemi operativi

Reti

Servizi
Applicazioni

Informazioni

Sedi

Locali

Armadi
Casseforti

Apparecchiature

Figura 12.6.1:

La politica del controllo accessi

Per ottenere un accesso, un utente deve identificarsi attraverso credenziali, di cui si parla nel seguito. Successivamente si tratta della gestione delle autorizzazioni, incluse quelle degli amministratori di sistema.

12.6.1 Credenziali e identificazione

Con il termine credenziali si indicano i parametri forniti a una persona per poterla riconoscere. Il riconoscimento avviene in due fasi:

identificazione: a una persona viene assegnato un codice identificativo;
autenticazione: si accerta che la persona sia effettivamente chi dichiara di essere.

In informatica, le credenziali sono spesso composte da una user-id per l'identificazione e da una password per l'autenticazione.

Ogni codice di identificazione deve essere assegnato a un'unica persona e non condiviso con altre. In caso contrario, i log non potrebbero rilevare i responsabili delle singole azioni (paragrafo 12.9.6.1).

Per l’assegnazione di identità condivise (per esempio quelle di amministrazione di alcuni sistemi informatici e quelle usate a nome dell’organizzazione per i social network, alcuni servizi cloud e alcuni servizi esterni come l’Internet banking) o di utenze per le entità non umane (per esempio per l’interfacciamento di diversi sistemi), è necessario stabilire precisi processi e responsabilità. Di questo si discute nel paragrafo 12.6.2.7.

Per quanto riguarda l’assegnazione, disabilitazione e rimozione delle identità, si veda il paragrafo 12.6.3.1.

Si raccomanda, sui sistemi che lo permettono, di verificare periodicamente le identità non usate, in modo da disabilitarle prima che siano compromesse da malintenzionati.

12.6.2 Autenticazione

A fronte di un codice di identificazione, come per esempio la user-id, un utente può autenticarsi, ossia dimostrare la propria identità, attraverso:

qualcosa che sa: una password o una “parola d’ordine”, un PIN, una sequenza o altro; ovviamente, l’utente deve mantenere segreta tale caratteristica; la ISO/IEC 27001 del 2013 utilizzava l’espressione informazioni segrete di autenticazione, mentre quella del 2022 utilizza l’espressione informazioni di autenticazione

qualcosa che ha: una tessera come la carta di credito, uno strumento da collegare al computer come una chiave USB, un cellulare o uno smartphone da utilizzare per ricevere password temporanee; si tratta quindi di un lasciapassare, da non affidare mai ad altri; spesso l’oggetto è indicato con il termine token;

qualcosa che è: caratteristiche fisiche personali come l’impronta digitale o la

retina (caratteristiche biometriche); rientrano in questo caso la foto su un documento d'identità e la firma autografa.

I meccanismi sopra descritti sono controlli tra loro alternativi, ma anche complementari: per esempio, le tessere bancomat (qualcosa che si ha) possono essere utilizzate se è noto il PIN (qualcosa che si sa). In questi casi, si parla di meccanismi di autenticazione forte (strong authentication, multi-factor authentication o MFA) o, quando i fattori sono due, two-factor authentication (2FA), descritti nel seguito.

In alcuni casi l'identificazione e l'autenticazione avvengono attraverso il medesimo strumento. Per esempio, un documento d'identità permette di assegnare un'identità a una persona e autenticarla grazie alla foto (qualcosa che è) e al suo possesso (qualcosa che ha).

Alcuni strumenti, come le chiavi, non permettono di identificare precisamente una persona: il loro possesso dimostra solo il suo ruolo e il suo diritto ad accedere a delle informazioni, a dei locali o a fare uso di certi strumenti. A questi strumenti, spesso condivisi, è dedicato il paragrafo 12.6.2.7.

12.6.2.1 Le password

La password è il meccanismo di autenticazione più diffuso, ma non per questo più sicuro (paragrafo 11.2). Il PIN è un particolare tipo di password, composto di soli numeri.

Le password devono essere complicate (o robuste o complesse) per evitare che un malintenzionato le possa individuare per poi accedere a informazioni o

strumenti senza autorizzazione.

È sempre meglio impostare i sistemi informatici affinché verifichino in automatico se le password scelte dagli utenti sono sufficientemente complesse: fosse per loro, eviterebbero di impostarle o, se proprio costretti, ne utilizzerebbero di molto semplici (lo dimostrano i numerosi tablet e smartphone configurati dagli utenti senza alcuna forma di controllo di accesso e alcuni studi⁷⁷).

Le organizzazioni devono quindi configurare i sistemi affinché controllino la complessità delle password scelte dagli utenti (lunghezza di almeno 8 caratteri, ma 15 è preferibile, presenza di numeri, lettere maiuscole e lettere minuscole).

Regole di complessità più rigorose devono essere valutate con attenzione, per evitare che gli utenti, gravati dalla numerosità e complessità di password da ricordare, anche per accedere a servizi personali (email, social network, PIN della carta Bancomat, eccetera), le scrivano su dei fogliettini in prossimità del PC. Oggi si ritiene preferibile non richiedere più password complesse, ma solo di lunghezza di almeno 8 caratteri, non presenti su un dizionario, non uguali al nome dell'utente o del servizio per cui sono usate o password notoriamente banali come “123456”[57].

Esempio 12.6.1. Una guida per scegliere password complesse è la seguente:

scegliere una frase o una poesia;

usare le prime lettere delle parole della frase o poesia;

mescolare lettere maiuscole e minuscole;

aggiungere un po' di punteggiatura come virgolette, punti esclamativi, punti di domanda e parentesi e/o cambiare le lettere con numeri simili (A diventa 4, B diventa 8), e/o indicare il numero di lettere che si ripetono;

aggiungere un simbolo come asterisco, apostrofo, accento circonflesso.

Per esempio, dal noto “Nel mezzo del cammin di nostra vita mi ritrovai per una selva oscura ché la diritta via era smarrita” si può ricavare la password NMdcdN5MR*1SoKld53S.

Oggi non è più ritenuto necessario richiedere il cambiamento periodico della password, visto che il tempo necessario a un malintenzionato per indovinarla sarebbe comunque molto breve e il cambiamento frequente della password disincentiva molte persone a sceglierne di buona qualità. Devono però essere attivi meccanismi di blocco o allarme dopo un certo numero di tentativi falliti. È anche necessario valutare la possibilità che le persone condividano, nonostante i divieti le proprie password con altri e quindi la necessità di azzerare periodicamente il numero di tali persone con il cambio della password.

È sempre opportuno fare in modo che gli utenti possano cambiare autonomamente e quando vogliono le proprie password, in modo da farlo appena hanno il sospetto che sia stata compromessa. Dall'altra parte, anche gli amministratori devono poter imporre il cambio della password se hanno il sospetto che sia stata compromessa.

Ulteriori controlli prevedono la verifica del dispositivo usato per connettersi, dell'origine geografica della richiesta di connessione, dell'orario, eccetera. La ISO/IEC 27002:2022 indica queste verifiche con il termine originale di dynamic access management.

Autenticazione forte

Un meccanismo di autenticazione forte (strong authentication o two-factor authentication o 2FA) richiede, oltre a user-id e password, un codice generato da un dispositivo (token) in possesso dell'utente; altri l'uso di una smart card o di un'impronta digitale, attraverso apposite periferiche collegate al PC.

Esempio 12.6.2. Gli strumenti più diffusi di 2FA sono:

l'invio di una password aggiuntiva (detta one-time password o OTP) via SMS; questa è considerata l'opzione meno sicura;

l'invio di un OTP a un'applicazione per smartphone o tablet (esempi sono Google Auth e MS Authenticator, oltre alle app di molte banche);

la visualizzazione di un OTP su un dispositivo specifico (esempio è RSA SecurID);

la connessione di un token USB al PC o di un dispositivo Bluetooth o NFC allo smartphone o tablet; a loro volta, questi token e dispositivi sono attivabili con PIN o impronta digitale (esempi sono YubiKey di Yubico, U2F Security Key di Feitian e Titan Key di Google, basati sul protocollo FIDO); questa è considerata l'opzione più sicura.

Quando si usa uno smartphone

Single sign on

Per evitare un eccessivo numero di credenziali per accedere ai diversi sistemi informatici di un'organizzazione, sono disponibili sul mercato degli strumenti di single sign on (SSO): permettono agli utenti di accedere ai sistemi dopo essersi identificati e autenticati un'unica volta. Gli strumenti di single sign on permettono di centralizzare la gestione delle credenziali e delle autorizzazioni e rendere più efficiente il lavoro degli amministratori di sistema. D'altra parte, prima di stabilire se adottarli, è necessario valutare il rischio per cui con una sola password un malintenzionato può accedere a numerosi sistemi.

Da osservare che non tutti programmi si possono interfacciare con tutte le soluzioni SSO disponibili e pertanto è necessario prevedere un'analisi approfondita prima di introdurli in un'organizzazione.

Oggi molte organizzazioni interfacciano le diverse applicazioni con l'Active Directory di Microsoft, in modo che questo funga da strumento SSO.

12.6.2.2 Sicurezza dell'autenticazione

Per la sicurezza dell'autenticazione informatica sono necessari alcuni accorgimenti, oggi solitamente previsti da tutti i software e da tutti i sistemi:

non fornire informazioni sul sistema (per esempio sistema operativo, software e relative versioni) prima dell'autenticazione;

non fornire troppi dettagli nei messaggi d'errore (per esempio non specificare se è sbagliata la user-id o la password);

validare le credenziali solo sul server e solo al termine del loro inserimento e

dopo conferma dell’utente (per esempio dopo aver premuto un bottone);

contrastare gli attacchi a forza bruta attraverso il blocco dell’utenza o il rallentamento del meccanismo di autenticazione e l’invio di un allarme all’utente o agli amministratori di sistema dopo un certo numero di errori; oggi si usano anche meccanismi di autenticazione cosiddetti di challenge/response, il cui più noto è il CAPTCHA;

registrare i tentativi di accesso riusciti e falliti, in modo da ricostruire gli eventi;

non mostrare la password in chiaro a video per evitare che sia vista da qualcuno alle spalle dell’utente;

non memorizzare in chiaro le password sui sistemi informatici, per evitare che il file delle password, se compromesso da un malintenzionato, possa essere usato impropriamente; per questo sono a disposizione numerose e valide tecniche basate sulla crittografia;

trasmettere le credenziali su canali cifrati;

presentare un avviso sulle responsabilità dell’utente all’accesso;

terminare le sessioni dopo un certo tempo di inattività.

Per quanto riguarda la visualizzazione delle password, i sistemi odierni, soprattutto quelli di tipo touch, per aiutare gli utenti, in particolare quelli disabili, ed evitare il blocco per l’eccessivo numero di errori, mostrano brevemente il carattere inserito in modo che l’utente possa essere sicuro di averlo fatto correttamente. Altri sistemi permettono di visualizzare la password prima di inviarla al sistema, così l’utente, quando è sicuro di non essere osservato, può verificare se è quella corretta.

Come già scritto sopra, si possono usare meccanismi di autenticazione a più fattori o attivare controlli basati sulla locazione, sul dispositivo o sull’orario.

12.6.2.3 Consegnare le credenziali

Difficile da gestire è la prima consegna di credenziali. La tecnica più utilizzata prevede l'uso di canali distinti per comunicare user-id e password. Per esempio, si comunica la user-id a voce e la prima password via SMS; gli emettitori di carte di credito inviano via posta e separatamente la carta e il PIN. Questi metodi non garantiscono la massima sicurezza perché gli SMS e le lettere possono essere intercettati; il metodo più sicuro consiste nel: comunicare le credenziali di persona, dopo riconoscimento con documento d'identità, e richiedere la modifica della password alla prima connessione. Oggi il PIN è anche comunicato tramite un'app per dispositivi mobili, come avviene nel caso dei PIN delle carte di credito e di debito (Bancomat), visualizzabili tramite l'app della banca emettitrice.

Alcuni sistemi propongono password iniziali uguali per tutti, che devono essere cambiate al primo accesso. In altri casi sono gli amministratori di sistema che forniscono password iniziali, e anch'esse vanno cambiate al primo accesso. È importante cambiare queste password, dette di default, perché spesso diventano note a malintenzionati che possono sfruttarle per accedere in modo non autorizzato ai sistemi.

Per i sistemi di strong authentication devono essere consegnati token o registrate le caratteristiche biometriche in modo che siano riconosciute dai sistemi quando l'utente vuole autenticarsi. I token possono essere consegnati di persona o inviati via posta e attivati solo quando si ha conferma della ricezione da parte del destinatario. Le caratteristiche biometriche sono necessariamente registrate, tranne casi particolari, con la presenza dell'utente.

Quando è necessario ripristinare le credenziali, per esempio se l'utente ha dimenticato la password o ha perso eventuali token, deve essere seguito il medesimo processo di prima consegna, ma non sempre ciò è possibile. Alcuni siti web utilizzano tecniche insicure, basate su domande segrete, facilmente

indovinabili, o l'invio della password via email, facilmente intercettabile.

Per compensare l'assenza di controlli robusti, alcuni sistemi avvertono l'utente, al momento del suo accesso, quando è avvenuta la precedente connessione, in modo che possa notare se qualcuno ha abusato delle sue credenziali.

12.6.2.4 Istruzioni agli utenti

Quando sono assegnate credenziali e autorizzazioni, le persone vanno istruite su come gestirle, in particolare:

usare password robuste (vedere sopra);

tenere segrete le password;

non scrivere le proprie password e, nel caso questo si renda necessario, non lasciarle in evidenza (per esempio un foglietto vicino al PC) o in luoghi facilmente accessibili (per esempio, sotto la tastiera del computer o nel primo cassetto della scrivania);

non inserire le proprie credenziali (neanche la user-id) quando qualcuno può osservare;

custodire con cura i token;

non usare, per accedere ai sistemi dell'organizzazione, le stesse password usate per accedere ad altri servizi esterni come email personale, socialnetwork, siti di e-commerce;

disconnettersi da tutti i servizi informatici quando non li si utilizza, in modo da evitare attacchi di session hijacking (paragrafo 11.20);

bloccare il PC se non presidiato;

dopo essersi identificati e autenticati, non permettere ad altri di utilizzare i sistemi informatici a cui si ha accesso.

12.6.2.5 Affidabilità degli strumenti biometrici

Quando si usano strumenti biometrici, bisogna valutarne l'affidabilità e in particolare verificare quanto specificato dai produttori in merito a:

la percentuale di falsi positivi, ossia con quale probabilità permettono l'accesso a persone non autorizzate perché scambiate per persone autorizzate;

la percentuale di falsi negativi, ossia con quale probabilità negano l'accesso a persone autorizzate perché scambiate per persone non autorizzate.

Bisogna valutare le modalità da seguire in caso di emergenza, ossia quando il meccanismo di riconoscimento si guasta e quando una persona non può usare la propria caratteristica biometrica (per esempio perché deve tenere fasciato il dito utilizzato per il riconoscimento dell'impronta digitale).

Quando si utilizzano strumenti biometrici, è sempre necessario prestare attenzione a quanto prescritto dalle normative relative al trattamento dei dati personali (paragrafo 12.15.1.9) e alla tutela dei lavoratori perché richiedono precise misure per tutelare i dati relativi alle caratteristiche biometriche.

12.6.2.6 Smart card

Le smart card sono tessere con microprocessore. Esempi sono le SIM dei cellulari e le carte di credito. Queste ultime sono oggi a tecnologia mista: banda magnetica (senza meccanismi di sicurezza) e microprocessore.

Il microprocessore è un piccolo computer, con una memoria nella quale sono conservate delle informazioni (per esempio, parametri biometrici o di firma digitale) e un processore per le elaborazioni; vi sono inoltre dei meccanismi per controllare gli accessi alla memoria e al processore. La carta si attiva solo se inserita in un lettore o, se wireless, avvicinata a esso.

Le smart card sono solitamente costruite con meccanismi di anti-tampering: se qualcuno cerca di accedere alla loro memoria manomettendola fisicamente, si autodistruggono.

È opportuno utilizzare smart card di tipo match on card, per cui le elaborazioni dei dati per il riconoscimento sono effettuate dalla carta stessa e non dal lettore, in modo da evitare l'intercettazione dei dati conservati nella memoria della carta.

12.6.2.7 Strumenti e credenziali condivise

Per l'accesso ad alcuni sistemi non è sempre possibile disporre di utenze distinte per ciascun utilizzatore e quindi le credenziali sono condivise tra più persone. Tra questi meccanismi vi sono i codici per attivare o disattivare alcuni allarmi di rilevazione delle intrusioni negli uffici e alcune password di amministrazione dei sistemi informatici. Da considerare anche le smart card per i sigilli (ossia le firme) digitali se ne esiste una per tutta l'organizzazione e utilizzata da più persone.

In alcuni casi, la condivisione di questi strumenti e credenziali è necessaria per garantire la continuità di certe operazioni: se note a una sola persona e questa fosse assente, non sarebbe più possibile accedere ai sistemi.

Per tutte le credenziali condivise vanno stabilite deleghe precise alle persone che le possono conoscere e utilizzare e un processo per il ritiro delle deleghe quando necessario: recupero dello strumento (per esempio la smart card), modifica delle credenziali e comunicazione dei nuovi parametri agli altri delegati.

12.6.2.8 Autenticazione delle macchine

Per i sistemi di automazione d'ufficio, l'autenticazione riguarda il singolo utente. Per far però interagire tra loro più computer, software o macchine, è necessario che queste si autentichino come singole entità.

Questo può avvenire per molti usi: servizi di backup e di distribuzione degli aggiornamenti, sistemi industriali, inclusi i robot e per connettere dispositivi nell'ambito dell'Internet of Things (IoT).

L'autenticazione delle macchine avveniva e, in alcuni casi, avviene tuttora con la verifica dell'indirizzo MAC, ossia un codice univoco assegnato alle schede di rete. Questo metodo è però molto insicuro perché facilmente modificabile con programmi software.

Alcuni programmi software, invece, per interfacciarsi tra loro, usano delle credenziali spesso inserite nel loro codice (password di servizio). Questa pratica è molto diffusa, anche se fortemente sconsigliata per motivi di sicurezza: le credenziali sono note a tutti i programmatori e possono essere recuperabili da malintenzionati grazie a un'analisi del codice con tecniche di reverse engineering; inoltre le credenziali di interfacciamento sono spesso associate ad autorizzazioni molto ampie e quindi la loro compromissione potrebbe avere conseguenze disastrose.

Oggi si usano i certificati digitali: un certificato è installato sulla macchina che si vuole autenticare e, di volta in volta, la sua firma è verificata dalle altre macchine che vogliono interagire con essa o da un sistema centrale di controllo della rete.

Bisogna dire che uno sviluppo più sicuro e la modifica degli interfacciamenti esistenti possono essere molto onerosi, soprattutto quando si tratta di sistemi complessi. Nel caso quindi siano usate password di servizio, sono da considerare come condivise (vedere il paragrafo precedente).

12.6.3 Autorizzazioni

Le autorizzazioni corrispondono alle operazioni che può effettuare una persona su un sistema informatico o su dei dati. Le operazioni sui sistemi informatici possono essere: lettura o visualizzazione di informazioni, modifica di informazioni, utilizzo di programmi software o di loro singole funzionalità, modifica delle configurazioni.

Per gli ambiti fisici le autorizzazioni possono prevedere l'accesso a sedi, locali e archivi.

I principi relativi alle autorizzazioni sono spesso riassunti in tre espressioni inglesi:

minimum privilege: a ciascuno devono essere date solo le autorizzazioni minime di cui ha bisogno, a seconda del suo ruolo, mansioni e responsabilità;

need to know (to use): l'accesso a informazioni, programmi software, strumenti

e archivi deve essere concesso solo a quanti hanno la necessità di accedere a quelle informazioni o usare quegli strumenti o programmi, a seconda del loro ruolo, mansioni e responsabilità;

segregation of duties (separazione dei ruoli): alcune operazioni vanno iniziate, controllate e approvate da persone distinte (paragrafo 12.3.2).

Le autorizzazioni devono essere assegnate, modificate e ritirate secondo un processo ben definito e documentato.

Un processo con queste caratteristiche permette di dimostrare anche come sono state autorizzate le persone al trattamento dei dati personali, come richiesto dalla normativa vigente.

Ci sono diversi modelli per assegnare le autorizzazioni, anche sulla base della classificazione delle informazioni. I due modelli generali più noti sono indicati dai termini discretionary access control (DAC) e mandatory access control (MAC), mentre i due modelli specifici più noti sono il modello Bell-LaPadula e il modello Biba [32, 135].

12.6.3.1 Assegnazione e ritiro delle autorizzazioni

Quando una persona entra o esce da un'organizzazione è necessario gestirne gli accessi ai sistemi informatici, alle sedi, ai locali e agli archivi. Deve essere stabilito un processo affinché gli accessi siano attivati secondo le mansioni ricoperte dalla persona, modificati quando cambia mansione e disattivati quando lascia l'organizzazione.

In alcune organizzazioni, ogni ruolo è controllato dall'ufficio del personale, il solo ad avere i poteri per assegnare o modificare le autorizzazioni, comunicando quanto necessario ai responsabili dei sistemi informatici, a quelli della sicurezza fisica e alle altre funzioni pertinenti (per l'assegnazione o il ritiro di automobili, telefoni, badge, eccetera). Nel caso di consulenti, fornitori, clienti e partner, questa responsabilità può essere assegnata all'ufficio acquisti, all'ufficio vendite o alla persona responsabile del loro contratto.

In altre organizzazioni, l'ufficio del personale e l'ufficio acquisti hanno solo la responsabilità di comunicare la presenza di una nuova persona agli uffici pertinenti affinché gli siano assegnate le autorizzazioni e le apparecchiature base (un computer, l'accesso alla email, alla intranet e alla sede dell'organizzazione). Ulteriori aggiunte o modifiche alle autorizzazioni di base devono essere richieste da alcuni ruoli opportunamente designati, spesso coincidenti con i responsabili di funzione.

Quando si segue questo secondo approccio, si possono presentare i seguenti due casi:

i responsabili di funzione richiedono per i propri collaboratori autorizzazioni molto ampie, non corrispondenti al principio di minimumprivilege, per evitare di doverle modificare quando una persona cambia mansioni all'interno della stessa funzione;

i responsabili di funzione non comunicano quando le autorizzazioni devono essere disabilitate a causa di cambi di mansione; sono molto comuni i casi di persone che, avendo svolto più mansioni all'interno della medesima organizzazione, hanno sempre visto incrementare le proprie autorizzazioni senza che fossero cancellate quelle precedenti, con il risultato di averne di più di certi dirigenti.

Nel caso dei fornitori, le autorizzazioni devono essere impostate in modo che

scadano insieme al contratto, salvo richiesta di prolungamento dell’ufficio acquisti o del responsabile del contratto o di altre funzioni definite a priori. In alcune organizzazioni, per evitare che siano attive più autorizzazioni del necessario, tutte quelle assegnate agli esterni non possono avere durata superiore ai sei o dodici mesi e le richieste di estensione possono essere inoltrate solo poco tempo prima della scadenza.

Sono da prevedere eccezioni: una persona potrebbe avere bisogno di permessi non corrispondenti alla propria mansione perché sostituisce qualcuno temporaneamente o perché partecipa a un progetto o attività particolare e temporanea. In questi casi deve essere stabilito chi può chiedere e approvare queste eccezioni e chi ne tiene traccia. Se gli accessi sono controllati da strumenti automatici, le eccezioni vanno impostate con una scadenza.

Nel caso dei clienti, è necessario stabilire chi attiva i loro utenti. I casi sono due:

il fornitore attiva uno o più utenti amministratori del cliente che a loro volta gestiscono gli utenti finali (solitamente il processo prevede che il commerciale mantenga i rapporti con un unico referente tecnico del cliente che gli comunica gli amministratori da attivare; a sua volta, il commerciale si interfaccia con i propri amministratori di sistema per le opportune configurazioni);

il fornitore agisce come amministratore delle utenze del cliente come se fosse una funzione interna del cliente e quindi le richieste di attivazione degli utenti sono inviate da specifiche persone (p.e. dall’ufficio del personale o dai responsabili di funzione).

Le funzioni pertinenti devono registrare l’assegnatario di ciascun asset nell’apposito inventario (paragrafo 12.5.2) e le autorizzazioni assegnate sui sistemi informatici. Questo permette di ritirare o modificare quanto necessario al momento di un cambio di mansione o di uscita dall’organizzazione di una persona.

Asset particolari sono i token usati per apporre firme e sigilli digitali. In questo caso è necessario stabilire le regole da seguire per il loro utilizzo e vanno esplicitamente delegate le persone autorizzate al loro utilizzo.

Quando una persona lascia l'organizzazione, bisogna seguire un processo inverso a quello descritto in precedenza: l'ufficio del personale o l'ufficio acquisti comunicano quanto necessario agli uffici pertinenti perché provvedano al ritiro degli asset e alla disabilitazione delle autorizzazioni non oltre l'ultimo giorno di collaborazione della persona interessata. È interessante osservare come, sebbene i sistemi informatici permettano di configurare una data di scadenza, in molte organizzazioni si aspetti l'effettiva uscita della persona per disabilitare le autorizzazioni assegnate, con la conseguenza che molte volte rimangono attive per lungo tempo oltre il necessario. Sono molti gli aneddoti su persone che, uscite da un'organizzazione, hanno potuto continuare a consultare da remoto la casella di posta o i documenti condivisi.

Nel caso di uscita di utenti dei clienti, come sopra, va seguito lo stesso processo seguito per l'attivazione, stabilendo chi ha la responsabilità di avviarlo. Per esempio, il referente del cliente può richiedere agli amministratori di sistema la disabilitazione di un'utenza o concordare con il commerciale, che poi coinvolgerà il personale tecnico per le attività operative, la rescissione o il non rinnovo del contratto. Quando un cliente rescinde o non rinnova il contratto, è necessario accompagnare la sua disabilitazione con la cancellazione dei dati, come approfondito al paragrafo 12.9.9.

Il processo di uscita potrebbe prevedere delle eccezioni. Per esempio, la disabilitazione degli accessi ai sistemi più critici nel momento stesso in cui una persona dichiara la propria intenzione di lasciare l'organizzazione, oppure un'estensione di alcuni accessi (per esempio all'email) anche a seguito della conclusione del rapporto di lavoro. Relativamente ai dispositivi, alcune organizzazioni permettono all'utente di acquistarli al termine del rapporto di lavoro e questo va collegato a un processo di cancellazione delle informazioni

(paragrafo 12.8.2.7) e di gestione delle licenze del software installato (vedere anche il paragrafo 12.15.1.3).

12.6.3.2 Riesame delle autorizzazioni

Periodicamente devono essere riesaminate le utenze e le autorizzazioni censite sui sistemi informatici (inclusi quelli di controllo dei meccanismi di sicurezza fisica). Questo perché il processo sopra descritto non sempre funziona.

Questa attività richiede, per ogni sistema informatico, di elencare gli utenti registrati in modo da confrontarli con quelli previsti dall'ufficio del personale, dall'ufficio acquisti e dai responsabili di funzione.

I clienti dovrebbero riesaminare autonomamente le autorizzazioni assegnate al proprio personale e ai propri utenti. È compito dell'organizzazione mettere loro a disposizione report o interfacce per condurre queste verifiche.

I sistemi raramente dispongono di una funzione per ottenere un elenco facilmente leggibile degli utenti e delle loro autorizzazioni. Alcuni hanno realizzato dei programmi per questo scopo, ma a costi molto elevati. Sovente, quindi, si preferisce non fare nulla, con il risultato che sui sistemi rimangono attive utenze o autorizzazioni ormai obsolete.

Analoghi riesami vanno fatti relativamente agli assegnatari degli asset e a coloro in possesso di strumenti e credenziali condivise.

12.6.3.3 Chiavi tradizionali

Le chiavi tradizionali (o chiavi meccaniche) sono strumenti di autenticazione, perché sono qualcosa che una persona ha, e può quindi dimostrare il proprio ruolo, e di autorizzazione all'accesso. Le chiavi possono essere utilizzate per sedi, locali, armadi, eccetera, oppure in caso di emergenza, per esempio quando qualche meccanismo informatico di controllo degli accessi si guasta. Alcuni fornitori possono essere in possesso di chiavi: addetti alle pulizie, manutentori, eccetera.

Le chiavi tradizionali sono strumenti condivisi (paragrafo 12.6.2.7) per i quali stabilire ulteriori regole: quante copie si possono fare (almeno tre: una per il normale utilizzo, una per garantire l'accesso quando la prima non è disponibile e la terza per effettuare delle copie se la prima si rompe), chi può autorizzare qualcuno ad avere una copia delle chiavi, come i possessori delle chiavi sono registrati, come le chiavi vanno restituite, cosa fare quando una chiave è persa o non restituita, vietare le copie alle persone non autorizzate.

12.6.3.4 Gli amministratori di sistema

Gli amministratori di sistema (vedere 12.3.1.3) hanno autorizzazioni molto ampie che permettono loro di eseguire pressoché qualunque operazione sui sistemi e possono attaccare in modo molto efficace l'organizzazione e commettere errori involontari con impatti considerevoli. Per questo motivo è necessario stabilire un processo con responsabilità chiare per selezionare persone con le adeguate competenze e attitudini.

Misure di base prevedono di censire queste figure in un documento insieme al loro ambito di lavoro e di attivare meccanismi di logging sulle loro attività (vedere il paragrafo 12.9.6).

Come per tutti gli utenti esterni, anche nel caso di amministratori esterni si raccomanda di impostare una data di scadenza dell’utenza. Questo è particolarmente importante per i poteri assegnati.

Ogni sistema informatico prevede utenze con poteri assoluti (indicate come root o admin). Sovente tali utenze non possono essere disabilitate, ma non vanno utilizzate salvo casi particolari e le password a esse associate vanno gestite con misure di custodia delle password, in modo che non siano conosciute da un’unica persona. Solitamente sono comunicate a più persone determinate o scritte e archiviate in luogo sicuro ad accesso limitato a poche persone. Di tali persone va mantenuto un elenco e tale responsabilità va formalmente assegnata.

Quando si usano credenziali condivise di amministrazione, vanno seguite le regole descritte al paragrafo 12.6.2.7. In particolare, in caso di uscita o cambio di ruolo di una persona che le conosce, vanno modificate e le nuove credenziali vanno comunicate alle persone autorizzate e ne va aggiornato l’elenco. Il cambio delle credenziali può essere molto complesso se, per esempio, i sistemi informatici coinvolti sono numerosi e non è attivo un meccanismo di single sign on.

Purtroppo molti amministratori trovano comodo utilizzare le utenze di admin per tutte le attività e condividere tra loro le relative password. Questa pratica deve essere scoraggiata perché: un errore commesso con quelle utenze può essere fatale, le utenze condivise non permettono di risalire al responsabile di ciascuna azione (paragrafo 12.9.6), l’organizzazione potrebbe essere sanzionata⁷⁸.

Gli amministratori di sistema dovrebbero disporre di due o più utenze distinte, tra cui una come utente generico per svolgere le normali attività (come visitare siti web, redigere documenti, scambiare email) per cui un errore (per esempio aprire un file o visitare un sito web con del malware) non avrebbe gravi

conseguenze. In molti non adottano questo accorgimento, dimostrando di non essere sufficientemente competenti o attenti.

Alcuni cercano di affrontare questo problema richiedendo agli amministratori di sistema di usare una macchina virtuale, opportunamente configurata in modo sicuro (con tecniche dette di hardening), quando devono svolgere attività di amministrazione. Però questa misura non è ottimale e, anzi, fornisce un falso senso di sicurezza: se infatti il PC di partenza, non configurato attentamente, è compromesso, anche la macchina virtuale viene facilmente compromessa (è infatti consigliabile fare l'inverso: rendere sicuro il computer a cui si accede inizialmente e poi rendere disponibili macchine virtuali meno sicure⁷⁹).

Le attività e le prassi seguite dagli amministratori di sistema sono raramente controllate dai responsabili dell'organizzazione. In molti casi viene detto che si ha fiducia nel proprio personale, in altri casi vengono presentati problemi tecnici “insormontabili” per cui non è possibile assegnare credenziali personali agli amministratori. La verità è che il rischio non viene percepito come tale per la cosiddetta sindrome di Fort Apache: si pensa che i “cattivi” siano tutti fuori, mentre dentro ci sono solo i “buoni” [56].

Esempio 12.6.3. Un amministratore di sistema della rete dati di una società, a seguito di un'azione disciplinare e per ripicca, avendo accesso a tutti i sistemi, ha modificato tutte le password di amministrazione, impedendo l'accesso a tutti gli utenti.

L'organizzazione ha previsto una spesa straordinaria di oltre 1 milione di dollari per far fronte a questo incidente⁸⁰.

12.6.3.5 Installazione di programmi

Le misure relative alla gestione dei cambiamenti in ambito informatico sono al paragrafo 12.9.3.

L'installazione dei programmi software deve essere oggetto di esplicite autorizzazioni. Infatti, ogni programma, installato anche temporaneamente per piccoli test o analisi, può introdurre vulnerabilità e quindi causare comportamenti anomali o essere sfruttato da malintenzionati (vedere esempio 9.3.6).

Esempio 12.6.4. Il software pericoloso non riguarda solo i computer, ma ogni dispositivo.

Nel 2016, le prime versioni del popolarissimo gioco per dispositivi mobili Pokemon GO richiedevano accesso completo ai dati presenti sui dispositivi. La casa produttrice segnalò che si era trattato di un errore (poi effettivamente corretto), ma in molti sospettarono che la Nintendo volesse raccogliere dati per successive finalità di marketing⁸¹.

Esempio 12.6.5. Molte applicazioni per dispositivi mobili si sono dimostrate pericolose, anche quelle di utilità, e periodicamente sono individuate applicazioni con malware sui sistemi di distribuzione di software per dispositivi mobili⁸².

Bisogna distinguere tra due gruppi di utenti che potrebbero installare software: gli utenti generici e gli amministratori di sistema.

È possibile impedire agli utenti generici l'installazione di software non autorizzato emanando regole comportamentali, purtroppo non sempre seguite nella pratica. Un metodo efficace consiste nella configurazione dei computer loro assegnati in modo che solo gli amministratori di sistema possano installare del software, spesso attraverso un sistema centralizzato di distribuzione e aggiornamento. È quindi da stabilire una procedura affinché ogni utente possa chiedere agli amministratori di sistema di installare nuovo software e questi eseguano il cambiamento secondo il processo stabilito (paragrafo 12.9.3).

Per gli amministratori di sistema il blocco dei computer è più difficile da garantire perché essi stessi devono poter installare software sui server e sui PC. A tal fine, la prima misura consiste nello stabilire una lista precisa dei programmi autorizzati (incluse le backdoor, le exit e gli strumenti di amministrazione che possono aggirare gli altri meccanismi di sicurezza) e la pubblicazione di regole precise. Oltre a ciò, sono da attivare i log per registrare le installazioni fatte.

Molti amministratori di sistema installano nuovi programmi sui PC e sui server per verificarne le funzionalità. È quindi opportuno mettere loro a disposizione un laboratorio isolato dagli altri sistemi (oggi facilmente realizzabile grazie alle tecniche di virtualizzazione).

12.7 Crittografia

Il termine crittografia indica gli strumenti che permettono di rendere inintelligibili (ossia cifrare) messaggi in modo tale che siano comprensibili solo a persone designate (che li possono quindi decrittare o decifrare).

Per cifrare un messaggio occorre un algoritmo crittografico, ossia una funzione matematica, e una chiave crittografica, ossia una variabile. Un messaggio viene cifrato utilizzando l'algoritmo insieme alla chiave; per decifrare il messaggio, il destinatario deve conoscere l'algoritmo e la chiave per decifrarlo.

La crittografia è utilizzata per diverse finalità, collegate a molti controlli di sicurezza. Le finalità sono le seguenti:

controllo degli accessi ai dati digitali memorizzati su hard disk di PC o server, chiavette USB, supporti di backup, strumenti portatili come smartphone o tablet, eccetera;

controllo degli accessi ai dati trasmessi, in modo che, se intercettati, i malintenzionati non possano interpretarli (quasi tutti i servizi Internet instaurano una connessione cifrata tra utente e server quando sono richieste delle credenziali di autenticazione o un numero di carta di credito); la crittografia, in questo contesto, permette anche un migliore controllo della correttezza dei dati trasmessi perché eventuali corruzioni impediscono la decifrazione e il destinatario deve chiedere la ritrasmissione;

generazione di numeri casuali (più propriamente detti semi-casuali), cifrando successivamente dei numeri in modo da rendere non prevedibile la sequenza se non si hanno a disposizione le variabili iniziali;

cancellazione sicura dei dati, sovrascrivendoli con numeri casuali;

firma di messaggi [138];

marcatura temporale di messaggi, ossia il loro collegamento con un riferimento temporale certo.

Il principio di Kerckoff stabilisce che la sicurezza della crittografia non è garantita dalla segretezza dell'algoritmo, ma della chiave; questo principio è valido soprattutto al giorno d'oggi perché necessariamente gli algoritmi devono essere condivisi tra molteplici entità che comunicano tra loro. La robustezza del messaggio cifrato è quindi garantita dal mantenimento della segretezza della chiave da parte degli interlocutori.

Conoscendo l'algoritmo, se un malintenzionato intercetta un messaggio cifrato, potrebbe cercare di decifrarlo provando tutte le possibili combinazioni di chiavi (attacco brute force). Ovviamente, più lunga è la chiave utilizzata, più tempo, fino a diversi anni, è richiesto all'attaccante per individuarla. La lunghezza della chiave è quindi un parametro molto importante.

In alcuni algoritmi sono state individuate delle vulnerabilità che permettono di limitare il numero di chiavi da provare in un attacco a forza bruta e per questo sono ritenuti insicuri.

Dato che i computer sono sempre più potenti e permettono di effettuare sempre più velocemente gli attacchi a forza bruta e di individuare vulnerabilità negli algoritmi, è necessario un continuo aggiornamento delle liste di algoritmi ritenuti sicuri anche perché capaci di gestire chiavi sempre più lunghe. Il Governo USA effettua periodicamente delle analisi sugli algoritmi da considerare standard crittografici [130].

12.7.1 Algoritmi simmetrici e asimmetrici

Quando due persone intendono scambiarsi messaggi cifrati, devono concordare l'algoritmo da utilizzare e la relativa chiave crittografica. Scambiarsi una chiave

crittografica senza che venga intercettata da un malintenzionato non è compito facile, soprattutto se gli interlocutori sono tra loro distanti e non hanno la possibilità di incontrarsi di persona.

Nel 1976 [30] sono stati inventati algoritmi che permettono agli interlocutori di cifrare con una chiave (la chiave pubblica) e di decifrare con un'altra chiave (la chiave privata): chi vuole inviare un messaggio cifrato a una persona deve conoscere la sua chiave pubblica e glielo invia; il destinatario sarà l'unico a poter decifrare il messaggio con la propria chiave privata. Questi algoritmi sono detti algoritmi crittografici a chiave pubblica o algoritmi crittografici asimmetrici.

In precedenza venivano usati solo algoritmi per i quali è necessario usare la medesima chiave per cifrare e decifrare. Questi algoritmi sono detti algoritmi crittografici a chiave privata o algoritmi crittografici simmetrici

L'uso di algoritmi asimmetrici richiede molta più potenza computazionale di quella basata su algoritmi simmetrici perché sono necessarie chiavi crittografiche molto più lunghe. Al momento dell'uscita di questo libro sono ritenuti sicuri algoritmi simmetrici con chiavi lunghe almeno 256 bit, mentre per quelli asimmetrici sono necessarie chiavi di almeno 2048 bit.

Per le comunicazioni sono utilizzate combinazioni di algoritmi asimmetrici e simmetrici: i primi sono usati solo per scambiarsi le chiavi da usare con gli algoritmi simmetrici; questi sono poi usati per tutto il resto della comunicazione.

Senza entrare troppo nei dettagli, è anche opportuno segnalare che la crittografia a chiave pubblica è alla base dei meccanismi di firma digitale: se una persona cifra un messaggio con la propria chiave privata, poiché ne è l'unico possessore, dimostra la propria identità.

12.7.2 Le funzioni hash

Le funzioni hash furono introdotte nei primi anni '50 per verificare eventuali errori di trasmissione e senza scopi crittografici. Esse trasformano messaggi di lunghezza qualsiasi in stringhe di lunghezza predefinita. Oggi con il termine di hash si intendono le funzioni hash a senso unico che hanno, tra le altre, le seguenti proprietà:

il risultato di una funzione hash ha sempre la medesima lunghezza;

se h è il risultato della funzione hash di m , è difficile, avendo solo h , ricavare m ;

se h è il risultato della funzione hash di m , è difficile trovare un altro messaggio m_1 che dia come risultato della funzione hash lo stesso h (in questo caso, m_1 sarebbe una collisione).

Spesso si indica come hash direttamente il risultato di una funzione hash.

12.7.3 Protocolli crittografici

L'insieme degli algoritmi da utilizzare per le diverse finalità e dei requisiti di lunghezza delle chiavi prende il nome di protocollo crittografico.

I protocolli crittografici includono meccanismi affinché gli interlocutori di una comunicazione possano riconoscersi tra loro. Tra i diversi meccanismi disponibili vi sono i certificati digitali, emessi e firmati digitalmente da una certification authority (CA).

I certificati digitali hanno scadenze e costi di mantenimento. Recentemente sono disponibili servizi gratuiti da parte di alcune CA⁸³, nate con lo scopo di mantenere più sicuro Internet, visto che molti siti non usano i certificati digitali a causa dei loro costi.

Per qualsiasi ambito di utilizzo della crittografia, si deve stabilire e documentare: quali protocolli e quali software crittografici utilizzare.

12.7.4 Chiavi crittografiche

Per la gestione delle chiavi crittografiche, si deve stabilire e documentare:

chi ha l'autorizzazione per generare, cambiare o aggiornare le chiavi crittografiche;

come devono essere generate, distribuite, conservate e infine distrutte queste chiavi;

come garantire il recupero delle chiavi in caso vengano perse;

come gestire la sicurezza dei dati cifrati quando l'algoritmo utilizzato inizialmente non è più ritenuto sicuro.

Dall'elenco sopra riportato, due elementi richiedono un approfondimento. Il primo riguarda le modalità di conservazione delle chiavi: devono essere memorizzate in modo che siano sicure (oggi si utilizzano smart card molto resistenti agli attacchi fisici e informatici, come le SIM dei cellulari, oppure delle chiavi USB configurate in modo particolare) e ad accesso controllato (spesso si

utilizza un PIN, che dovrà essere mantenuto segreto e gestito come una password). In alcuni contesti, per esempio quando si parla di transazioni con carte di credito o di firme digitali con valore legale, sono utilizzate macchine hardware particolari per la generazione e conservazione delle chiavi (hardware security module o HSM), tali da essere difficilmente violabili grazie a controlli di accesso volti a evitare abusi da parte degli operatori o di malintenzionati (per esempio richiedendo la presenza di almeno tre persone autorizzate).

Il secondo elemento riguarda il recupero delle chiavi crittografiche nel caso vadano perse. Il meccanismo normalmente utilizzato prevede di depositarne una copia, a sua volta protetta, presso un’entità fidata (in Italia si usano spesso i notai). Un meccanismo più sicuro prevede di depositare parti distinte delle chiavi presso diverse entità fidate. Questi meccanismi prendono il nome di key escrow.

12.7.5 Servizi fiduciari

La crittografia, come già detto, permette di firmare documenti, verificare la validità di tali firme e apporre marche temporali. Questi meccanismi possono essere approvati da specifiche autorità in modo che abbiano validità legale. Questi sono detti servizi fiduciari(vedere il paragrafo 12.15.1.7). Anche con i fornitori di tali servizi è necessario stabilire contrattualmente le reciproche responsabilità e i livelli di sicurezza e servizio.

Un servizio fiduciario particolare è quello del “deposito in garanzia”, più noto con il termine inglese di escrow, di materiale in formato digitale. Esso fa uso di algoritmi crittografici.

Esempio 12.7.1. Un’organizzazione compra un programma software sviluppato da un suo fornitore. Per evitare di non poter più aggiornare il

software nel caso in cui il fornitore dovesse fallire, gli chiede di consegnargli anche il codice sorgente. Il fornitore potrebbe rifiutarsi per evitare di consegnare un proprio segreto industriale.

Per ovviare a questa situazione, il fornitore consegna al cliente il codice sorgente dopo averlo cifrato e consegna a un'entità fidata una copia della chiave utilizzata per la cifratura.

Così facendo, se il fornitore dovesse fallire e l'organizzazione avesse bisogno del codice sorgente, potrebbe far valere il proprio diritto presso l'entità fidata che consegnerà la chiave per decifrare il codice sorgente.

12.7.6 Normativa applicabile alla crittografia

Alcuni Paesi limitano l'uso della crittografia arrivando a considerarla come arma; ciò non si applica all'Italia. Ogni organizzazione dovrebbe analizzare la normativa applicabile alla crittografia. Se scambia messaggi con altre organizzazioni in altri Paesi, dovrebbe considerare la normativa applicabile in tutti i Paesi.

Più complesso è il tema delle firme digitali. Quando queste sono legalmente riconosciute, anche in sostituzione della firma autografa, devono essere conformi a specifiche normative e standard tecnici, in continua evoluzione. I protocolli richiedono il coinvolgimento di almeno tre entità: l'utente, un'organizzazione che emette il dispositivo di firma (autorità di registrazione) e una che ne attesta la validità (certificatore di firma digitale).

In Europa, le firme digitali e i servizi fiduciari sono oggetto del Regolamento eIDAS (vedere paragrafo 12.15.1.7).

In Italia, vi è un'autorità nazionale preposta alla redazione delle regole tecniche⁸⁴ e alla messa a disposizione della normativa italiana ed europea aggiornata.

12.8 Sicurezza fisica

Quando si parla di sicurezza fisica bisogna distinguere tra la sicurezza della sede, delle apparecchiature e degli archivi.

È opportuno ricordare che le misure relative alla salute e sicurezza delle persone non sono oggetto di questo libro, anche se sono importantissime.

12.8.1 Sicurezza della sede

La sicurezza della sede inizia dalla recinzione esterna, dove applicabile, continua con il controllo accessi all'interno della recinzione, poi all'edificio e infine ai singoli uffici.

12.8.1.1 Perimetro di sicurezza fisica

Il perimetro è delimitato da mura, cancellate, grate e mura (controlli passivi).

Bisogna determinare come disporre gli ingressi e, quindi, gli uffici, gli archivi e le sale server, in modo da garantire un'adeguata protezione.

Le agenzie bancarie forniscono un ottimo esempio: vi è un'area aperta al pubblico, un'area più interna per gli uffici il cui accesso è permesso al solo personale interno, il caveau a cui possono accedere solo alcuni impiegati e i clienti con cassette di sicurezza, le singole cassette di sicurezza all'interno del caveau a cui possono accedere solo i singoli clienti. Allo stesso modo andrebbero disposti gli uffici e le aree di un'organizzazione: nei pressi dell'ingresso gli uffici dove sono trattate informazioni meno critiche e poi, sempre più lontano, le aree più critiche, incluse quelle dove sono disposti i server e altre apparecchiature informatiche.

Lungo il perimetro ci sono uscite di sicurezza e finestre. Queste dovrebbero essere allarmate per segnalare se sono lasciate aperte quando non presidiate.



Figura 12.8.1:

Porta lasciata aperta senza autorizzazione e, evidentemente, non allarmata

12.8.1.2 Sicurezza ambientale

La sede deve essere progettata per far fronte alle minacce fisiche naturali, a seconda di dove è posizionata: incendi, allagamenti, terremoti, eccetera.

Per gli incendi devono essere presenti rilevatori di fumo ed estintori di incendio, automatici o manuali. Quelli automatici sono da evitare negli ambienti dove il materiale può essere compromesso dal sistema di spegnimento (oggi sono comunque diffusi sistemi basati su gas, che vanno valutati anche considerando la sicurezza delle persone). In Italia le organizzazioni devono avere un CPI (certificato prevenzione incendi), rilasciato dai Vigili del fuoco, o un'analisi che ne attesti la non necessità.

Per gli allagamenti, oltre a prestare attenzione a dove sono situate le tubature e porre il materiale deperibile (come archivi cartacei e sistemi informatici) su ripiani o pavimenti soprelevati, è possibile prevedere sensori per la presenza di acqua e pompe per raccoglierla.

In alcune aree geografiche è necessario verificare se l'edificio è antisismico o presenta accorgimenti per evitare di restare isolato a causa della neve.

Se l'organizzazione può essere oggetto di attacchi violenti, inclusi quelli terroristici, è necessario prevedere un perimetro robusto, per esempio in muratura e con vetri antisfondamento.

Deve essere previsto un piano di evacuazione da attuare in caso di incendi e terremoti. Esso deve sempre mettere al centro la sicurezza delle persone. È però opportuno che raccomandino, per quanto possibile, di assicurarsi di aver bloccato i PC e chiuso archivi e casseforti.

12.8.1.3 Controllo degli accessi alla sede e ai locali

Per evitare l'accesso di persone non autorizzate alla sede e alle aree interne è possibile affidarsi a personale addetto alla vigilanza affinché verifichi ogni singola persona, oppure a porte chiuse, tornelli, bussole o altri meccanismi anti pass back per impedire il passaggio di più persone contemporaneamente.

Per l'accesso sono necessari meccanismi di identificazione, autenticazione e autorizzazione, tra cui chiavi, tessere di riconoscimento, smart card, PIN, verifica delle impronte digitali o della geometria della mano. Per questi meccanismi e i relativi processi di assegnazione, cambiamento e ritiro, vedere il paragrafo 12.6.

Quando si usano strumenti automatici, per evitare abusi è buona pratica programmarli in modo da bloccare le entrate a chi non risulta essere uscito.

Gli accessi e le uscite dovrebbero essere registrate per esempio per sapere chi era presente nel caso sia rilevato un reato o un incidente o per verificare che tutte le persone sono uscite a fine giornata o in caso di evacuazione.

Molte organizzazioni richiedono alle persone presso le proprie sedi di tenere in vista una tessera (o badge), in modo da riconoscere il personale interno, i fornitori abituali e i visitatori, oppure le persone con diritto di accesso a determinate aree. Si osservi che, solitamente, i primi a non esibire il proprio badge sono i dirigenti, dando così un pessimo esempio al personale.

Alle persone, inclusi fornitori abituali e ospiti (per esempio, addetti alle pulizie, spesso trascurati quando si tratta di sicurezza delle informazioni, tenuto conto della libertà di movimento di cui godono), devono essere distribuite regole di comportamento, tra cui: cosa fare in caso di emergenza, tenere sempre il badge visibile, non fare mai accedere alla sede e ai locali altre persone (inclusi coloro che asseriscono di avere dimenticato badge o chiavi).

12.8.1.4 Visitatori

L'accesso alla sede degli ospiti e dei fornitori è sovente controllato dal personale di reception: l'ospite si presenta dice con chi ha appuntamento e la reception contatta la persona indicata affinché venga per accompagnare l'ospite.

Non è necessario chiedere un documento di identità all'ospite (soprattutto se la persona con cui ha appuntamento lo riconosce), ma è sicuramente più pratico per poterne comunicare correttamente il nome; non è necessario prendere nota del nome del visitatore, anche se utile per verificare che tutti siano usciti alla chiusura o in caso di evacuazione; e nemmeno richiedere al visitatore di esibire un badge, soprattutto se il personale interno non lo fa e al visitatore basta mettersi il badge in tasca per non palesare il proprio ruolo.

L'ospite deve essere sempre accompagnato quando accede ad aree non aperte al

pubblico e ricevere regole di comportamento da rispettare tra cui: cosa fare in caso di allarme, non utilizzare materiale e trattare informazioni senza il permesso del proprio referente interno, non utilizzare eventuali connessioni wi-fi per finalità estranee alla propria visita.

12.8.1.5 Aree di consegna e ritiro di materiali

Attenzione va rivolta ai trasportatori e agli addetti della manutenzione di qualsivoglia tipo: molto spesso sono lasciati soli, con possibili effetti indesiderati. È successo di non trovare più il proprio PC in ufficio dopo che era uscita una persona “entrata per consegnare una lettera” senza che della lettera vi fosse traccia.

12.8.1.6 Controllo del materiale in uscita

Quando qualcuno esce dalla sede dell’organizzazione, sarebbe da verificare che non abbia con sé del materiale senza autorizzazione.

Ciò è molto difficile da attuare. In alcune organizzazioni si registra il numero di serie dei PC dei visitatori per verificare all’uscita che non ne abbiano altri. Spesso questa misura è inefficace perché non accompagnata da una verifica delle borse, peraltro assimilabile alla perquisizione e quindi raramente permessa; la sua unica utilità è dare un falso senso di sicurezza a chi l’ha introdotta.

12.8.1.7 Antintrusione e videosorveglianza

Per evitare intrusioni si possono utilizzare meccanismi tradizionali (detti passivi), come le grate alle finestre, e sistemi di rilevamento delle intrusioni e di allarme (detti attivi).

L'attivazione e disattivazione dei sistemi di antintrusione è spesso controllata da codici condivisi, da gestire come riportato nel paragrafo 12.6.2.7.

La videosorveglianza non è utilizzata solo per antintrusione, ma anche per il controllo di alcuni ambienti di lavoro o aperti al pubblico. Per esempio, è diffusa nelle organizzazioni in cui si trattano grandi quantità di denaro contante o negli esercizi commerciali.

Per i sistemi di videosorveglianza è sempre necessario seguire quanto prescritto dalle normative relative al trattamento dei dati personali (paragrafo 12.15.1.9) e alla tutela dei lavoratori: segnalare la presenza delle telecamere, controllare gli accessi ai monitor e alle registrazioni e cancellare le registrazioni dopo alcuni giorni.

12.8.1.8 Uffici, stanze e aree di servizio

Gli uffici, le stanze e le aree di servizio devono essere protette con misure di controllo accesso e ambientali (per esempio rilevatori fumi, estintori di incendi, eccetera) già descritte in precedenza.

Le misure di controllo accesso devono essere applicate per le aree di servizio (per esempio quelle che ospitano i generatori, i quadri elettrici, la strumentazione informatica), non solo per prevenire attacchi ma anche danni accidentali.

Oggi molti uffici sono organizzati come open space, ma questo deve essere attentamente valutato in alcuni casi, come quello che riguarda l'ufficio del personale o altri uffici critici. Per questi uffici sono spesso applicate misure di isolamento e di controllo degli accessi.

È bene evitare di avere troppe persone in un ufficio (almeno per evitare danni involontari dovuti al poco spazio a disposizione) o materiale troppo pesante sul pavimento. L'eccesso di persone e materiale deve essere evitato perché può comportare un insufficiente raffreddamento da parte del sistema di aria condizionata.

Se sono trattate informazioni riservate, queste non dovrebbero essere visibili dalle finestre. Nei piani bassi possono essere usate pellicole adesive per mascherare le attività dall'esterno e, allo stesso tempo, far entrare la luce naturale.

In molti casi, spesso la notte o nei fine settimana o durante le vacanze, molti lavoratori, inclusi gli amministratori di sistema, sono soli. Misure per questo personale solitario includono allarmi nel caso in cui una persona abbia un incidente e chiamate periodiche per verificare che non ci sono problemi.

12.8.1.9 Aree speciali

Per alcune aree, come il CED, possono essere stabilite regole specifiche per il controllo degli accessi e di comportamento. Queste ultime possono essere comunicate attraverso cartelli e includere il divieto di bere, mangiare, introdurre telefoni cellulari o smartphone, prendere fotografie o registrare audio e video.

12.8.2 Sicurezza delle apparecchiature

Le apparecchiature possono essere server, PC e altri dispositivi informatici e strumenti di ufficio come stampanti o fax.

12.8.2.1 Disposizione delle apparecchiature

Le apparecchiature dovrebbero essere disposte su pavimenti flottanti, a distanza da condutture di liquidi, in locali ad accesso limitato, per evitare quello di estranei e i danni dovuti a disattenzione, con rilevatori di fumo e di allagamento e con sistemi di spegnimento degli incendi.

In organizzazioni dove agenti chimici o polvere possono essere pericolosi sono da adottare ulteriori cautele come pellicole per proteggere le tastiere, gli schermi e i cavi.

I server e gli apparati di rete sono normalmente posti in appositi armadi detti rack, a loro volta in locali ad accesso limitato (detti centri elaborazione dati, CED, sale server, sale macchine o data center). Tali sale, quando possibile, andrebbero poste in un'area interna dell'edificio in modo da ridurre al minimo gli accessi non autorizzati. Sono numerosi i casi in cui il CED è posto in un piano seminterrato o interrato; in questo caso va analizzato e valutato il rischio di allagamento.

Nei CED, come in tutte le aree speciali, devono essere rispettati i divieti di mangiare, bere e fumare.

In molti edifici, alcune apparecchiature sono disposte fuori dai CED, in particolare alcuni apparati di rete. Anche per esse bisogna prevedere un controllo degli accessi e un posizionamento tale da evitare incidenti (per esempio, in rack sopraelevati e lontani da finestre e dai distributori del caffè).

I rack dovrebbero essere sempre chiusi e anonimi, in modo da non facilitare eventuali malintenzionati. La chiusura dei rack è importante nei CED condivisi con altri, anche per evitare che un addetto alla manutenzione acceda, inavvertitamente o volontariamente, alle apparecchiature sbagliate. Nei CED non condivisi non è sempre necessario chiudere a chiave i rack. In tutti i casi è sempre opportuno accompagnare o monitorare con sistemi di videosorveglianza i visitatori e manutentori e prevedere la presenza di almeno due persone per prevenire eventuali confusioni in fase di manutenzione.

Esempio 12.8.1. In un CED di una pubblica amministrazione, nel 2019, un manutentore esterno doveva sostituire un disco di un server. Fece confusione e staccò un disco di un altro server, causando il fermo dei servizi per qualche ora.

12.8.2.2 Infrastrutture e CED

Nei CED, l'aria condizionata, i rilevatori di fumo e di allagamento, gli estintori di incendi e le telecamere di sorveglianza sono posizionati con particolare cura. Questi impianti e l'alimentazione sono duplicati o triplicati in modo che un'avaria non interrompa il loro servizio e sono collegati ad allarmi in modo che eventuali malfunzionamenti vengano affrontati tempestivamente.

I CED devono garantire l'alimentazione elettrica delle apparecchiature e degli impianti. Normalmente questo avviene attraverso la connessione a più fornitori di energia, l'uso di UPS (uninterruptible power supply) e batterie tampone (per protezione da brevi black-out o discontinuità elettriche) e generatori elettrici (per protezione in caso di lunghi black-out, purché sia garantita la disponibilità di combustibile per alimentarli).

UPS, batterie e generatori devono avere la potenza necessaria per sostenere tutte le apparecchiature a essi collegate e il sistema di condizionamento deve assicurare la sua capacità di raffreddamento. Pertanto questi impianti vanno costantemente verificati e monitorati, soprattutto quando si introducono nuove apparecchiature nel CED. Discorso analogo riguarda lo spazio, che deve essere monitorato per assicurarne la disponibilità.

Per tutte le apparecchiature critiche e gli impianti del CED ci si dovrebbe informare sul tempo medio previsto tra le avarie (mean time between failures, MTBF), in modo da effettuare l'opportuna manutenzione e sostituirli quando indicato. Questo dato non è però generalmente noto a causa della continua evoluzione tecnologica.

12.8.2.3 Mautenzione degli impianti

Tra gli impianti vi sono quelli di: rilevazione ed estinzione incendi, aria condizionata, ventilazione, riscaldamento, rilevazione e trattamento allagamenti, telesorveglianza, impianti elettrici, batterie e UPS, generatori elettrici, porte tagliafuoco, sistemi di antintrusione e allarmi fisici, ascensori, termometri e igrometri, apparati di telecomunicazione.

Tutti questi meccanismi, per garantirne l'operatività ed evitare alcuni rischi (per esempio, alcune UPS diventano esplosive se la carica è inferiore a certi livelli),

devono essere regolarmente mantenuti secondo le istruzioni del loro produttore o secondo la normativa vigente. Da predisporre un programma di manutenzione per verificare le scadenze, tenere traccia degli interventi fatti e dei fornitori coinvolti.

Da monitorare la continua adeguatezza degli impianti, considerandone l'eventuale obsolescenza e valutando se garantiscono le prestazioni previste.

Esempio 12.8.2. In un'azienda dedicata all'hosting di sistemi informatici, a seguito dell'acquisizione di nuovi clienti e dell'introduzione delle loro apparecchiature nel CED, le UPS non potevano più erogare la potenza energetica richiesta in caso di necessità, il che provocò un'interruzione del servizio al primo blackout.

I manutentori esterni, anche in caso di emergenza, quando accedono alla sede per svolgere le loro attività, sono da trattare come visitatori (paragrafo 12.8.1.4).

Oggi molte attività di manutenzione sono fatte da remoto. In questi casi è necessario limitare il più possibile l'accesso dei manutentori esterni alla rete informatica dell'organizzazione.

Per ridurre i rischi, le seguenti misure sono spesso applicate:

la connessione da remoto è controllata da un firewall, che viene configurato solo dal personale dell'organizzazione (non del manutentore) affinché l'accesso sia concesso di volta in volta per un limitato periodo di tempo;

eventuali connessioni che rimangono aperte sono solo quelle in uscita per inviare allarmi al manutentore;

le credenziali per accedere all’impianto sono create dall’organizzazione, anche per evitare che il manutentore usi le stesse usate per altri impianti di altri clienti;

il personale dell’organizzazione sorveglia le attività svolte dal manutentore.

12.8.2.4 Cablaggio

Per i cavi di alimentazione elettrica e di telecomunicazione, le buone norme prevedono che siano:

disposti in canaline sotto un pavimento flottante o aeree per evitare danneggiamenti involontari;

disposti in canaline corazzate se transitano fuori dalla sede per evitare manomissioni volontarie (tampering) o danneggiamenti da parte di ruspe o martelli pneumatici quando sono effettuati scavi;

disposti in canaline distinte per il cablaggio di alimentazione e quello di telecomunicazione a evitare interferenze reciproche;

protetti dai roditori con veleni o mediante canaline adeguatamente resistenti;

corredati di etichette (soprattutto se molto lunghi) all’inizio e alla fine per poterne comprendere rapidamente la funzione.

Quando possibile, per garantire la disponibilità dei sistemi, il cablaggio tra le apparecchiature e gli apparati sono duplicati.

Come già ricordato, gli armadi (o rack) dove sono disposti gli apparati (per esempio switch) vanno tenuti chiusi a chiave, a meno che non siano in un CED dedicato, già ad accesso controllato.

12.8.2.5 Apparecchiature e impianti fuori sede

Esempi di apparecchiature installate fuori sede sono i terminali Bancomat (o ATM, automated teller machine), le biglietterie automatiche, i totem informativi, le antenne, i PC usati presso i cantieri temporanei.

Per evitare furti e danneggiamenti, vanno previste misure di sicurezza supplementari rispetto a quelle previste per le apparecchiature disposte in sede.

La misura più semplice consiste nel disporre queste apparecchiature in luogo visibile alle persone incaricate del controllo. Casi più complessi, applicabili agli ATM, richiedono specifiche di costruzione molto rigorose a evitare che siano alterati o manomessi (tampering).

Per i dispositivi portatili, vedere il paragrafo 12.9.8.

I CED esterni ospitano apparecchiature fuori sede. Per questi valgono le stesse regole dei CED interni, tranne che i rack devono essere chiusi a chiave e le chiavi gestite appropriatamente (in particolare, non devono rimanere attaccate al rack, come spesso succede). In alcuni casi, i rack hanno allarmi e telecamere che si attivano ogni volta che la porta viene aperta.

12.8.2.6 Sicurezza dei supporti

I supporti da considerare sono le schede SD, le chiavi USB, i CD, i DVD, eccetera. Per la conservazione dei supporti e dei documenti cartacei, vedere il paragrafo 12.8.3.

Per i supporti digitali bisogna indicare quando cifrarli e mettere a disposizione i software necessari per farlo e le relative istruzioni. Bisogna anche fornire regole per i supporti:

se consegnati ad altri, devono contenere solo le informazioni a cui sono autorizzati ad accedere,

devono essere cancellati in modo sicuro a trasferimento concluso (vedere il paragrafo successivo).

Per alcuni supporti è possibile verificarne il degrado e l'obsolescenza. In particolare, i software usati per i backup conteggiano il numero di volte in cui un supporto è stato riutilizzato e, superato un certo limite, ne richiedono la sostituzione.

I supporti vanno etichettati per poterne riconoscere il contenuto e, in alcuni casi, le modalità per poter accedere al contenuto (per esempio il software e la versione da usare). Le etichette vanno poste considerando che potrebbero richiamare attenzioni non desiderate (per esempio se riportano diciture come “segreto”).

Per il trasporto dei supporti, si veda il paragrafo 12.10.4.3.

12.8.2.7 Dismissione, riuso e cancellazione delle apparecchiature e dei supporti

Tutte le apparecchiature, quando dismesse, assegnate a un nuovo utilizzatore o consegnate a un fornitore (per esempio per manutenzione o alla conclusione del noleggio), devono essere opportunamente ripulite da dati o informazioni riservate.

Questa attività riguarda, tra gli altri, computer, stampanti, scanner, fax, cellulari, smartphone, tablet e memorie esterne.

Per evitare il recupero dei dati cancellati, è necessario modificare tutti i bit del supporto di memoria con software di wiping o erasing. Particolare attenzione va posta su certe tecnologie; per esempio per gli hard disk tradizionali vanno usati sistemi di wiping diversi da quelli per SSD⁸⁵.

Nel 1996 un articolo sostenne che, per rendere veramente irrecuperabili dei dati, è necessario sovrascriverli almeno 35 volte [61]. Per gli hard disk di oggigiorno questo non è più vero e, anzi, li danneggia: un'unica sovrascrittura è sufficiente. Solo in casi veramente critici, per cui dei malintenzionati dispongono di tempo e risorse notevoli e possono ricorrere ad analisi con microscopio elettronico, sono consigliate più sovrascritture.

Metodi alternativi prevedono la smagnetizzazione della memoria con un degausser o la prosaica distruzione fisica con un martello. Il secondo metodo, ovviamente, non consente il riutilizzo della memoria.

Per dispositivi come stampanti, scanner, fax, cellulari, smartphone e tablet, per una cancellazione sufficientemente sicura, è raccomandato l'uso della funzionalità di ripristino alle condizioni di fabbrica (factory reset) [102]. Una strada più sicura prevede la distruzione della memoria, ma non sempre può essere seguita a causa di difficoltà tecniche o perché il dispositivo non è di proprietà dell'organizzazione o il contratto di manutenzione lo vieta.

Per i dispositivi cartacei (e anche per CD e DVD), sono disponibili apparecchi per distruggerli. Essi devono essere selezionati a seconda della criticità delle informazioni, visto che la condizione, la forma e la dimensione del supporto dopo la distruzione varia a seconda della macchina suata (per esempio possono essere strisce o particelle di varie dimensioni). La ISO/IEC 21964 è usata per classificare le macchine di distruzione dei supporti.

12.8.2.8 Schermatura magnetica

Per evitare l'intercettazione delle radiazioni magnetiche di schermi o tastiere, si utilizzano protezioni basate sul principio della gabbia di Faraday. I meccanismi più efficaci seguono le specifiche cosiddette Tempest della NATO [155].

Le apparecchiature vendute in Europa, dovendo rispettare le Direttive in materia di emissioni elettromagnetiche, riducono già notevolmente la possibilità di una loro intercettazione o di interferenze con altre apparecchiature. Per i cavi di telecomunicazione posti in ambienti non protetti è sempre necessario verificarne la schermatura.

In ambiti molto critici come i CED, alcuni vietano di portare cellulari, smartphone o altri dispositivi elettronici perché potrebbero interferire con le apparecchiature.

12.8.3 Archivi fisici

Gli archivi fisici possono essere utilizzati per conservare documenti su supporto non digitale (carta, fotografie, microfiche, eccetera) o digitale (hard disk, nastri, CD, DVD, eccetera).

Per il trasporto dei documenti su supporto non digitale, si veda il paragrafo 12.10.4.3.

12.8.3.1 Controllo accesso agli archivi fisici

L'accesso agli archivi fisici va regolamentato attraverso l'assegnazione di opportune autorizzazioni (paragrafo 12.6). I meccanismi di controllo degli accessi possono essere condivisi, come chiavi tradizionali o combinazioni (paragrafi 12.6.2.7 e 12.6.3.3), oppure personali, come quelli basati sulla lettura di tessere magnetiche, smart card o caratteristiche biometriche.

Se i documenti e i supporti contengono informazioni molto diverse tra loro e con diversi livelli di criticità, può essere necessario disporli in archivi distinti e con differenti autorizzazioni per l'accesso.

12.8.3.2 Sicurezza dei documenti

I documenti devono essere conservati in locali con temperatura e umidità controllate, sistemi di rilevamento fumi e spegnimento incendi, su scaffali

soprelevati per evitare i danni da allagamento.

Per la sicurezza dei documenti bisogna anche considerare fax e stampanti, disporli in aree ad accesso limitato e richiedere che vengano ritirati i documenti il prima possibile (per questo è anche possibile bloccarli fino a quando non viene inserito un PIN personale direttamente sull'apparecchio, in modo da dimostrare la presenza fisica dell'utilizzatore).

12.8.3.3 Scrivania pulita

Nella sede di lavoro tutti i documenti vanno conservati negli archivi e sulla scrivania devono essere presenti solo quelli strettamente indispensabili; questo per evitare che persone non autorizzate li possano leggere. Questa regola è detta clear desk policy.

In questo ambito sono incluse ulteriori misure: verificare di non aver lasciato documenti riservati nelle sale alla conclusione di una riunione, di aver pulito completamente le lavagne (anche quelle digitali) e di non aver lasciato tracce sui fogli inutilizzati delle lavagne a fogli mobili o dei taccuini.

12.9 Conduzione dei sistemi informatici

Sovente, la conduzione dei sistemi informatici viene indicata come IT operations o solo operations quando è implicito il riferimento ai sistemi informatici. Si usa anche il termine esercizio.

Oggi sono sempre più diffusi impianti e oggetti informatici con limitate capacità di calcolo, ma connessi a Internet. Tra questi possiamo includere: lavatrici e frigoriferi, automobili, navigatori satellitari, impianti anti intrusione e sorveglianza. Questi impianti e oggetti costituiscono l'Internet of things o IoT e devono essere gestiti con molta attenzione, considerandoli sistemi informatici a tutti gli effetti.

I punti da considerare in questo contesto sono molti. In questo paragrafo si tratta di: documentazione a supporto della conduzione dei sistemi informatici, configurazione dei sistemi informatici, gestione dei cambiamenti, malware, backup, monitoraggio, dimensionamento dei sistemi, dispositivi personali, cancellazione dei dati.

12.9.1 Documentazione

Come già specificato nel paragrafo 12.1, le attività relative alla conduzione dei sistemi informatici devono essere documentate a un livello di approfondimento che tenga conto delle competenze del personale. In molte organizzazioni non si documenta alcunché perché è faticoso, tutti pensano di ricordarsi tutte le cose da fare e l'assenza di una persona non è vista come un problema. Questo succede fino a quando una persona lascia l'organizzazione e nessun altro sa fare il suo lavoro, o i sistemi si bloccano perché non correttamente configurati per dimenticanze.

Esempio 12.9.1. Una semplice attività come la configurazione di un personal computer richiede molti passaggi: aggiornamento del sistema operativo, installazione di tutti i programmi software necessari, configurazione della posta elettronica, installazione e aggiornamento dell'antivirus, eccetera.

È molto facile dimenticare una o più operazioni, con il risultato che poi l'utente deve ricorrere ai tecnici.

Sono da prevedere documenti quali: manuali per gli utenti, manuali di installazione e configurazione per ogni sistema e applicazione, manuali di amministrazione e di gestione degli allarmi (inclusi quelli dei sistemi di backup e antivirus), schemi della rete informatica e degli impianti elettrici, istruzioni per la gestione delle chiamate al service desk.

È bene ricordare che le istruzioni possono essere ridotte a una lista delle operazioni da fare (check list) e i manuali possono essere composti anche da un solo foglio o da una pagina di un sito web, inclusi quelli sviluppati con tecnologie wiki⁸⁶.

Come già richiamato in precedenza, la documentazione va protetta con opportuni controlli di sicurezza, soprattutto di controllo degli accessi (paragrafo 12.6 e sugli scambi di informazioni (paragrafo 12.10.4).

12.9.2 Configurazione dei dispositivi e dei sistemi informatici

La configurazione dei sistemi informatici esige attenzioni particolari per l'elevato numero di opzioni da disabilitare (tra cui utenze e servizi predefiniti) e da attivare (tra cui il logging o la cifratura delle connessioni).

Esempio 12.9.2. Anche per configurare in sicurezza sistemi semplici, come i Raspberry Pi, sono necessarie competenza e attenzione⁸⁷.

Tutti i dispositivi e sistemi (PC, tablet, smartphone, server, software, servizi cloud, eccetera) devono essere configurati in modo sicuro per evitare che una vulnerabilità di uno solo di essi possa essere sfruttata per attaccare l'organizzazione.

La configurazione sicura dei sistemi più critici è denominata hardening. Alcuni enti mettono a disposizione linee guida per la configurazione sicura degli apparati di rete, server e altri tipi di sistemi⁸⁸.

Anche per gli impianti industriali (ICS o Industrial Control Systems o SCADA o Supervisory Control And Data Acquisition), sono disponibili pubblicazioni specializzate [143, 147].

Nel caso dell'IoT, bisogna considerare le diverse componenti del sistema [19]: dispositivi e sensori, applicazioni per dispositivi mobili, gateway e server centrali (detti, in questo contesto, cloud, anche se non sfruttano necessariamente tecnologie cloud).

La configurazione sicura di un dispositivo dovrebbe includere, per quanto applicabile alla sua tipologia e al suo uso previsto:

bloccare l'installazione di software da parte degli utenti;

bloccare le connessioni non sicure, per esempio quelle basate su protocolli non cifrati;

installare, mantenere aggiornato e attivo un software anti-malware;

installare, mantenere aggiornato e attivo un personal firewall;

configurare la connessione con un sistema di backup;

sconnettere automaticamente le sessioni non usate dopo un certo periodo di tempo;

concedere l'accesso al sistema solo con un sistema di autenticazione;

bloccare l'accesso dopo un certo periodo di inattività e concederlo solo con un sistema di autenticazione;

cifrare il disco;

eliminare le utenze standard (root e admin);

cambiare le password di default;

eliminare i servizi e software non necessari;

sincronizzare gli orologi con un server NTP unico per tutta l'organizzazione;

installare strumenti per la cancellazione sicura;

installare un sistema per la cancellazione da remoto dei dati (remotewiping);

bloccare le porte USB e SD.

Per assicurare la completa e omogenea attuazione delle configurazioni stabilite, i sistemi e i dispositivi dovranno essere collegati a sistemi di controllo centrali (per esempio Windows Group policies e, per i dispositivi portatili, MDM).

Per i dispositivi personali (endpoint device), è sempre necessario fornire le regole di configurazione da seguire, anche perché spesso gli utenti o usano dispositivi propri o hanno una certa libertà di azione. Le regole sono oggetto del paragrafo 12.9.8.

12.9.3 Gestione dei cambiamenti

In questo paragrafo si tratta dei cambiamenti in ambito informatico. Gli stessi principi presentati in questo paragrafo vanno adottati per tutti i cambiamenti (di sede, archivi, impianti, eccetera), come già ricordato nel paragrafo 12.3.3.

Il processo qui illustrato è applicabile anche allo sviluppo dei sistemi informatici, oggetto del paragrafo 12.11.

Quanto segue ha l'obiettivo di introdurre un argomento molto complesso che richiede competenze di qualità e gestione dei progetti, da approfondire con altri testi [60, 95, 105, 114, 142].

Ambito e tipo dei cambiamenti

I cambiamenti o change informatici riguardano tutti gli ambiti: infrastrutture (server e client), hardware, software di base, middleware, applicazioni, sistemi di sicurezza, servizi cloud.

Possono essere di diversa complessità:

un cambiamento hardware o infrastrutturale può riguardare la sostituzione di un singolo hard disk o di un intero server, fino ai progetti di modifica dell'intera rete;

un cambiamento di sistema operativo (o di un software di base o di un middleware) può riguardare un piccolo cambio di configurazione, l'installazione di un fix (ossia una correzione), l'aggiornamento della versione o la migrazione su nuove piattaforme;

un cambiamento di un'applicazione può riguardare piccole modifiche grafiche, correzioni di errori, fino a comprendere aggiunte di funzionalità, adattamenti a nuove infrastrutture e l'installazione di interi nuovi servizi complessi;

un cambiamento di un servizio cloud può essere quello di una configurazione estetica fino alla sua completa personalizzazione o alla sua chiusura.

La chiusura di un servizio o la dismissione di un'apparecchiatura sono change perché possono avere impatti sulla sicurezza, sulla funzionalità di altri sistemi e l'operatività degli utenti.

Ulteriori cambiamenti da considerare con attenzione riguardano l'introduzione di nuovi dispositivi. Alcune organizzazioni, prima di permettere l'uso di smartphone e tablet, o di cambiarne il tipo, condussero un'analisi degli impatti e predisposto preventivamente delle regole e dei meccanismi tecnologici di controllo. Questo approccio va considerato anche quando si vogliono trasferire sistemi sul cloud o dal cloud, introdurre soluzioni IoT, autorizzare il BYOD (paragrafo 12.9.8.5), eccetera.

Un cambiamento può essere correttivo, ossia originato dalla necessità di correggere un errore come un guasto hardware o un difetto software (bug), o evolutivo, volto a migliorare le prestazioni o funzionalità di un servizio informatico. Alcuni distinguono altre tipologie di cambiamenti, da cui quelli adattativi e perfettivi.

Un tipo di cambiamento è quello in emergenza e si attua in caso di incidente o rilevazione di vulnerabilità gravi. Questo tipo di cambiamento richiede di essere

effettuato molto più velocemente dei precedenti (paragrafo 12.9.3.9).

Cambiamenti e rischi

Ogni cambiamento, inclusa la sostituzione del toner di una stampante, può rappresentare una minaccia relativa alla sicurezza delle informazioni.

Esempio 12.9.3. Alcune minacce collegate ai cambiamenti:

il cambio di sistema operativo o di web browser possono impedire l'utilizzo di certe applicazioni se queste non sono compatibili con essi e questo è uno dei motivi per cui molte organizzazioni nel 2017 continuavano a usare il sistema operativo Windows XP, nonostante non fosse più in vendita dal 2008 e il supporto terminato nell'aprile 2014;

una sostituzione di una piccola componente hardware può provocare piccole interferenze elettromagnetiche con conseguente danneggiamento dell'intero sistema;

un aggiornamento dell'antivirus può bloccare i sistemi⁸⁹.

Esempio 12.9.4. Il timore di apportare cambiamenti o la scorretta gestione di sistemi, anche critici, può provocare danni elevati.

Nel 2015 un problema a un vecchio PC con Windows 3.1 bloccò l'aeroporto di

Parigi⁹⁰.

Il processo di gestione dei cambiamenti

Ogni cambiamento deve essere tenuto sotto controllo, in modo da non introdurre involontariamente delle vulnerabilità nei sistemi informatici. Va quindi definito e attuato un processo con ruoli e responsabilità ben definite. Questo processo, di cui in figura 12.9.1 è presentato uno schema, deve essere descritto in più procedure dedicate, per esempio, alle diverse tipologie di tecnologie (applicazioni, server, apparati di rete, sistemi di controllo di accesso fisico, eccetera) o ai diversi livelli di complessità dei cambiamenti. In molte organizzazioni queste procedure sono accorpate in un unico documento.



Figura 12.9.1:

Processo di gestione dei cambiamenti o di change management

La rappresentazione del processo potrebbe ricordare il cosiddetto metodo waterfall per la progettazione e sviluppo dei sistemi informatici. In realtà è facilmente applicabile anche quando si seguono altri metodi, come quelli di tipo agile [137].

Nei paragrafi seguenti, dopo aver introdotto alcuni termini e alcuni concetti sul ticketing e sugli ambienti informatici, si approfondiscono le fasi del processo.

Terminologia di base

È opportuno specificare preliminarmente cosa si intende con i termini applicazione e infrastruttura informatica, sebbene non vi siano definizioni condivise.

Applicazione: programma software direttamente utilizzato dall'utente finale, attraverso opportune interfacce.

Infrastruttura informatica: insieme di hardware e sistemi operativi, inclusi quelli di rete, che costituiscono la base di ogni sistema informatico e sono necessari per il funzionamento e l'utilizzo delle applicazioni.

Fa parte dell'infrastruttura il middleware, ossia l'insieme di programmi di supporto alle applicazioni e non utilizzati direttamente dagli utenti (per esempio i web server e i database management system). Sistemi operativi e middleware sono sovente indicati con il termine di software di base o software di sistema.

Il termine sistema informatico è utilizzato per indicare genericamente un'applicazione e l'infrastruttura a suo supporto, oppure una sua componente (come il sistema operativo).

Gli elementi sopra elencati possono essere presso l'organizzazione o un suo cliente, fornitore, partner e possono essere oggetti fisici o di un servizio cloud. Il cloud infatti mette a disposizione le risorse prima elencate, ma solo virtualmente.

Altri termini utilizzati nel seguito sono:

input: dati che un programma riceve da un utente o da un altro programma informatico;

output: dati forniti da un programma a un utente o a un altro programma;

server: programmi che forniscono servizi o computer su cui sono installati dei programmi server;

client: programmi che richiedono servizi a programmi server, come il client di posta elettronica e il web browser; questo termine è utilizzato anche per indicare i PC;

modulo software: componente di un programma software deputato a offrire specifiche funzionalità; per esempio, i sistemi ERP possono essere costituiti dai moduli “contabilità”, “magazzino”, “vendite”, eccetera.

Un programma è inizialmente scritto come codice sorgente, comprensibile al programmatore, che poi viene compilato e costruito (built) in modo da renderlo comprensibile al computer (la compilazione non è sempre necessaria, ma i concetti che seguono sono comunque applicabili). Il codice compilato è composto da molti file, detti oggetti, tra loro integrati.

Una suddivisione molto diffusa, soprattutto nelle applicazioni web, prevede tre moduli (three tiers): quello di presentazione per la visualizzazione delle pagine per gli utenti e quelli di elaborazione e di base dati (database) non accessibili direttamente dagli utenti finali. Questa suddivisione permette una più efficace ed efficiente manutenzione delle parti del programma e permette di separare la parte meno critica (quella di presentazione, a cui hanno accesso gli utenti) da quelle più critiche e di filtrare ogni comunicazione con il database.

Ticketing

Per registrare i cambiamenti si usa spesso un sistema informatico detto di ticketing, che permette di tracciare gli stati delle operazioni e i loro responsabili. Questo sistema è utile per ricostruire quanto fatto in caso di problemi e per obbligare il personale a non saltare alcun passaggio.

In molte organizzazioni il sistema di ticketing è utilizzato anche per registrare gli incidenti; in altre, il termine ticketing si riferisce solo all'assistenza agli utenti e alla gestione degli incidenti, mentre per i cambiamenti si utilizzano termini diversi.

Ambienti

Per ciascun sistema informatico possono essere presenti tre ambienti:

sviluppo, in cui lavorano le persone addette allo sviluppo software e in cui si trova il codice sorgente; se non viene sviluppato software, questo ambiente non è necessario;

test, che a sua volta può essere suddiviso negli ambienti per i test tecnici e per i test degli utenti; questi ambienti prendono diversi nomi, come integrazione, collaudo, staging o user acceptance test (UAT);

produzione o esercizio, dove sono installate le applicazioni utilizzate dagli utenti finali e i programmi loro necessari.

La sicurezza degli ambienti è approfondita al paragrafo 12.9.3.10.

Per gestire in modo sicuro e controllato l'archiviazione e la modifica del codice sorgente, sono disponibili programmi di configuration management. Essi hanno l'obiettivo di rendere più efficiente la programmazione, impedire l'esecuzione di cambiamenti tra loro conflittuali, configurare le autorizzazioni per l'accesso al codice, tenere traccia di tutte le modifiche effettuate ai sorgenti e dei loro autori, controllare (per finalità di rollback e analisi) le diverse versioni dei file e dei programmi e interfacciarsi con gli strumenti di compilazione (compilatori e builder).

12.9.3.1 Richiesta e requisiti

Ogni cambiamento deve essere richiesto da una persona autorizzata ed essere descritto per iscritto nella cosiddetta Request for change o RFC. La richiesta può essere molto breve (per esempio, “sostituire un hard disk guasto”) o molto lunga (per esempio se si richiede di introdurre un nuovo sistema informatico o

modificare ampiamente uno esistente).

Uno dei principi di sicurezza delle informazioni recita: “i requisiti di sicurezza vanno stabiliti prima di approvare e attuare ogni cambiamento e devono essere adeguati al livello di rischio calcolato per le informazioni trattate dal sistema”. In caso contrario, la sicurezza verrebbe attuata peggio, con errori e inefficienze, e a costi superiori⁹¹. Questo principio va attuato per:

lo sviluppo di applicazioni, per cui i requisiti di sicurezza vanno stabiliti sin dalle prime analisi funzionali e tecniche;

la modifica di applicazioni, per cui devono essere sempre valutati gli impatti della modifica sui meccanismi di sicurezza già esistenti e i requisiti da prevedere per i nuovi moduli o oggetti (per esempio, quando si aggiungono moduli a un’applicazione, l’accesso deve essere controllato in modo simile agli altri moduli);

l’acquisizione di prodotti hardware e software e di servizi cloud, i cui requisiti di sicurezza devono essere stabiliti prima di avviare la ricerca del prodotto o servizio;

la modifica di configurazioni hardware, software, infrastrutturali o dei servizi cloud (inclusi i ritiri di componenti), per cui è necessario stabilire su quali meccanismi di sicurezza preesistenti potrebbe avere impatto.

L’analisi degli impatti sui sistemi preesistenti deve valutare se i seguenti meccanismi di sicurezza rimangono validi anche dopo il cambiamento:

sistemi di monitoraggio;

logging;

controllo degli accessi al sistema e ai dati;
controllo della rete (firewall, IDS, eccetera);
backup e sincronizzazione con i siti di disaster recovery;
prestazioni hardware;
interfacciamenti e comunicazioni con altri sistemi.

Il metodo migliore per non dimenticare requisiti è creare una check list. In appendice E sono elencati diversi requisiti, sia di prodotto che di servizio.

I requisiti dovrebbero essere stabiliti da rappresentanti degli utilizzatori e degli addetti allo sviluppo, configurazione e amministrazione del sistema, oltre che dal responsabile della sicurezza, se previsto. La scelta dei requisiti da parte dei soli utenti o dei soli tecnici informatici si rivela sempre inadeguata e richiede poi correzioni.

Particolari richieste derivano dalle segnalazioni dei produttori di software quando pubblicano correzioni (dette patch o fix) o nuove versioni dei programmi già in uso. Queste richieste sono da valutare attentamente perché non sempre le correzioni o gli aggiornamenti sono applicabili ai sistemi utilizzati (paragrafo 12.13.3).

Esempio 12.9.5. Nel 2014, Microsoft pubblicò l'aggiornamento di sicurezza 2982791, descritto da MS14-045, che provocò instabilità in alcuni sistemi, fino a bloccarli.

12.9.3.2 Autorizzazione ai cambiamenti

È necessario stabilire a chi devono essere inoltrate le richieste di cambiamento affinché siano valutate in merito al loro potenziale impatto sugli utilizzatori finali, sui sistemi già esistenti e sui controlli di sicurezza. Se il cambiamento ha impatti accettabili, può essere autorizzato.

L'autorizzazione può essere data da una singola persona (detta change manager) o da un gruppo di persone (detto change advisory board). Il coinvolgimento di più persone è necessario quando il cambiamento riguarda più ambienti informatici utilizzati, amministrati e conosciuti da persone diverse.

12.9.3.3 Pianificazione dei cambiamenti

Devono essere pianificate le attività per attuare il cambiamento, le scadenze e le responsabilità.

Anche per attività di breve o brevissima durata vanno garantiti i tempi e le risorse sufficienti per: determinare i requisiti di sicurezza, sviluppare correttamente quanto necessario e condurre test di sicurezza significativi.

Troppe volte, per risparmiare tempo, si riduce proprio quello relativo ai test funzionali e di sicurezza. Questo ha poi come conseguenza che i difetti vengono rilevati dopo la chiusura del cambiamento e quindi si deve aprire una nuova richiesta di cambiamento, a costi superiori rispetto a quelli che si sarebbero sostenuti inizialmente.

12.9.3.4 Sviluppo e ingegnerizzazione (sicuri)

Gli operatori informatici, inclusi gli sviluppatori e i programmatori, devono conoscere le tecniche di ingegnerizzazione e sviluppo sicuri per evitare di introdurre vulnerabilità.

Lo sviluppo e ingegnerizzazione sicuri si basano su principi noti quali:

security by design: la sicurezza deve essere considerata fin dalle prime fasi della progettazione;

defence in depth: i controlli di sicurezza non devono ridursi a uno solo;

default deny: permettere solo le cose esplicitamente autorizzate;

fail securely: eventuali malfunzionamenti non devono introdurre vulnerabilità;

least privilege: ogni utente e funzionalità deve avere le autorizzazioni minime per poter svolgere il proprio compito; il principio del “non si sa mai” non deve essere applicato.

Questi principi vanno poi attuati in fase di progettazione e sviluppo. Sono attivi diversi progetti di raccolta e pubblicazione di tecniche più dettagliate [62, 64, 111, 115, 120, 124, 142, 152, 161] e includono tecniche di sviluppo sicuro, alcune approfondite nel seguito, quali:

meccanismi di autenticazione;

validazione degli input;

virtualizzazione (che può permettere un più veloce ripristino ed evitare il

propagarsi degli errori);

codifica sicura.

Purtroppo, molti sembrano completamente disinteressati agli studi in materia di ingegnerizzazione e sviluppo sicuri, anche perché la loro adozione richiede di aumentare il tempo di alcune fasi di lavoro. Il risultato, immancabile, è che poi sono individuate vulnerabilità e il tempo risparmiato viene perso con gli interessi nelle successive attività di correzione e manutenzione.

I principi di ingegnerizzazione e le tecniche di sviluppo da adottare vanno descritti in procedure dedicate e distribuite al personale interno e ai fornitori coinvolti nelle attività. Gli addetti devono essere adeguatamente competenti per realizzare quanto richiesto senza commettere errori.

Vanno quindi documentati:

i processi da seguire per la progettazione e lo sviluppo;

i processi da seguire per installare le modifiche in ambiente di produzione (paragrafo 12.9.3.8).

Seguono alcuni dettagli sui principi di ingegnerizzazione e sulle tecniche di sviluppo sicuri.

Esempio 12.9.6. Un sistema si interfaccia con altri sistemi.

Il programma di gestione delle vendite si interfaccia con quello del magazzino e con quello della contabilità; il programma di gestione del personale si interfaccia anch’esso con quello di contabilità.

Interfacciamenti particolari coinvolgono sistemi di supporto o di sicurezza, come quello di gestione delle utenze e autorizzazioni (per esempio LDAP) o quelli di monitoraggio.

Il primo punto è fare attenzione a come i vari sistemi, moduli e oggetti si interfacciano tra loro, in particolare se installati su server o segmenti di rete diversi: le connessioni devono essere cifrate per garantirne la riservatezza, i sistemi devono riconoscersi tra loro attraverso lo scambio di certificati digitali e la correttezza delle trasmissioni va verificata attraverso meccanismi crittografici (o evoluzioni del “carattere di controllo” o check digit).

Il secondo punto prevede di controllare ogni richiesta di accesso ai dati o agli oggetti per verificare se è stata originata da un utente autorizzato. Nelle applicazioni web, una delle vulnerabilità più diffuse è proprio l’assenza di meccanismi di gestione delle autorizzazioni tra gli oggetti [117].

Interfacce particolari sono quelle degli utenti. Normalmente sono previsti campi in cui essi possono inserire dei caratteri (per esempio, per comprare un biglietto aereo). Questi campi possono essere utilizzati da un malintenzionato con tecniche di attacco di buffer overflow, SQL Injection o cross site scripting. È quindi necessario validare gli input, ossia controllare tutti i dati inseriti dagli utenti e prevenire errori (esempio banale: rilevare se sono state inserite lettere in un campo dove è richiesto un numero di telefono o sequenze di caratteri che permettono di compromettere il sistema) e attacchi. Questi controlli devono essere effettuati da un modulo installato su un server e non sul PC dell’utente, in modo che questi non possa modificarlo e gli impedisca di procedere agli appropriati controlli.

Il controllo dei dati di input va effettuato anche quando i dati sono ricevuti da altri programmi, come nel caso di batch inviati periodicamente da un sistema affinché siano elaborati da un altro sistema.

Altro punto riguarda i dati di output, visualizzabili tipicamente a video o su foglio stampato: occorre verificare che ogni visualizzazione non fornisca più dati del necessario. Esempi di questi casi sono: password visualizzabili nell'URL, funzioni di ricerca che consentono l'accesso a dati altrimenti riservati, messaggi di errore con dettagli sulla configurazione del sistema utilizzabili per un attacco.

Riutilizzo di codice

È pratica comune, e in molti contesti consigliata, riutilizzare il codice o i programmi già fatti da altri. Esistono librerie da cui prelevarli gratuitamente o a pagamento.

Molto comune, per esempio, è il riutilizzo di codice per introdurre meccanismi crittografici nei programmi⁹².

Prima di adottare il codice sviluppato da altri è da seguire il medesimo processo di acquisizione dei sistemi informatici, oggetto del paragrafo 12.11.

Esempio 12.9.7. Nel 2014, fu individuata Heartbleed, una vulnerabilità del diffusissimo software open source OpenSSL. Quasi tutti i server del mondo ebbero quindi la necessità di essere aggiornati.

Il codice di OpenSSL, fino a quel momento, aveva ricevuto donazioni per circa 2.000 dollari all'anno ed era seguito da un unico addetto a tempo pieno⁹³, nonostante fosse utilizzato da migliaia di aziende anche commerciali.

Appare quindi evidente come l'uso di software open source non metta al riparo da vulnerabilità e attacchi e siano sempre da monitorare gli aggiornamenti.

.

Modifica dei pacchetti software

I pacchetti software sono mantenuti dai propri produttori, che mettono a disposizione aggiornamenti anche per correggere eventuali vulnerabilità identificate. È opportuno limitare le modifiche da apportare a tali pacchetti affinché gli aggiornamenti siano sempre applicabili.

12.9.3.5 Codifica sicura

La scrittura del codice deve seguire regole di sicurezza per evitare di usare comandi e costruzioni sconsigliate in quanto potrebbero introdurre vulnerabilità. La codifica sicura può essere vista come parte dell'ingegnerizzazione e sviluppo sicuri.

Una delle prime misure da adottare, anche se non strettamente di sicurezza,

consiste nel documentare le convenzioni per ciascun linguaggio di programmazione adottato, tra cui come denominare i metodi, le variabili, gli oggetti e i moduli⁹⁴.

Un’ulteriore misura di sicurezza, anche se apparentemente banale, consiste nel commentare il codice, in modo da permetterne una più semplice manutenzione e nel cancellare i commenti quando il codice è trasferito in ambiente di produzione per evitare di fornire informazioni utili a malintenzionati.

Altre regole dipendono dal linguaggio di programmazione usato e pertanto è compito degli sviluppatori consultare le guide messe a disposizione. Alcune guide, dedicate soprattutto allo sviluppo web, sono messe a disposizione da OWASP [116, 133]. Oggi sono disponibili strumenti (per esempio SAST e DAST) che verificano automaticamente la qualità e sicurezza del codice sorgente.

12.9.3.6 Riesami

Quando si attuano cambiamenti complessi, è necessario riesaminare periodicamente dell’avanzamento dei lavori coinvolgendo i gruppi di lavoro pertinenti (per esempio, i sistemisti e i programmatore) e le parti interessate (per esempio, i rappresentanti degli utenti) per stabilire se quanto fatto è adeguato e affrontare per tempo questioni che potrebbero diventare critiche. Il riesame potrebbe evidenziare necessità di ripianificazione.

12.9.3.7 Verifiche e test

Uno dei principi della sicurezza è: ciascun cambiamento va verificato con test prima della sua introduzione nell’ambiente di produzione.

Purtroppo è prassi non condurre i test in modo controllato e ben strutturato: sia perché è un’attività che richiede tempo e quindi costa, sia perché il personale tecnico si ritiene in grado di evitare errori. Numerosi esempi dimostrano quanto si sbagliano.

Nel caso del software, i test vanno effettuati in diversi momenti dello sviluppo: inizialmente sui singoli oggetti sviluppati (unit test), poi sul programma nel suo complesso (test di integrazione), poi in un ambiente simile a quello di produzione (test di collaudo), poi con l’aiuto degli utenti (test di accettazione o UAT, User acceptance test). I test devono riguardare anche i software non sviluppati direttamente dall’organizzazione e i pacchetti software.

Relativamente alla sicurezza, i test possono essere di diverso tipo:

test funzionali, in cui sono verificate le funzioni di sicurezza (per esempio si prova a inserire una password sbagliata per vedere come reagisce il software);

test non funzionali, in cui è verificato il codice e l’architettura; per questo si possono usare strumenti di controllo del codice (SAST per l’analisi statica e DAST per l’analisi dinamica, ossia durante il suo funzionamento o una sua simulazione), da integrare nelle interfacce di sviluppo, che verificano il codice ogni volta che viene compilato o fatta una build;

test di vulnerability assessment e penetration test, in cui si simulano le attività di

un attaccante (paragrafo 12.15.4); questi test sono fatti nell'ambito del collaudo o dell'accettazione;

test di non regressione (in inglese regression test, senza l'avverbio di negazione), in cui sono verificate funzionalità non oggetto del cambiamento, ma che, a causa delle interrelazioni tra i componenti del sistema, potrebbero presentare errori dovuti al cambiamento; caso particolare riguarda i cambiamenti di componenti dell'infrastruttura (per esempio il sistema operativo o il database), che potrebbero richiedere verifiche anche ai software che la utilizzano.

I test devono essere pianificati (ossia devono essere identificati i test da fare e i risultati attesi) e documentati in un rapporto di test (insieme a chi li ha eseguiti, la data e il risultato), perché solo così il personale addetto non dimentica alcuna verifica ed è possibile risalire all'origine degli errori che si dovessero presentare.

Devono essere registrati anche i test con esito negativo. Questi devono essere accompagnati da un piano di rientro (ossia come e quando si prevede di correggere l'errore) e, una volta corretti, l'esito positivo. Alcuni esiti negativi possono non pregiudicare il passaggio in produzione del cambiamento; in questi casi deve essere registrata la decisione insieme alla persona che l'ha presa e la sua giustificazione.

I test non devono mai essere condotti negli ambienti di produzione o accedendo ai dati utilizzati dai sistemi di produzione. Questo per evitare di corromperli e creare disservizi agli utenti. Devono però essere condotti in ambienti il più possibile uguali a quelli di produzione per identificare gli errori prima del passaggio in ambiente di produzione.

12.9.3.8 Installazione in ambiente di produzione

Dopo aver effettuato i test, se positivi, il cambiamento può essere installato in ambiente di produzione. Sovente si usa il termine rilascio per una cattiva traduzione dell’inglese release.

È opportuno predisporre procedure di rollback, in modo che si possa tornare alla situazione precedente in caso di necessità, ed effettuare un backup dei dati potenzialmente coinvolti dal cambiamento. Anche le procedure di rollback andrebbero verificate con test prima di procedere.

Nel caso di cambiamenti alla configurazione di un sistema, che in genere richiede pochissime operazioni, è necessario accertarsi che sia possibile ripristinare la situazione precedente.

Ulteriore accortezza prevede di archiviare le precedenti versioni dei software in modo da poter accedere a vecchi file in caso di necessità.

Da un punto di vista organizzativo va stabilito chi può autorizzare l’installazione, anche considerando i risultati dei test. Con largo anticipo rispetto alla data di installazione, occorre: avvisare gli utenti per segnalare potenziali interruzioni o rallentamenti dei servizi, aggiornare i manuali e istruire gli operatori del service desk affinché possano rispondere a eventuali richieste di assistenza a seguito del cambiamento.

Dopo aver effettuato le operazioni di installazione in ambiente di produzione, prima di chiudere il cambiamento vanno fatte le ultime verifiche: correttezza della connessione ai sistemi di monitoraggio, correttezza e completezza dei log, adeguatezza dei controlli degli accessi e della rete, aggiornamento dei sistemi di backup e di disaster recovery e del piano di continuità, prestazioni, correttezza dell’interfacciamento con gli altri sistemi.

Infine va aggiornato il CMDB con i nuovi asset o le nuove versioni degli asset presenti nell’ambiente di produzione (paragrafo 12.5.2).

Dopo lo sviluppo e l’installazione iniziali, i software e i sistemi vanno mantenuti, seguendo le stesse pratiche qui descritte. Al termine del ciclo di vita del sistema o di un suo componente, anche cloud, si deve procedere alla sua dismissione, seguendo lo stesso processo di gestione dei cambiamenti, con particolare attenzione alla cancellazione dei dati (vedere il paragrafo 12.9.9).

12.9.3.9 Cambiamenti in emergenza

I cambiamenti in emergenza seguono lo stesso processo degli altri cambiamenti, anche se in maniera più veloce.

Solitamente i test dei cambiamenti in emergenza sono poco approfonditi perché si ritiene troppo rischioso rallentarne l’installazione, malgrado ogni cambiamento possa introdurre vulnerabilità.

Per questo, una volta installato il cambiamento in emergenza, si deve ripartire dalla pianificazione, in modo che i requisiti siano confermati e i test completati.

Questi cambiamenti vanno monitorati con attenzione, visto che, per evitare di effettuare tutti i test necessari, alcuni dichiarano come “emergenza” tutti i cambiamenti.

12.9.3.10 Sicurezza degli ambienti

Gli ambienti di sviluppo, test e produzione sono da tenere tra loro ben separati, in modo che eventuali anomalie negli ambienti di sviluppo e test non si propaghino agli ambienti di produzione.

Non sempre è possibile disporre di ambienti di sviluppo e test separati dall’ambiente di produzione. Ci possono essere problemi tecnici (per esempio, alcuni interfacciamenti con altri sistemi non possono essere attivati negli ambienti di test) o economici (quando l’hardware o le licenze software sono molto costosi). In questi casi vanno prese tutte le opportune cautele affinché un cambiamento possa essere attentamente verificato appena installato in ambiente di produzione e si possa ritornare alla situazione precedente attraverso procedure di rollback.

L’accesso ai diversi ambienti va sempre controllato. In particolare, l’accesso al codice sorgente delle applicazioni va regolamentato per evitare che sia alterato da malintenzionati o per errore, oppure copiato da persone non autorizzate.

Anche le autorizzazioni per l’accesso ai programmi di configuration management e ai loro archivi e agli ambienti di test e produzione devono essere assegnate tramite il processo di gestione delle credenziali e delle autorizzazioni (paragrafo 12.6).

Esempio 12.9.8. Il famoso attacco a SolarWinds di fine 2020 si basò sul malware Sunburst, installato nell’ambiente di build del prodotto⁹⁵dopo l’intrusione degli attaccanti.

Esempio 12.9.9. Nel 2017 furono attaccati con successo gli ambienti di sviluppo di Uber⁹⁶, in cui erano presenti numerosi dati dei clienti.

Per proteggere ulteriormente gli ambienti, è sempre opportuno non concedere mai l'accesso diretto, ma sempre mediato dagli strumenti di sviluppo, configuration management, build, eccetera e tracciare le azioni degli sviluppatori, fino alle modifiche delle singole righe di codice.

Tutti gli ambienti e gli strumenti di sviluppo (inclusi builder, integratori, compilatori, sistemi di controllo della configurazione e librerie interne ed esterne) devono essere aggiornati con le ultime versioni disponibili di patch e configurati in modo sicuro. È quindi opportuno che in tutti gli ambienti siano installati solo i programmi strettamente necessari al loro funzionamento (paragrafo 12.6.3.5).

Infine, il codice sorgente dovrebbe essere oggetto di backup.

12.9.3.11 Dati di test

Come regola generale, i test non mai effettuati direttamente sui dati di produzione o su loro copie.

Quando è necessario effettuare test con i dati di produzione, ne va usata una copia e mai vanno condotti test negli ambienti di produzione.

Quando i dati copiati hanno caratteristiche di riservatezza, specialmente perché personali, vanno utilizzati meccanismi di anonimizzazione delle copie dei dati prima di utilizzarli (vedere paragrafo 12.5.1.7). Come alternativa si possono applicare misure rigorose di controllo accesso in modo da limitare al minimo le persone che possono accedervi. In tutti i casi, i dati riservati vanno cancellati al termine delle operazioni.

12.9.4 Malware

Il metodo più noto per proteggersi dal malware consiste nell'installare e mantenere attivo e aggiornato un antivirus.

Gli antivirus agiscono soprattutto riconoscendo virus già noti (comparandoli con le cosiddette signature, file che richiedono aggiornamenti frequenti) ed effettuando analisi sul comportamento del sistema (analisi euristica). Alcuni attacchi sono detti zero-day perché sfruttano vulnerabilità appena scoperte e non sono censiti nelle signature; per questo è opportuno far eseguire periodicamente all'antivirus analisi complete dei sistemi, in modo che rilevi malware eventualmente non individuati in precedenza con vecchie versioni delle signature.

Quando si installa un antivirus, le sue opzioni sono usualmente già impostate per garantire un adeguato livello di protezione: controllo delle email e delle periferiche, aggiornamento automatico delle signature e verifica periodica di tutto il sistema. È quindi inopportuno modificarle. Alcuni antivirus gratuiti

propongono l'installazione di altri programmi e la modifica della home page del browser; in quei casi, il rifiuto di queste opzioni non crea problemi di sicurezza.

In ambito lavorativo, gli antivirus devono essere installati sui personal computer, sui dispositivi portatili e su alcuni server (per esempio, quello di posta elettronica) ed essere controllati da un sistema centrale, che verifichi se qualcuno ha l'antivirus non aggiornato o disinstallato e impedisca la connessione alla rete a PC non opportunamente configurati.

Tutto ciò non è sufficiente: visto che il malware sfrutta vulnerabilità dei programmi software, è necessario che anche questi siano aggiornati regolarmente secondo le indicazioni dei loro produttori. L'attività di patching spesso è colpevolmente non effettuata o effettuata con ritardo, con conseguenze anche disastrose; se ne discute nel paragrafo 12.13.3.

Ulteriori accorgimenti, non sempre applicabili, prevedono di:

impedire agli utenti di installare software sui personal computer per evitare che installino inavvertitamente del malware;

non permettere agli utenti di modificare le configurazioni dei programmi software installati sui personal computer per evitare che modifichino anche quelle dei meccanismi di sicurezza, incluso l'antivirus;

impedire la connessione di qualsiasi dispositivo e supporto di memorizzazione alle porte USB e SD per evitare che eventuale malware presente sulle periferiche si propaghi sul PC dell'utente e poi sui sistemi collegati alla medesima rete, oltre a evitare altri attacchi come l'ipodslurping;

bloccare la ricezione di file da esterni via email, social network, strumenti di file sharing, eccetera, perché potrebbero contenere del malware;

disattivare le macro dei documenti;
disabilitare l'esecuzione di autorun e script.

Neanche l'organizzazione più rigorosa può bloccare tutti i computer (gli stessi amministratori dei sistemi informatici devono poter installare e aggiornare i programmi), né avere installate tutte le patch disponibili. Inoltre alcuni malware sono progettati per non essere intercettati dagli antivirus (per esempio, i malware polimorfici). Per questo occorre informare gli utenti dei rischi di infezione da malware e invitarli a prestare attenzione quando si naviga su Internet o si ricevono file via email o altro supporto. In particolare il personale deve essere invitato a installare solo il software esplicitamente autorizzato dalle regole dell'organizzazione.

Da prevedere procedure destinate al personale su come comportarsi in caso di rilevazione di malware sul proprio computer: non prendere alcuna iniziativa, neanche spegnere il computer, ma solo avvisare il service desk e seguire la procedura di gestione degli incidenti (paragrafo 12.13).

Per difendersi dallo spamming, forma particolare di malware, si possono attivare dei filtri antispam sui server e sui singoli client di posta elettronica. I filtri sono da configurare con molta prudenza per evitare i falsi positivi, ossia il blocco di email legittime.

Per difendersi dai più recenti attacchi di ransomware, oltre alle misure sopra elencate, si raccomanda⁹⁷ di effettuare backup offline per poter recuperare i dati senza che il malware li corrompa.

12.9.5 Backup

Il backup è una copia di file da utilizzare se la versione originale è alterata o persa. Si possono fare backup di dati, di software e di interi sistemi informatici.

I backup possono essere fatti su diverse tipologie di supporti: nastro magnetico (ormai in disuso), nastro digitale, dischi esterni, altri computer o in ambienti cloud. In tutti i casi, vanno tenute presenti le seguenti accortezze:

accesso limitato alla copia dei dati: questo si può ottenere configurando opportunamente il sistema di backup o con meccanismi crittografici o attraverso controlli di sicurezza fisica per la protezione del supporto; se il supporto di backup è un altro computer, le persone autorizzate ad accedervi devono essere in un sottoinsieme di quello delle persone autorizzate ad accedere ai dati originali;

conservare i supporti di backup in luoghi diversi da quelli dove sono i dati originali per poterli recuperare in caso di incendi o allagamenti.

Va stabilita la periodicità e la tipologia dei backup considerando la frequenza di aggiornamento dei dati: non troppo frequenti, perché deteriorerebbero i supporti e rallenterebbero i sistemi; non troppo rari, perché, in caso di incidente tra un backup e il successivo, i dati persi potrebbero essere troppi e quindi difficili da ricostruire.

Ci sono diversi tipi di backup:

completi: prevedono la copia di tutti i dati (se i dati sono molti, la creazione del backup richiede molta potenza computazionale per lungo tempo);

incrementali: prevedono la copia dei soli dati modificati dall'ultimo backup

completo o incrementale (per recuperare i dati è quindi necessario ripristinare l'ultimo backup completo e poi tutti i successivi incrementali);

differenziali: prevedono la copia dei soli dati modificati dall'ultimo backup completo (risultano quindi più lenti da effettuare rispetto a quelli incremental, ma consentono di recuperare più velocemente i file persi);

sincronizzati: viene effettuata una copia di ogni file appena è modificato (in questo caso, si corre il rischio che un errore in un file si propaghi anche sulla copia di sincronizzazione; per questo motivo la sincronizzazione è spesso affiancata da ulteriori backup meno frequenti).

Molti effettuano un backup completo nel fine settimana per evitare di rallentare i sistemi durante l'orario di lavoro, e uno incrementale o differenziale durante ogni notte della settimana. In questo modo, nel peggior caso possibile, a seguito di un incidente sono da ricostruire unicamente i dati del giorno precedente.

È importante prestare attenzione ai servizi cloud, visto che il fornitore potrebbe non assicurare il servizio di backup. Il cliente deve quindi verificare se il servizio di backup è incluso e, in caso contrario, decidere se provvedere autonomamente, oppure estendere il contratto per includerlo, oppure coinvolgere un altro fornitore (in questo caso, se i sistemi del fornitore cloud sono compromessi, i backup potrebbero non esserlo perché presso un altro fornitore).

È da stabilire il tempo di conservazione (retention time). Solitamente si conservano le ultime due copie di backup completi, così da ridurre i rischi consequenti al danneggiamento di una di esse. In questo modo, normalmente, si hanno le copie dei file delle ultime due settimane. Può essere necessario conservare alcuni backup per un periodo più breve o più lungo se richiesto da normative o da altre esigenze. Esempi: la normativa in materia di privacy richiede che le videoregistrazioni non siano conservate per più di 24 ore (sono possibili eccezioni); le registrazioni contabili e finanziarie vanno conservate per 10 anni; documenti e registrazioni possono essere conservati per esercitare il diritto di difesa.

Quando le memorie usate per il backup (inclusi nastri e hard disk) cambiano utilizzo o risultano obsolete, vanno cancellate in modo sicuro (vedere 12.8.2.7).

Deve essere infine redatto un elenco dei backup previsti per ogni sistema o gruppo di sistemi: tipo di backup, frequenza, tempo di conservazione e modalità di verifica.

Cambiamenti e backup

È già stata ricordata nel paragrafo 12.9.3.8 la necessità di verificare l'adeguatezza dei backup dopo i cambiamenti ai sistemi informatici poiché possono modificare la struttura dei dati oggetto di backup.

Esempio 12.9.10. In un'azienda, dopo aver costituito un nuovo ufficio e avergli assegnato un'area del file server dove archiviare i propri documenti, non era stato aggiornato il sistema di backup.

Dopo un anno, il server si è danneggiato e i file del nuovo ufficio non furono recuperati perché mai stati oggetto di backup.

Verifica dei backup

Deve essere verificata la correttezza dei backup e periodicamente effettuate

prove di ripristino dei sistemi partendo dai soli backup, simulando un incidente grave ai sistemi informatici.

Molti tecnici asseriscono che si tratta di un'operazione inutile perché, se i backup sono ben configurati, i ripristini sono facili da fare. Questi tecnici non hanno mai ripristinato alcun sistema informatico nella loro vita; altrimenti saprebbero che non esistono dei ripristini semplici, anche se oggi il backup di intere macchine virtuali ha semplificato queste operazioni.

12.9.6 Logging e monitoraggio

I sistemi sono da monitorare per rilevare attività anomale, dovute a malintenzionati o altri eventi.

Le attività degli utenti vanno registrate anche al fine di poter individuare i responsabili di certe azioni. Questo non necessariamente per cercare colpevoli, né per diffidenza nei confronti del personale, ma per poter ricostruire esattamente gli eventi anomali, stabilire se si tratta di incidenti e trattarli in maniera adeguata.

12.9.6.1 Logging

Occorre stabilire quali attività registrare nei cosiddetti log (il nome deriva dai diari di bordo delle navi). I log sono generati automaticamente dai sistemi e utilizzati dai sistemi di monitoraggio o per ricostruire eventi significativi (in questo caso, prendono anche il nome di audit trail).

I log cosiddetti applicativi registrano le attività degli utenti di una determinata applicazione. Per esempio, le applicazioni delle banche tracciano quanto fatto da ciascun operatore di cassa.

Altri log possono essere quelli dei sistemi operativi che tracciano le connessioni e disconnessioni degli utenti, l'attivazione e la disattivazione dei servizi, eccetera.

A rigore, le registrazioni manuali, come quelle effettuate sul sistema di ticketing, sono dei log.

I log devono riportare l'identificativo dell'utente che ha effettuato l'attività, la data e l'ora.

Tutti gli operatori devono poter leggere i log riguardanti i sistemi da loro amministrati affinché siano in grado di ricostruire eventi significativi e utili al miglioramento dei sistemi informatici.

È da stabilire cosa registrare per evitare di disporre di troppi dati impossibili da analizzare e di riempire gli hard disk con informazioni non utili. Alcuni eventi possono essere: accesso e uscita degli utenti da sistemi, applicazioni e file; tentativi non riusciti di accesso ai sistemi e alle applicazioni e ai file; modifiche alle configurazioni, ai file e ai record (aggiunte, cambiamenti, eliminazioni); attività degli amministratori di sistema; modifiche ai diritti di accesso; allarmi inviati.

Sempre per evitare che gli hard disk siano saturati dai log, è opportuno stabilire qual è il tempo minimo e massimo di conservazione (tempo di retention) oltre

che, ovviamente, monitorare l'occupazione delle aree di memorizzazione. Questa misura è necessaria anche perché i log contengono solitamente dati personali e pertanto non possono essere conservati per un tempo indefinito.

12.9.6.2 Protezione dei log

I log vanno adeguatamente raccolti e conservati in modo da assicurarne la riservatezza, anche perché sono dati personali, e l'integrità. Nessun operatore o attaccante deve avere la possibilità di modificare i log, nel caso in cui intenda coprire le tracce di propri abusi o errori. In alcuni casi devono essere conservati in modo da essere esibiti come mezzi di prova in caso di procedimenti legali (paragrafo 12.13.6) [1].

Molti usano le funzioni crittografiche di hashing o di firma per ogni log o file di log, così che, se il log è modificato, questo viene rilevato perché non più coerente con l'hash o la firma. Un risultato simile può essere ottenuto con le marche temporali. In questi casi, se il log è cambiato, non è comunque possibile rilevare cosa è cambiato e le cancellazioni dei log non possono essere rilevate tempestivamente a meno di non impostare specifici allarmi.

Per prevenire i cambiamenti ai log, si possono cifrare. Ovviamente, chi conosce le chiavi crittografiche non deve svolgere attività che devono essere tracciate su quei log.

Per prevenirne la cancellazione, i log dovrebbero essere trasferiti a un altro server (o su un supporto che permette un'unica scrittura), dove gli amministratori non hanno alcun tipo di accesso. In questo caso, gli amministratori di sistema e gli attaccanti che hanno ottenuto privilegi elevati non possono coprire le tracce di errori, ma, se l'attacco è pianificato in anticipo, possono alterare il trasferimento dei log prima di iniziare un'azione malevola.

Per un ulteriore livello di sicurezza, i log trasferiti possono essere marcati temporalmente, oggetto di hash (per verificarne l'integrità) e cifrati (per prevenire cambiamenti e limitare gli accessi).

12.9.6.3 Monitoraggio

Ancora oggi molte guide di sicurezza raccomandano di analizzare i log. Un tempo questo poteva essere fatto manualmente per specifiche attività, ma oggi questo non può che essere fatto con strumenti automatici che lanciano allarmi in caso di eventi particolari, per esempio quando un sistema o un'applicazione non risulta più attivo, se è individuato un virus o si sono verificati errori nell'esecuzione di un backup.

Gli intrusion detection system o IDS sono sistemi di monitoraggio che individuano i tentativi di attacco ai sistemi informatici: analizzano il traffico della rete o le attività dei server e lanciano allarmi quando rilevano qualcosa di sospetto. Alcuni di questi strumenti possono attivare automaticamente azioni di contrasto; in questo caso sono denominati intrusion prevention system o IPS.

Oggi sono usati strumenti di SIEM (security information and event management), con algoritmi di intelligenza artificiale, che raccolgono i log dai sistemi, li correlano, elaborano un modello di comportamento “normale” (baseline) dei sistemi informatici e, a fronte di scostamenti, segnalano l'evento.

Da non sottovalutare i monitoraggi non strettamente di sicurezza, come quelli relativi a fermi, rallentamenti e presenza di possibili colli di bottiglia. Infatti anche la disponibilità è un parametro di sicurezza e una segnalazione di questo tipo potrebbe comunque essere originata da eventi di sicurezza come intrusioni.

A fronte di ciascun allarme, gli operatori devono seguire il processo di gestione degli incidenti, descritto nel paragrafo 12.13.

Il problema dei monitoraggi è l'elevato numero di avvisi che possono inviare agli operatori. Devono essere quindi configurati (attività di fine tuning) per evitare di segnalare falsi positivi, ossia allarmi relativi a eventi non meritevoli di attenzione.

Chi effettua il monitoraggio

Il monitoraggio è di norma fatto da un gruppo di operatori indicati con termini quali control room o network operation centre.

I termini ritenuti più corretti sono:

Network operation centre (NOC): effettua il monitoraggio della rete, non solo per rilevare intrusioni o altri attacchi, ma qualsiasi evento anomalo;

Security operation centre (SOC): effettua il monitoraggio della rete per rilevare gli incidenti di sicurezza occorsi nella rete; in questo caso, si intendono come incidenti di sicurezza i soli attacchi volontari; il SOC può far parte del NOC o essere un'entità indipendente che, tra gli altri compiti, controlla l'operato del NOC;

Computer emergency response team (CERT), Computer incident response team (CIRT) or Information security incident response team (ISIRT): gruppo di persone, in alcuni casi parte del SOC, addetto alla risposta agli incidenti rilevati dal SOC; il termine ISIRT è usato quando il gruppo si occupa di incidenti non

solo in ambito informatico.

12.9.6.4 Clock

Affinché gli strumenti di registrazione e di monitoraggio (inclusi quelli usati per la sicurezza fisica e la videoregistrazione) forniscano dati significativi, è necessario che gli orologi (o clock) dei sistemi siano tra loro sincronizzati. Per questo si fa solitamente uso di un server a cui fanno riferimento gli altri sistemi attraverso il network time protocol (NTP) o il precise time protocol (PTP).

Esempio 12.9.11. Una grande azienda non aveva i clock sincronizzati tra loro, con il risultato di avere alcuni sistemi con il fuso orario europeo e altri con quello cinese. Questo non ha consentito di tracciare adeguatamente un certo numero di attività.

I protocolli NTP e PTP devono essere configurati in modo tale da non verificare troppo spesso la sincronizzazione dei clock, generando un traffico di rete eccessivo, né effettuare le verifiche troppo di rado, consentendo la deriva dei clock.

Per assicurare una maggiore affidabilità del riferimento temporale, il server va collegato a un servizio di sincronizzazione per la rete Internet⁹⁸. Per un livello ulteriore di affidabilità, vanno usati più server pubblici in modo da evidenziare eventuali scostamenti.

Esempio 12.9.12. È qui opportuno riportare un esempio di come un controllo di sicurezza possa introdurre nuovi rischi, come già accennato nel paragrafo 9.3.1.4.

A fine 2013 sono stati condotti diversi attacchi DDoS sfruttando vulnerabilità del protocollo NTP⁹⁹.

Questo protocollo è infatti spesso configurato dagli operatori quando installano un nuovo sistema e poi “dimenticato”, tanto che raramente è censito nel CMDB e oggetto di patching.

12.9.6.5 Blockchain e registro distribuito

La tecnologia blockchain nacque per tenere traccia delle transazioni con valuta bitcoin, ossia come libro mastro. In questo caso, i log non sono conservati in un server centrale, ma sui computer dei partecipanti all'iniziativa. Osservando che i partecipanti non sono necessariamente persone fidate, i meccanismi per assicurare l'integrità e l'inalterabilità dei log furono progettati e realizzati per essere molto robusti.

La tecnologia fu poi generalizzata con il termine di registro distribuito e molte società hanno avviato progetti per utilizzarla in ambiti dove la tracciabilità è molto importante, come nel settore alimentare.

Nonostante molti ne parlino e siano di moda, spesso non è conveniente usare tecnologie di registro distribuito. Infatti queste applicazioni devono essere necessariamente complesse e poco flessibili¹⁰⁰ e questo, in molti settori, non è

auspicabile. Inoltre, proprio l'interesse eccessivo verso queste tecnologie ha portato all'avvio di progetti con finalità sbagliate, come se le tecnologie di registro distribuito possano garantire la qualità dei dati immessi, aumentare la fiducia in una singola azienda, rendere più veloce il tracciamento, conservare i documenti a lungo termine o il voto elettronico. Le difficoltà incontrate da molti progetti basati su blockchain o la loro irrilevanza, hanno dimostrato che spesso un'applicazione centrale ben progettata e realizzata è più economica, semplice da usare e veloce di una basata su registro distribuito.

12.9.7 Gestione della capacità

Va monitorata la capacità dei sistemi, ossia se la CPU, la RAM, la memoria di massa e la banda di rete, anche negli ambienti cloud, sono sature o prossime alla saturazione. Quando il livello di utilizzo di queste risorse supera una certa soglia, viene lanciato un allarme (un caso comune si verifica quando una mailbox sul server occupa troppo spazio). Quando una risorsa è satura o vicina alla saturazione, si possono aggiungere risorse (da gestire come cambiamenti, come descritto nel paragrafo 12.9.3) o intraprendere altre azioni.

È quindi una buona pratica produrre rapporti sulla capacità e analizzarli in modo da rilevare tendenze e prevenire problemi legati alla capacità.

Le azioni dovrebbero essere pianificate anche considerando il tempo necessario per la ricezione dei beni: questo è importantissimo quando sono usati strumenti particolari e il produttore deve essere contattato per tempo per inviare i nuovi componenti o le parti di ricambio. In alcuni casi vanno considerati rallentamenti burocratici, per esempio dovuti alle pratiche doganali.

Quando un nuovo sistema o un cambiamento significativo sono pianificati, vanno previsti stress test. Questi verificano che il sistema può lavorare alle

prestazioni previste quando riceve molte richieste simultanee, o sono connessi molti utenti o molti dati devono essere elaborati.

Gli ambienti di test hanno solitamente prestazioni inferiori a quelli di produzione e pertanto vanno previsti calcoli accurati per comprendere il reale risultato degli stress test.

Per gli stress test, potrebbero essere usate copie dei dati di produzione quando è troppo dispendioso creare da zero la quantità necessaria di dati. In questi casi, i dati delle copie dovrebbero essere mascherati o anonimizzati (vedere paragrafo 12.5.1.7).

Il termine “capacità” è solitamente usato per i sistemi informatici, ma riguarda anche il numero di persone e le loro competenze, lo spazio negli uffici e nei CED, il peso e i componenti che riscaldano e consumano energia dei CED (vedere 12.4.3, 12.8.1.8, 12.8.2.2).

12.9.8 Dispositivi portatili e personali

Tra i dispositivi portatili o mobili (mobile device) vi sono: PC portatili, tablet, cellulari o smartphone, chiavi USB e smart card. Ciascuno di questi oggetti può essere facilmente perso o rubato.

12.9.8.1 Controllo dei dispositivi

Come si è già visto in precedenza, i dispositivi devono essere censiti e assegnati

solo attraverso un preciso processo di autorizzazione, in modo da poterli ritirare quando opportuno. Per i cellulari e smartphone, vanno anche censiti i dati utili per bloccarli in caso di furto (codice IMEI).

Ai dispositivi portatili si devono applicare le medesime misure di sicurezza dei normali PC già descritte al paragrafo 12.9.2. Tra di esse vi sono: controllo degli accessi, cifratura dei dati, limitazione delle applicazioni da installare, limitazione delle connessioni, presenza di antivirus e backup dei dati.

Per i telefoni cellulari, gli smartphone ed i tablet, esistono alcuni programmi, in particolare i Mobile device management (MDM) e i Mobile application management (MAM), che consentono di configurarli centralmente, di impedire all'utilizzatore di modificare le misure di sicurezza e di controllare gli accessi alle applicazioni. Per i computer, sono disponibili software simili, tra cui il Windows Group Policies.

12.9.8.2 Regole per l'uso dei dispositivi

Al personale vanno fornite regole per l'uso dei dispositivi portatili e personali, anche quando meccanismi automatici di sicurezza sono attivi nella strumentazione fornita. Questo perché ne siano consapevoli.

Regole da fornire sull'uso di tutti i dispositivi:

non farli usare a persone non autorizzate per evitare che li danneggino (alcuni PC di lavoro versano in condizioni miserevoli perché lasciati ai figli per giocare) o compromettano la sicurezza dei dati deliberatamente o per errore, per esempio alterandoli o inviandoli a persone non autorizzate;

bloccarli con password se non utilizzati;

cifrare tutti i dati memorizzati, in modo che un eventuale furto non comporti anche la perdita di riservatezza delle informazioni.

Regole specifiche relative ai dispositivi portatili sono:

non lasciarli mai incustoditi (per evitare i furti; soprattutto in automobile e nelle aree di sosta delle autostrade);

evitare di usarli in luoghi pubblici con la possibilità che altri osservino i dati visualizzati a video (sono in commercio delle pellicole da applicare sui monitor per renderne impossibile l'osservazione a chi non si trova esattamente davanti a esso);

per quanto riguarda i cellulari e smartphone, ricordare di non intrattenere conversazioni riservate in luoghi pubblici e non lasciare messaggi vocali (perchè troppe persone, anche per maleducazione, li ascoltano in vivavoce).

12.9.8.3 Clear screen

Con l'espressione clear screen policy si designa la regola secondo la quale non devono essere letti documenti riservati su dispositivi informatici, non solo portatili, quando persone non autorizzate sono in grado di spiare lo schermo.

Da prestare attenzione anche al cosiddetto “desktop del computer”, evitando di avere su di esso troppi documenti, anche riservati o di avere abilitati avvisi pop-up di messaggistica, in modo che non appaiano quando persone non autorizzate potrebbero vederli.

12.9.8.4 Chiavi USB

Le chiavi USB sono dei dispositivi portatili molto critici, perché utilizzate per conservare dei dati e possono essere facilmente rubate o perse. Per questo alcune organizzazioni configurano i sistemi affinché non sia possibile collegarle, oppure sia possibile usarle solo se sono attivi dei meccanismi crittografici.

Gli utenti devono memorizzare sulle chiavi USB solo i dati a cui possono accedere le persone con cui sono condivise le chiavi.

Infine, agli utenti devono essere messi a disposizione degli strumenti per cancellare in modo sicuro i dati dalle chiavi USB (paragrafo 12.8.2.7).

12.9.8.5 COIT e BYOD

Oggi è sempre più diffuso il fenomeno detto consumerization of IT (COIT) o, in italiano, IT aziendale guidato dal consumatore. Riguarda l'uso di strumenti hardware e software personali per attività lavorative. Questo fenomeno si sta sempre più diffondendo perché spesso i dispositivi personali sono più potenti, leggeri e facilmente utilizzabili di quelli forniti dall'organizzazione per cui si lavora (si osserva qui, come segno dei tempi, che 10 anni fa si aveva il problema dell'utilizzo del materiale aziendale per scopi personali, mentre oggi si ha l'inverso).

Durante l'emergenza COVID, molte persone che lavoravano unicamente in ufficio e con strumentazione fissa sono state costrette a ricorrere al BYOD, ossia

usare in casa i propri PC personali in attesa che la loro organizzazione si approvvigionasse di dispositivi portatili e li distribuisse al personale.

Parte di questo fenomeno è noto come bring your own device (BYOD) ed è riferito alle persone che utilizzano strumenti hardware personali per lavoro. Si tratta soprattutto di cellulari, smartphone, tablet e computer portatili.

Nel COIT sono compresi anche gli utilizzi a scopo lavorativo degli account personali dei social network (Facebook, LinkedIn e altri) o dei sistemi di condivisione dei documenti (Dropbox, Google Drive e altri).

L'uso di strumenti personali per attività lavorative introduce vulnerabilità: molti non impostano le password per l'accesso ai propri dispositivi oppure li fanno utilizzare ad altre persone che potrebbero leggere, alterare o trasmettere dati riservati. In generale, l'uso di strumenti personali può portare alcune persone a ritenere come personali le informazioni dell'organizzazione e quindi a usarle in modo non corretto.

Un ulteriore rischio riguarda il personale addetto all'assistenza informatica, che potrebbe essere sottoposto a un sovraccarico di lavoro dovuto alla numerosità e eterogeneità degli strumenti da tenere sotto controllo.

Alcune organizzazioni non permettono l'uso di strumenti personali, oppure lo permettono solo a condizione che corrispondano a certi modelli e siano stati configurati da parte dei tecnici dell'organizzazione o gestiti attraverso l'MDM o il MAM dell'organizzazione. Più spesso le aziende accettano il COIT e forniscono al personale delle regole a cui attenersi, anche se questa è una misura molto debole.

Da ricordare che, se si mette a disposizione un servizio di webmail per l’accesso all’email dell’organizzazione, visto che è accessibile dal web, si consente implicitamente l’uso di dispositivi personali. I Cloud access security broker (CASB) possono essere usati per selezionare i dispositivi che accedono alle applicazioni di un’organizzazione disponibili su Internet.

12.9.9 Cancellazione dei dati

Le informazioni vanno cancellate quando si è concluso il loro tempo di conservazione (vedere 12.5.1.8). Questo è importante per i dati personali perché tutelati dalla normativa in materia di privacy. Le tecniche sono illustrate al paragrafo 12.8.2.7.

Per alcuni dati, e in particolare per i dati personali, è opportuno stabilire meccanismi automatici di distruzione o di avviso a scadenze prefissate o allo scadere del tempo di conservazione (retention time).

Bisogna prestare attenzione ai dati presso i fornitori, quando termina la collaborazione: essi vanno ritirati o copiati e poi cancellati in modo sicuro. L’operazione è solitamente lasciata al fornitore, al quale però vanno imposti metodi di cancellazione sicuri.

Da ricordare che molti fornitori (per esempio consulenti del lavoro e commercialisti) devono conservare autonomamente i dati per un tempo successivo alla chiusura del contratto per poter gestire eventuali contestazioni o richieste da parte dell’autorità giudiziaria.

Tra i fornitori sono da considerare quelli dei servizi cloud. Essi solitamente

mettono a disposizione dei clienti gli strumenti necessari per la cancellazione sicura dei dati o, per esempio per i servizi IaaS (dove è fornita un'infrastruttura in ambiente cloud), i clienti possono installarli in autonomia.

In tutti i casi, prima di iniziare a usare i servizi di un fornitore, è buona norma informarsi sui metodi di cancellazione previsti.

12.10 Sicurezza delle comunicazioni

Nei paragrafi precedenti abbiamo visto molti aspetti applicabili alla gestione delle comunicazioni: la necessità di effettuare ogni cambiamento in modo controllato e tenendo presenti i requisiti di sicurezza (paragrafo 12.9.3), configurare le trasmissioni in modo che siano cifrate soprattutto quando attraversano reti pubbliche (paragrafo 12.7), controllare gli accessi agli apparati di rete (paragrafo 12.6), monitorare le attività sospette e registrare alcune operazioni per ricostruire quanto avvenuto (paragrafo 12.9.6).

Questo paragrafo è dedicato a ulteriori aspetti di sicurezza della rete informatica e degli scambi di informazioni.

12.10.1 Servizi autorizzati

Una prima questione riguarda quali servizi esterni possono essere utilizzati dal personale all'interno di un'organizzazione: in alcuni casi, infatti, è impedito l'uso di posta elettronica personale, instant messaging, social network o altri servizi Internet e siti web (per esempio, pornografici o di scambio di video, musica o materiale illegale) attraverso firewall per il controllo delle connessioni e meccanismi di web content filtering per il controllo dei siti visitati e per

impedire l'accesso a siti notoriamente dannosi (che per esempio distribuiscono malware). Questo per evitare perdite di tempo del personale, comportamenti moralmente discutibili, scambio non autorizzato di materiale riservato o di file dannosi e saturazione delle risorse informatiche. Inoltre, meno servizi sono accessibili, meno vulnerabilità sono sfruttabili da malintenzionati.

Il blocco dei servizi può essere aggirato dal personale se connette il proprio computer a Internet attraverso il proprio cellulare o smartphone. Questa pratica è molto pericolosa perché, se il computer è collegato contemporaneamente al cellulare o smartphone e alla rete interna dell'organizzazione, un malintenzionato può usarlo come “ponte” per accedere alla rete interna. Pertanto tale pratica va vietata esplicitamente dalle regole e politiche dettate al personale e, se possibile, configurando opportunamente i computer in dotazione.

Una seconda questione riguarda quali servizi dell'organizzazione (siti web, condivisione file, email, applicazioni, eccetera) possono essere utilizzati da persone all'esterno di essa, come utenti, clienti, fornitori e partner. In questo caso occorre bilanciare il principio per cui meno servizi sono attivi, meno vulnerabilità possono essere sfruttate da malintenzionati, insieme alla necessità di interfacciarsi con il mondo esterno. Queste scelte fanno parte della valutazione del rischio.

Per esempio, alcuni permettono l'accesso all'email ma non al file server (anche se oggi sono spesso ambedue sul cloud e accessibili da ogni luogo).

Una terza questione riguarda i servizi terzi che devono essere usati dal personale per ragioni di lavoro. Per questi è necessario considerare i livelli di sicurezza e di servizio offerti da questi servizi e la capacità del fornitore di rispettare gli impegni (vedere anche il paragrafo 12.12). La scelta dei servizi, e quindi dei livelli di sicurezza e di servizio offerti, da valutare in modo via via diverso, è molto ampia e include: social network gratuiti per la ricerca del personale e la promozione della propria organizzazione; servizi a pagamento per la

conservazione di documenti o l'elaborazione delle buste paga; email; gestione della sicurezza della rete con soluzioni cloud; gestionali per le vendite e le opportunità commerciali.

12.10.1.1 Social network

I social network, possono costituire un mezzo per lo scambio non autorizzato di informazioni, far perdere tempo alle persone, essere usati per diffamare la propria organizzazione¹⁰¹. Il blocco di questi servizi non elimina certamente tali minacce, perché comunque gli utenti possono accedervi da casa o da dispositivi personali, ma può ridurne l'estensione.

D'altra parte, i social network permettono di monitorare il mercato e le opinioni sui propri prodotti o servizi e di interagire con i propri clienti. Alcune organizzazioni, quindi, permettono l'accesso ai social network solo ad alcune funzioni o persone.

Spesso i social network sono gestiti da società estere e pertanto, prima di decidere se usarli per le attività lavorative, è necessario valutare se ammissibili dalla normativa vigente in materia di protezione dei dati personali.

12.10.1.2 Servizi di file sharing

Per i servizi di file sharing offerti da entità esterne è necessario stabilire, dopo un'attenta valutazione delle garanzie offerte, quali sono quelli autorizzati e per quali informazioni.

Alcune organizzazioni vietano l'uso di tutti i servizi di file sharing, bloccandoli anche con i firewall; altre ne permettono alcuni, elencati nelle procedure distribuite al personale; altre ancora ne gestiscono autonomamente uno per le comunicazioni con i propri clienti, fornitori e partner (questo è un esempio di servizio informatico condiviso).

Da evitare i servizi di file sharing pubblici per ovvi motivi di riservatezza, i link diretti perché possono essere usati in modo scorretto¹⁰² e server FTP privati perché insicuri a causa di numerose vulnerabilità (si possono usare server SFTP e FTPS).

Come per i social network, molti di questi servizi sono offerti, anche gratuitamente, da società estere e pertanto ne vanno valutati gli impatti sulla normativa in materia di privacy. In alcuni casi, è possibile configurare questi servizi affinché usino solo server in determinate zone geografiche (per esempio in Europa), ma non sempre le autorità ritengono questa misura sufficiente, visto che il personale addetto alla loro manutenzione risiede in altri Paesi.

12.10.1.3 Servizi di configurazione

I servizi di configurazione consentono di gestire i sistemi informatici a distanza. Questa possibilità è molto comoda per gli operatori perché non devono accedere al CED ogni volta che devono effettuare dei cambiamenti. I malintenzionati possono attaccare questi servizi per potere, a loro volta, prendere il controllo dei sistemi.

Da stabilire quali di questi servizi sono da utilizzare per poi bloccare tutti gli altri, soprattutto quelli noti per le loro vulnerabilità, come l'SNMP o l'ICMP. Per ognuno è necessario stabilire se possono essere accessibili dall'esterno dell'organizzazione. In tutti i casi le comunicazioni vanno protette con

meccanismi crittografici.

12.10.1.4 Reti wi-fi

L'uso delle reti wi-fi è sempre oggetto di discussione perché i loro meccanismi di controllo degli accessi presentano diverse vulnerabilità sfruttabili da malintenzionati per accedere a una rete senza la necessità di connettersi fisicamente.

Molte organizzazioni hanno deciso di non installare reti wi-fi. Altre di installarle solo per gli ospiti e tenerle separate dalla rete interna. Altre ancora le rendono disponibili agli interni e le collegano alla rete interna, ma dopo aver attivato ulteriori meccanismi di sicurezza per evitare le intrusioni di malintenzionati.

Le reti wi-fi non protette per gli ospiti potrebbero essere usate dal personale interno se la connessione messa a loro disposizione limita o controlla gli accessi a taluni servizi Internet. Per questo, è conveniente controllare l'accesso a queste reti con password da consegnare solo agli ospiti e da modificare frequentemente e limitare l'utilizzo dei servizi Internet nello stesso modo con cui sono limitati per il personale interno.

Quando l'accesso alla rete wi-fi è controllato da credenziali, queste sono da gestire secondo un processo definito, come indicato nel paragrafo 12.6.

12.10.1.5 Accesso alla rete dei visitatori

Quando si permette a visitatori e fornitori l'accesso alla propria rete, sono da controllare i meccanismi di sicurezza presenti sui loro dispositivi, tra cui: antivirus, controllo degli accessi e limitazione dei programmi installati. Alcuni richiedono di utilizzare partizioni cifrate per archiviare i documenti consegnati.

Se i dispositivi non dovessero soddisfare i requisiti di sicurezza stabiliti, l'organizzazione deve impedire loro l'accesso alla propria rete ed, eventualmente, mettere a disposizione un computer opportunamente configurato per svolgere le attività previste o per accedere a Internet, ad esempio per consultare la propria posta elettronica.

Per controllare i dispositivi connessi alla rete sono in commercio strumenti denominati Network access control o NAC, utili anche per impedire la connessione di esterni che riescono ad avere accesso fisico ai nodi della rete dell'organizzazione.

12.10.2 Segmentazione della rete

La rete informatica di un'organizzazione deve essere:

separata da Internet, per evitare accessi non autorizzati;

segmentata al suo interno, per:

ridurre le possibilità di intercettazione di informazioni da parte di interni malintenzionati o di esterni che hanno ottenuto accesso a una parte della rete;

evitare la saturazione di tutta una rete a causa dell'eccessivo traffico di dati originato da una sua parte.

Caso particolare di segmentazione di rete si ha quando l'organizzazione è presente in più sedi e quando il personale deve accedere alla rete interna da Internet (paragrafo 12.10.2.4).

Le comunicazioni tra i segmenti di rete devono avvenire in modo sicuro, per esempio cifrandole.

12.10.2.1 Separazione da Internet

Le apparecchiature dedicate a filtrare il traffico, incluso quello da e a Internet, sono detti firewall.

I servizi esposti al pubblico (per esempio il modulo di presentazione di un servizio web con architettura three tiers o una parte dell'email server) dovrebbero trovarsi in un segmento di rete detto de-militarized zone o DMZ, separato da Internet e dalla rete interna da firewall. La DMZ permette di filtrare le richieste al server esposto al pubblico e le comunicazioni tra questo server e i sistemi interni di elaborazione o di database.

I server nella DMZ sono configurati in modo particolarmente attento con tecniche di hardening per limitare al massimo lo sfruttamento di vulnerabilità e funzionalità da parte di malintenzionati.

Sulle DMZ sono non di rado presenti ulteriori controlli di difesa perimetrale tra loro complementari, tra cui:

web proxy, IP filtering e firewall per controllare l'accesso ai servizi Internet da parte del personale interno ed evitare abusi o attacchi; questo può includere la limitazione nell'uso di social network, servizi di file sharing pubblici, webmail personali, siti pornografici, di entertainment e di gaming;

web content filtering per bloccare l'accesso a siti sospetti o con contenuti illegali;

antimalware e mail relay per rilevare virus nelle comunicazioni da e a Internet, incluse quelle via email;

intrusion detection system e intrusion prevention system per rilevare tentativi di attacco alla rete o prevenirli;

network address translation e reverse proxy per mascherare la configurazione della rete interna;

web application firewall o WAF per controllare le richieste che ricevono le applicazioni e, se sono attacchi a livello applicativo, le bloccano (i WAF vanno però riconfigurati ogni volta che un'applicazione è modificata).

Per approfondimenti si raccomanda lo studio di testi dedicati [34, 165].

Per i siti web, molte organizzazioni preferiscono averli su una rete completamente separata presso fornitori esterni, applicando così uno dei più diffusi esempi di condivisione del rischio.

12.10.2.2 Segmentazione della rete interna

Una rete interna è detta Local area network (LAN) e può venire suddivisa in

sottoreti. Tra di esse si possono trovare:

- la rete dei server dedicati all'elaborazione dati (application server);
- la rete dei server dedicati all'archiviazione dei dati (database server e storage server);
- la rete alla quale sono connessi i PC del personale;
- la rete alla quale sono connessi i PC degli amministratori di sistema (retedi management).

La segmentazione interna può avvenire tramite router e switch per rendere efficiente il traffico e firewall per filtrare le comunicazioni tra i vari segmenti. Anche gli switch permettono di attivare dei filtri, impostando delle Virtual LAN o VLAN.

La segmentazione della rete è la tecnica più efficace per ridurre gli impatti di un attacco ransomware (oltre ai backup offline e all'aggiornamento di tutti i sistemi), ma richiede, perché sia completa (per esempio, i sistemi usati per consultare l'email vanno separati completamente da quelli per l'amministrazione della rete) significativi investimenti.

Un'ulteriore segmentazione richiederebbe di rinunciare alla cosiddetta convergenza, ossia l'integrazione di tutti i sistemi informatici di un'organizzazione. La convergenza ha indubbi benefici perché permette, alle organizzazioni, di ridurre i costi e migliorare l'efficienza di alcune attività e, ai privati, di avere maggiori comodità (per esempio, controllando più dispositivi con uno smartphone). La scelta di perseguire la convergenza o segmentare per aumentare la sicurezza è quindi una scelta tra aumentare o mitigare il rischio di sicurezza delle informazioni.

Le reti interne possono essere segmentate con meccanismi di ponti levatoi (drawbridge), che permettono di isolare la rete appena si rilevano attacchi. Questo accorgimento è molto utilizzato negli ambienti manifatturieri (e in particolare di produzione dei medicinali), dove la rete di produzione deve rimanere attiva, anche se isolata, anche in caso di attacco.

12.10.2.3 Segmentazione della rete operativa

L'espressione operational technology (OT) è usata per indicare le tecnologie informatiche usate per il controllo degli impianti, inclusi quelli industriali. Per questi ultimi sono usate anche le espressioni industrial automation and control systems (IACS) e industrial control systems (ICS). Le tecnologie usate per il solo monitoraggio sono invece indicate dal termine supervisory control and data acquisition (SCADA).

In questi casi, si intende come information technology (IT) quella usata per le attività “di ufficio” (progettazione, disegno, navigazione Internet, ricezione e invio di email).

La rete OT va completamente separata da quella IT. Ovviamente questo accorgimento richiede una certa spesa e il rinunciare alla convergenza, ma oggi è sempre più necessaria, visti i numerosi attacchi che sono stati portati con successo compromettendo inizialmente i sistemi di ufficio e gli impatti potenzialmente devastanti che possono essere causati da malfunzionamenti degli oleodotti, dei gasdotti, dei sistemi di distribuzione dell'acqua potabile, della rete elettrica.

Esempio 12.10.1. Colonial Pipeline è una società statunitense dedicata al trasporto di carburante. Ad aprile 2021 fu attaccata da un ransomware e dovette quindi chiudere temporaneamente alcuni chilometri di rete.

Questo genere di attacchi era già stato segnalato dalla Cybersecurity and Infrastructure Security Agency (CISA) che aveva indicato, come principale misura di difesa, proprio la separazione delle reti OT e IT¹⁰³.

12.10.2.4 Connessioni esterne

Se l'organizzazione è suddivisa in più sedi, bisogna prevedere connessioni sicure tra di esse. La connessione tra più sedi della medesima organizzazione si definisce Wide area network (WAN). Oggi, solitamente, la si crea usando la rete Internet e attivando canali cifrati di comunicazione. In questo modo, si crea una specie di rete privata su un'infrastruttura pubblica, denominata VPN (Virtual private network).

Quando il personale fuori sede deve accedere alla rete dell'organizzazione effettua un accesso remoto. Anche in questo caso possono essere create delle VPN tra il PC della singola persona e la rete interna.

Una VPN può consentire l'accesso ai medesimi dati e alle medesime applicazioni di quando si è in sede. Questo può costituire una notevole vulnerabilità e quindi si devono limitare i servizi accessibili dal personale esterno a quelli essenziali e le persone devono essere opportunamente autorizzate a questo tipo di accesso.

12.10.2.5 Segmentazione e privilegi minimi

Per la segmentazione della rete deve essere seguito il principio dei privilegi minimi che prevede di bloccare ogni comunicazione tra i diversi segmenti e attivarla solo quando richiesto da persone autorizzate seguendo il processo previsto per la gestione dei cambiamenti (paragrafo 12.9.3).

Eventuali richieste di apertura temporanea di canali di comunicazione (per esempio, quando si effettuano determinati test tra reti di test e rete di produzione o quando si permette a fornitori esterni di svolgere le attività di assistenza da remoto) vanno registrate e tenute sotto controllo in modo da chiudere questi canali appena possibile.

Ogni configurazione deve essere verificata periodicamente: in molti casi, un servizio viene disattivato o non è più utilizzato, ma le porte utilizzate per accedervi rimangono aperte e possono essere utilizzate per attaccare la rete. Per questa ragione, molti firewall permettono di condurre analisi sulle porte non utilizzate.

12.10.3 Sicurezza della rete

12.10.3.1 Gestione della rete

Per la sicurezza della rete devono essere attuate misure già approfondite in altri paragrafi. Tra di esse ricordiamo:

mantenere documentazione aggiornata, inclusi diagrammi di rete (vedere 12.9.1);

prevedere canali di comunicazione cifrati (vedere 12.7);

tracciare e monitorare le azioni significative per la sicurezza (vedere 12.9.6);

autenticare i sistemi sulla rete (vedere 12.6.2.8 e 12.10.3.3)

limitare e filtrare le connessioni dei sistemi alla rete (vedere 12.10.2);

segregare la rete interna, inclusa la rete di amministrazione dalle altre reti (vedere 12.10.2.2);

configurare in modo sicuro i dispositivi di rete (vedere 12.9.2);

disabilitare i protocolli di rete vulnerabili (vedere 12.9.2 e 12.10.1.3).

12.10.3.2 Sicurezza degli apparati di rete

Con il termine apparati di rete si intendono tutti i sistemi di controllo del traffico e della sicurezza di rete, tra cui router, switch e firewall.

Queste apparecchiature sono spesso vendute come appliance, ossia strumenti integrati hardware e software, dedicati al compito per cui sono stati progettati. Le medesime funzionalità possono essere svolte da normali computer (anche su macchine virtuali), purché abbiano il giusto hardware e software; le appliance possono offrire prestazioni e livelli di sicurezza migliori perché specializzate.

Ogni modifica della configurazione degli apparati di rete deve seguire il processo di gestione dei cambiamenti (paragrafo 12.9.3); in particolare ogni cambiamento va autorizzato considerando i suoi impatti sulla sicurezza della rete.

Gli stessi apparati di rete devono essere configurati con tecniche di hardening (paragrafo 12.9.2). Tra le tante misure merita ricordare: limitazione delle utenze e delle autorizzazioni al minimo necessario, creazione di utenze personali per ciascun operatore addetto, logging delle attività, cifratura delle connessioni, disattivazione dei servizi e disinstallazione dei programmi non strettamente necessari e dei protocolli vulnerabili (per esempio SNMP e ICMP).

È opportuno ricordare che gli apparati di rete sono complessi da gestire e non sicuri come si potrebbe immaginare. Per alcuni apparati, anche molto costosi, è complesso impostare i parametri di sicurezza minimali¹⁰⁴. Questo perché sovente le impostazioni predefinite privilegiano la facilità di utilizzo rispetto alla sicurezza. È quindi fondamentale avere personale tecnicamente preparato, con le opportune certificazioni professionali, e aggiornato (paragrafo 12.4.3). Si raccomanda infine di predisporre delle check list per garantire la correttezza delle operazioni (paragrafo 12.9.1).

Gli apparati di rete, come i server, non sono normalmente gestiti collegandosi direttamente a essi con uno schermo e una tastiera (accesso diretto o da console), ma da remoto, da personale che si collega dalla rete di management. Per evitare intercettazioni, la connessione va cifrata (con protocolli SSH quando si usa l’interfaccia a carattere o HTTPS quando si usano interfacce grafiche di tipo web).

12.10.3.3 Controllo degli accessi agli apparati di rete

Gli apparati di rete, spesso, permettono la creazione di un solo utente addetto alla loro amministrazione. Questa credenziale è quindi condivisa e va gestita come visto nel paragrafo 12.6.2.7. È possibile fare uso di alcuni strumenti per imporre l’uso di credenziali personali (per esempio RADIUS e TACACS), ma, per poter intervenire in caso di emergenza, tali strumenti sono spesso inefficaci

per gli accessi da console, a cui si può accedere facendo uso dell’utenza unica di amministrazione.

Gli accessi da console vanno quindi regolamentati, specificando le persone autorizzate e attivando anche controlli di accesso fisico.

Oggi sono disponibili software di password management o password vault per memorizzare questo tipo di credenziali e fare in modo che ciascun operatore autorizzato possa vedere solo quelle a lui necessarie (per esempio, gli addetti alla gestione dei firewall non possono visualizzare le password di accesso ai router).

In molti, per pigrizia (indicata però come “efficienza”), impostano per tutti gli apparati le medesime credenziali di accesso da console. In questo caso, quando un operatore lascia l’organizzazione, tutte le credenziali devono essere modificate. Oggi questa attività può essere semplificata con gli strumenti di gestione delle credenziali degli apparati di rete.

Particolarmente critico è il caso in cui si fa uso di fornitori per la manutenzione degli apparati: alcune grandi organizzazioni, come le banche o gli operatori di telecomunicazioni, fanno uso di fornitori per gli interventi sui sistemi presso filiali e clienti sparsi sul territorio. In questo caso gli apparati devono essere configurati con ciascuno le proprie credenziali per l’accesso da console e tale regola deve essere imposta ai fornitori; inoltre si devono stabilire dei processi da seguire quando si cambiano fornitori e quando cambiano i loro operatori, in modo da modificare le credenziali a loro note.

Per accedere agli apparati sono solitamente disponibili due tipologie di interfacce: a carattere o grafica. Gli amministratori di sistema molto esperti preferiscono le interfacce a carattere, maggiormente flessibili. D’altra parte, le interfacce grafiche offrono spesso funzionalità per ridurre al minimo gli errori

degli operatori, per esempio instaurando automaticamente una connessione cifrata e chiedendo più volte conferma delle modifiche. Quali che siano le modalità scelte, vanno regolamentate per iscritto anche per evitare la proliferazione di strumenti tra loro diversi.

12.10.4 Scambi di informazioni

Questo argomento non riguarda solo l'IT, ma anche lo scambio di informazioni in formato non digitale, per esempio cartaceo o orale.

Questo paragrafo è quindi suddiviso in:

regole generali;

misure informatiche;

misure non informatiche.

Si discute anche di non ripudiabilità, introdotta nel paragrafo 2.2.

12.10.4.1 Regole generali

La prima misura di sicurezza per garantire la sicurezza degli scambi di informazioni consiste nel chiarire quali sono quelle riservate e critiche; ciò può essere ottenuto attraverso la classificazione delle informazioni (paragrafo 12.5.1).

Devono quindi essere emesse regole per il trasferimento delle informazioni riservate o classificate, atte a stabilire quali informazioni possono essere trasferite, a chi lo possono essere (funzioni interne, clienti, fornitori, partner, eccetera) e quali strumenti utilizzare.

Tra le regole vanno incluse le modalità per segnalare ai destinatari l'eventuale classificazione e le caratteristiche di riservatezza delle informazioni trasferite, per esempio all'inizio del messaggio o nell'oggetto dell'email, nel nome del file o con etichette (vedere 12.5.1.4). Come già ricordato in precedenza, bisogna considerare il rischio che queste etichette possono attirare l'attenzione di estranei.

Le regole interne a un'organizzazione vanno poi condivise di volta in volta con gli interlocutori esterni come clienti, fornitori e partner. Se clienti, fornitori e partner hanno proprie regole, è da prevedere un processo per concordare e attuare regole comuni e utilizzare strumenti tra loro compatibili (per esempio, per cifrare e decifrare i messaggi).

12.10.4.2 Misure informatiche

Le misure informatiche devono essere regolamentate formalmente dall'organizzazione. Dopo averle discusse, in questo paragrafo si proporranno considerazioni in merito ad alcune tecnologie specifiche.

Regole per l'uso degli strumenti informatici

Per l'uso dei servizi di comunicazione come email, instant messaging, file sharing e social network, occorre fornire regole comportamentali a tutto il personale, oltre a stabilire quali servizi sono autorizzati e quali no, anche in relazione ai loro diversi livelli di sicurezza.

Una prima regola prevede di autenticare, in qualche modo, il destinatario. Gli indirizzi email e le identità sui social network possono essere falsificati¹⁰⁵. Non esiste un unico metodo per identificare l'interlocutore, ma è fondamentale non accettare istruzioni (per esempio sui metodi di pagamento) da indirizzi email o numeri di telefono mai usati in precedenza.

Le trasmissioni critiche vanno tracciate e solitamente gli strumenti informatici lo fanno.

Alcune regole, necessarie anche per evitare la saturazione della capacità della rete, sono: non utilizzare i servizi per attività illegali o moralmente discutibili, utilizzare i servizi messi a disposizione dall'organizzazione solo per scopi lavorativi e non trasferire file di grandi dimensioni se non in casi eccezionali e con specifici strumenti di file sharing segnalati dall'organizzazione stessa.

Se le regole richiedono l'uso di strumenti tecnologici, per esempio per cifrare le comunicazioni, è importante che questi siano forniti al personale insieme ai manuali d'uso: sono molti i casi in cui si chiede di cifrare dei documenti senza che al personale sia precisato quale programma utilizzare, come configurarlo e come utilizzarlo.

Per evitare che le trasmissioni vengano usate per attaccare la rete, è necessario verificare tutti i file ricevuti con strumenti di rilevazione del malware (vedere 12.9.4).

Le regole potrebbero richiedere di garantire la sicurezza di alcune comunicazioni attraverso meccanismi di cifratura dei dati o basati su password, di cui in figura 12.10.1 è riportato un esempio.

Password



'Documento-riservato.pdf' is protected. Please enter a Document Open Password.

Enter Password:

A password input field with a placeholder text 'Enter Password:' and a small yellow bullet icon to its left.

Cancel

OK

Figura 12.10.1:

File con accesso controllato da password

Per la crittografia, è necessario stabilire un metodo di scambio delle chiavi, come discusso nel paragrafo 12.7. La crittografia può essere usata per apporre firme digitali e quindi per prevenire il ripudio della ricezione del messaggio.

Quando sono utilizzati meccanismi basati su password, alcuni la concordano via SMS o via telefono, ma si tratta di metodi insicuri perché facilmente intercettabili: solo l'uso della crittografia a chiave pubblica garantisce un buon livello di sicurezza.

Email

Oggi l'email è uno dei mezzi più comuni per scambiare informazioni, anche se superato dai social network e dagli instant messages. Esso è molto insicuro perché semplice da intercettare, non fornisce al mittente la certezza del recapito, non dà alcuna certezza sulla sua velocità e può essere facilmente ripudiabile. Per comunicazioni importanti è quindi sempre necessario chiedere un riscontro al destinatario o utilizzare altri strumenti come il telefono.

In Italia è diffuso l'uso della Posta elettronica certificata (PEC, che sarà sostituita dalla SERC o servizio elettronico di recapito certificato o REM o registered email), come da Regolamento eIDAS), obbligatoria per le imprese, le ditte individuali, le Pubbliche amministrazioni e i professionisti. Essa è una forma di email equivalente alla lettera raccomandata con ricevuta di ritorno (non al documento firmato), se inviata ad altro indirizzo PEC, e può essere utilizzata per

prevenire il ripudio della ricezione delle comunicazioni.

Ulteriori regole per l'uso dell'email prevedono: non partecipare a catene di S. Antonio, non richiedere ricevuta delle email se non quando necessario, inserire i propri riferimenti al termine delle email con indicato il proprio ruolo.

L'uso dell'out-of-office, ossia degli avvisi ai mittenti quando il destinatario è assente, può essere utile per avvisare clienti, fornitori e partner, ma permette ai malintenzionati di sapere, per esempio, quando gli uffici di un'organizzazione non sono presidiati. Per questo motivo il loro utilizzo deve essere attentamente ponderato, valutato e regolamentato.

Per evitare spedizioni di email a destinatari sbagliati, è necessario educare il personale a prestare attenzione all'inserimento degli indirizzi dei destinatari, soprattutto quando "aiutato" da funzioni di auto-completamento (è inutile, e qui non raccomandata, la pratica di scrivere nelle email "se non sei il legittimo destinatario, distruggi questa email").

SMS, instant messaging e messaggi vocali

Come il servizio di email, anche gli SMS sono basati su protocolli inaffidabili, ossia non ne è garantita la ricezione da parte del destinatario. Il loro utilizzo per comunicazioni urgenti andrebbe quindi scoraggiato.

Gli strumenti di instant messaging (i più popolari sono WhatsApp, Messenger, WeChat, Telegram e Snapchat) stanno sostituendo gli SMS e sono più affidabili perché danno conferma di ricezione.

È da ricordare che questi strumenti sono di proprietà di società private (per esempio WhatsApp è di proprietà di Meta) che possono usare i contenuti dei messaggi per profilare le persone o raccogliere informazioni critiche. Un'organizzazione deve stabilire quali autorizzare, anche valutandone le funzionalità di sicurezza e, se gestiti da società estere, come ormai consueto, gli impatti sulla conformità alla normativa privacy.

Da evitare l'invio di messaggi con informazioni riservate, sia perché cellulari e smartphone possono essere rubati e quindi l'informazione diventare nota a persone non autorizzate, sia perché il ricevente, non aspettandosi di ricevere informazioni critiche, potrebbe visualizzare il messaggio quando è con altre persone che, pertanto, sarebbero in grado di leggerlo.

I servizi di instant messaging offrono funzionalità come i messaggi vocali (che possono essere ascoltati ad alto volume in luoghi pubblici) e pertanto il personale deve ricevere regole su come usarle.

L'impatto degli strumenti di messaggistica sulle persone e il rischio di burn-out non sono oggetto di questo libro, ma andrebbe comunque considerato.

Social network

Le organizzazioni dovrebbero fornire regole relative all'uso di social network. Molte di esse sono le stesse indicate per l'email e i sistemi di messaggistica istantanea, incluso il divieto di usarli per trasmettere informazioni riservate.

Regole specifiche per i social network sono:

non usarli, neanche con la propria utenza personale e non legata all’organizzazione, per commenti ingiuriosi verso il proprio datore di lavoro, i suoi clienti, i suoi fornitori, i suoi partner e le altre parti interessate;

non fornire, se non nei casi ammessi dall’organizzazione, dettagli sulla propria posizione lavorativa (anche se questo è molto difficile, considerando la diffusione di LinkedIn);

fare in modo che, se non nei casi ammessi dall’organizzazione, i propri commenti siano considerati solo come personali e non dell’organizzazione.

Servizi di file sharing

Come già specificato in 12.10.1.2, l’organizzazione deve stabilire se e quali sono i servizi file sharing autorizzati e renderli noti a tutto il personale.

Se si permette l’uso di servizi di file sharing, si raccomanda di vietarne l’uso con account personali per evitare, tra l’altro, che alcuni confondano i file di proprietà dell’organizzazione con quelli propri.

Programmi di automazione per l’ufficio

Per prevenire la diffusione imprevista di informazioni riservate, le persone vanno educate all’uso dei programmi di automazione per ufficio, in particolare affinché pongano attenzione agli strumenti di revisione, alle proprietà del documento (inclusa l’icona, perché spesso in forma di anteprima), alle copie di backup

generate automaticamente e ad altre funzionalità che potrebbero rivelare informazioni non previste dall'autore.

12.10.4.3 Misure non informatiche

Quando si trasferiscono informazioni in formato non digitale e i supporti digitali portatili (come le chiavi USB) all'esterno delle sedi dell'organizzazione o, in alcuni casi, anche all'interno dell'organizzazione, a seconda della loro classificazione, sono da stabilire le modalità di:

verifica della ricezione e il non ripudio: attraverso la posta ordinaria (anch'essa inaffidabile perché non dà certezza della consegna) o con avviso di ricezione, corrieri fidati o consegna di persona;

imbustamento, affinché le informazioni non vengano lette o modificate da persone non autorizzate: si può richiedere l'uso di buste senza trasparenze e l'applicazione di sigilli; per i casi più critici è possibile usare valigette con serratura e resistenti al fuoco;

tracciamento per poter dimostrare l'avvenuto invio e, come sopra ricordato, la ricezione;

etichettatura, per indicare al destinatario le caratteristiche di sicurezza delle informazioni, evitando però che possano essere sfruttate da malintenzionati;

verifica della completezza, nel caso il materiale sia numeroso, per esempio con liste di controllo;

trasporto, anche con istruzioni al personale addetto per assicurare l'integrità, oltre che la riservatezza, di quanto trapiantato.

Al personale fuori sede deve essere richiesto di non lasciare mai incustoditi i

documenti riservati e di prestare la dovuta attenzione affinché non siano letti da persone non autorizzate, per esempio in treno.

Fotocopiatrici, fax e stampanti

Ulteriori norme vanno fornite per l'uso di fotocopiatrici, fax e stampanti: capita spesso di trovare nei pressi di questi apparecchi documenti molto riservati non prelevati dalla persona interessata. Per l'invio di fax riservati (anche se oggi è preferibile l'invio via email della scansione, dopo averla cifrata o protetta con una password), bisogna preavvertire il destinatario affinché rimanga presso lo strumento fino alla completa ricezione del documento.

Per le stampanti, è già stato ricordato in precedenza che è possibile bloccarle fino a quando non viene inserito un PIN personale direttamente sull'apparecchio, in modo da dimostrare la presenza fisica dell'utilizzatore.

Comunicazioni orali

Per le comunicazioni orali, bisogna ricordare periodicamente di non intrattenere conversazioni (di persona o al telefono) su materie riservate in luoghi dove si può essere ascoltati da persone non autorizzate e di non lasciare messaggi vocali con informazioni riservate.

Esempio 12.10.2. Molti, quando ricevono una telefonata e si trovano in luoghi pubblici, non segnalano all'interlocutore la situazione e non chiedono di rimandare la discussione o, mentre parlano al telefono di argomenti riservati, per esempio in treno, consultano documenti cartacei o il computer,

facilitando ulteriormente i vicini a capire l'argomento.

Alcuni controllano la sicurezza delle conversazioni impedendo l'ingresso di ogni strumento elettronico nelle sale riunioni per evitare di essere intercettati o registrati.

Memorie rimovibili

Della sicurezza delle memorie rimovibili come chiavi USB o altro, se ne è già parlato nel paragrafo 12.9.8.

Quando si inviano memorie rimovibili, incluse quelle utilizzate per i backup, oltre a stabilire quale corriere utilizzare e le regole di cifratura o di impostazione del controllo degli accessi con password, è necessario prestare le dovute attenzioni perché non si danneggino o vengano rubate durante il trasporto.

12.11 Acquisizione, sviluppo e manutenzione dei sistemi informatici

La sicurezza applicativa non va considerata solo nello sviluppo dei sistemi informatici, di cui si è già discusso nel paragrafo 12.9.3, ma anche nella loro acquisizione.

12.11.1 Acquisizione dei sistemi IT

I sistemi informatici acquisiti possono essere sistemi operativi, apparecchiature hardware, appliance, programmi di amministrazione e supporto, meccanismi di sicurezza, programmi per le attività degli utenti. Questi programmi sono denominati in molti modi diversi, tra cui: Free and open-source software o FOSS per il codice libero e open source, commercial off the shelf o COTS se si tratta di pacchetti commerciali, Software Of Unknown Provenance o SOUP nel contesto dei dispositivi medici [66].

L'acquisizione riguarda anche i software o librerie di codice sviluppati da altri, pratica comune e in molti contesti consigliata [2].

Quando si acquisisce un prodotto informatico si deve:

- stabilire preliminarmente i requisiti di sicurezza;
- analizzare i potenziali prodotti e verificare se li soddisfano;
- scegliere quello più appropriato;
- gestire adeguatamente i fornitori (vedere paragrafo 12.12).

Prima di essere installati in ambiente di produzione, i prodotti acquisiti devono essere oggetto di verifica e test, anche relativi alla sicurezza delle informazioni, come i penetration test (paragrafo 12.15.4). Vanno verificati in particolare: il corretto funzionamento dei sistemi di monitoraggio e di log, il controllo degli accessi al sistema e ai dati, il backup e la sincronizzazione con i siti di disaster recovery, le prestazioni, il corretto interfacciamento con gli altri sistemi. Un elenco più esaustivo dei requisiti da considerare per i prodotti si trova in Appendice E.

Tra i requisiti di sicurezza è importante:

verificare se è prevista l'assistenza e in che tempi;

verificare se è previsto l'aggiornamento del prodotto con patch quando sono rilevate delle vulnerabilità e quando è prevista la fine vita (end of life o EOL) e la successiva fine del supporto (end of support o EOS) del prodotto;

prevedere cosa fare nel caso in cui il fornitore cessi le attività (se sono disponibili fornitori alternativi, se è necessario mantenere le versioni obsolete del software, se è possibile migrare i dati in un altro software).

Anche se sono effettuate analisi preventive, è da ricordare che nel tempo possono essere individuate vulnerabilità anche molto gravi nei prodotti acquistati¹⁰⁶. È quindi sempre necessario prestare attenzione a forum e newsletter specializzati per avere notizie immediate e poter agire di conseguenza.

Può essere un parametro di valutazione la certificazione della sicurezza di prodotti e sistemi IT basata sulle norme ISO/IEC 15048, Common Criteria for Information Technology Security Evaluation. L'appendice D tratta di questo argomento e delle precauzioni da porre nei prodotti certificati.

12.11.2 Internet of things

I sistemi IoT si compongono di numerosi elementi:

il dispositivo vero e proprio, composto da sensori (un rilevatore di temperatura) o attuatori (un comando per alzare o abbassare le tapparelle) o ambedue (un

rilevatore di temperatura e il regolatore dell'aria condizionata);
il cloud, ossia il server centrale usato per collegarsi al dispositivo da Internet;
l'applicazione per dispositivi mobili (smartphone e tablet), che si interfaccia solitamente con il cloud;
dispositivi di gateway o di edge a cui si connettono più sensori e attuatori per migliorare le prestazioni o l'integrazione di più dispositivi.

Il cloud e le applicazioni vanno sviluppate seguendo le normali regole di sicurezza. Diverso è il caso dei dispositivi, visto che essi potrebbero essere posti in ambienti fisici non controllati (per esempio in ambienti polverosi o senza controlli degli accessi) e i loro malfunzionamenti potrebbero avere impatti sulla sicurezza fisica delle persone o delle cose.

Per questo motivo vanno considerate misure di sicurezza per:

evitare accessi fisici non autorizzati;
assicurare il corretto funzionamento del dispositivo, seppure limitato, anche in caso di assenza di energia elettrica o di connessione a Internet.

Purtroppo i dispositivi sono spesso sviluppati senza l'adeguata attenzione alla sicurezza informatica e questo è stato sfruttato per numerosi attacchi (in particolare l'uso di password di default banali e non modificabili per l'accesso al dispositivo o firmware non aggiornato).

Negli ultimi anni sono numerose le pubblicazioni che trattano di sicurezza dell'IoT [38, 39, 46] e se ne raccomanda la consultazione a coloro che

sviluppano tali sistemi.

12.11.3 Intelligenza artificiale

I sistemi con funzionalità di intelligenza artificiale devono essere sviluppati considerandole le peculiari necessità di sicurezza. In questo libro questo argomento non è approfondito, ma sono disponibili numerose pubblicazioni in merito [37, 21].

12.12 Gestione dei fornitori

Il ricorso a fornitori è una forma di condivisione del rischio: una parte di esso resta sempre al cliente perché dovrà sostenere parte dei costi e affrontare i danni all'immagine conseguenti a un incidente.

È possibile distinguere tre tipi di fornitori con impatto sulla sicurezza delle informazioni:

fornitori di prodotti hardware e software e della relativa assistenza (esclusa quella che prevede l'accesso diretto ai sistemi informatici e alle informazioni dell'organizzazione);

fornitori di servizi non informatici, come quelli di vigilanza e delle pulizie;

fornitori di servizi informatici, inclusi quelli che conducono i sistemi informatici, alcuni consulenti, gli operatori di telecomunicazioni e i produttori di sistemi informatici che forniscono assistenza e possono accedere alle informazioni.

I fornitori del primo tipo e alcuni del secondo non accedono alle informazioni ma svolgono attività necessarie alla sicurezza delle informazioni.

Clienti e fornitori potrebbero far parte della medesima organizzazione (per esempio, due centri di costo distinti) o essere società appartenenti allo stesso gruppo di imprese: sono molti i casi in cui la casa madre fornisce servizi alle società del gruppo, agendo quindi come fornitore. Quando cliente e fornitore sono organizzazioni distinte, i requisiti di fornitura devono essere scritti in un contratto; negli altri casi, si stipula un contratto interno o un accordo.

Per tutte le forniture occorre stabilire un processo composto dalle seguenti fasi:

stabilire i requisiti di fornitura e del fornitore, in linea con quelli di sicurezza dell'organizzazione e dei suoi clienti;

verificare se i fornitori possono garantire i requisiti stabiliti, anche sulla base di esperienze pregresse o di verifiche preliminari;

stabilire se accettare che il fornitore non rispetti alcuni requisiti o ne attui di alternativi;

formalizzare un accordo o un contratto con il fornitore;

controllare il rispetto di quanto concordato, con verifiche e monitoraggi, fino alla scadenza dell'accordo o del contratto.

Sembrano passi dettati dalla logica e dal buon senso. Ma spesso si verificano i seguenti casi:

i requisiti non sono completamente stabiliti dall'organizzazione, che tende ad accettare le offerte dei fornitori senza verificare se sono adeguate alle proprie esigenze (dal 2018, con l'entrata in vigore del GDPR, si assiste al caso inverso, ossia a clienti che vogliono dettare ai fornitori i propri requisiti, spesso senza considerarne l'applicabilità);

non sono mai condotte verifiche in merito al rispetto di quanto concordato con il fornitore, se non quando si verificano incidenti.

12.12.1 Gli accordi e i contratti con i fornitori

Gli accordi e i contratti con i fornitori devono basarsi su requisiti preventivamente stabiliti dall'organizzazione.

Hanno una durata variabile: annuale o pluriennale fino a oltre dieci anni. È importante prestare attenzione agli accordi e ai contratti stipulati per un breve periodo e poi via via rinnovati con una breve lettera: i requisiti, nel tempo, perdono di validità perché basati su normative decadute o perché nuove esigenze non sono formalizzate.

Ogni contratto è diverso a seconda del tipo di fornitore coinvolto. Per esempio, non ha senso prevedere la clausola sul diritto di audit a uno studio legale perché i principi professionali lo escludono.

12.12.1.1 Clausole generali

Si potrebbero, considerando le tre tipologie di fornitori sopra indicate, prevedere tre casistiche di accordi o contratti, per i quali sono forniti dei requisiti in appendice F.

In generale, gli accordi e i contratti dovrebbero avere i seguenti elementi:

accordo di riservatezza, tale per cui il cliente e il fornitore si impegnano a non divulgare o comunicare ad altri informazioni riservate dell'uno e dell'altro anche dopo la conclusione del rapporto e a promuovere il medesimo impegno,

mediante accordi o contratti scritti, col proprio personale, gli altri fornitori e subfornitori;

le misure di sicurezza da rispettare (in appendice E si possono trovare spunti per i prodotti tecnologici);

i criteri di continuità operativa e il tempo massimo di indisponibilità dei servizi offerti (paragrafo 12.14);

le modalità con cui le attività del fornitore saranno monitorate o verificate e i prodotti valutati;

il diritto di audit del cliente, inclusi i suoi limiti, per esempio indicando il massimo numero di audit che potrà condurre, i tempi di preavviso, i casi in cui potrà condurre audit straordinari o a sorpresa; vanno inoltre specificate le procedure di audit, incluse le conseguenze delle non conformità e se queste potranno portare alla conclusione anticipata del contratto;

per quale carico di lavoro (per esempio: numero di utenti, di transazioni o di richieste di assistenza) sono garantite le prestazioni concordate;

i canali di comunicazione da utilizzare (paragrafo 12.10.4), anche per segnalare vulnerabilità, eventi e incidenti (paragrafo 12.13);

le modalità con cui inoltrare e gestire i reclami dal cliente al fornitore;

i reciproci obblighi per il rispetto della normativa vigente, in particolare quella sulla privacy, e i criteri da seguire in caso di modifiche alla stessa (paragrafo 12.15.1);

le modalità con cui devono essere gestiti i sub-fornitori (come minimo, è necessario stabilire come estendere gli obblighi di riservatezza e quelli relativi al rispetto della normativa vigente; in alcuni casi, il cliente decide preventivamente quali sub-fornitori autorizzare);

il processo da seguire per modificare o aggiornare il contratto e i requisiti tecnici;

i casi e le modalità con cui è possibile chiudere il contratto prima della sua naturale scadenza (per esempio, per gravi inadempienze di una delle due parti);

le modalità da seguire al momento della chiusura del contratto (passaggio di consegne, mantenimento degli obblighi di riservatezza, distruzione delle informazioni o loro mantenimento da parte del fornitore).

Per alcuni servizi non informatici sono da prevedere clausole contrattuali specifiche, come è il caso dei fornitori di servizi di conservazione della documentazione in formato non digitale (gli ospedali affidano spesso a fornitori esterni la gestione delle cartelle cliniche in formato non digitale).

12.12.1.2 Clausole specifiche per i servizi informatici

Nel caso in cui il fornitore offre servizi informatici, deve:

garantirsi rispetto a eventuali azioni dei clienti, specificando nel contratto che gli utenti devono utilizzare i servizi informatici secondo quanto previsto, non attuare azioni illecite, non cercare di manometterli;

chiarire i casi in cui il cliente è responsabile degli errori commessi o dell'errata configurazione dei propri strumenti;

in conformità alla normativa vigente, avvisare i clienti delle azioni che il fornitore potrebbe compiere in caso riscontrasse l'uso illecito e a scopo delittuoso dei servizi informatici offerti (per esempio, se gli utenti si scambiano file illegali);

ricordare nei manuali o nel contratto alcune misure di sicurezza di base che il cliente deve rispettare; tra queste: divieto di condividere un'utenza tra più persone e l'obbligo di mantenere segrete le password;

dichiarare che mai richiederà agli utenti informazioni personali, credenziali (neanche user-id) e non invierà link diretti a siti web o risorse su Internet.

12.12.2 Selezione dei fornitori

Prima di stabilire un rapporto con qualsiasi fornitore, devono esserne analizzati i rischi per potere stabilire quali controlli preventivi effettuare.

Si può evitare di svolgere un'analisi del rischio per ogni singolo fornitore e prevederne solo per tipologia di fornitura (per esempio se è previsto che i fornitori accedano alle informazioni dell'organizzazione o se si tratta della fornitura di prodotti usati per trattare le informazioni). Per esempio possono essere sufficienti analisi di mercato, le raccomandazioni di altre organizzazioni o il mantenimento di certificazioni di prodotto o di sistema di gestione. Nei casi più critici sono opportuni audit molto approfonditi presso il potenziale fornitore, includendo l'analisi delle condizioni finanziarie e organizzative (in questo caso, si parla anche di due diligence), e stabilire per contratto la periodicità di tali audit.

Tra le questioni da affrontare in fase di selezione dei fornitori, per assicurarne la riservatezza, ci sono sicuramente le modalità per trasferire le informazioni in fase di avvio delle attività e nelle fasi successive di normale amministrazione.

Relativamente alla chiusura della relazione, aspetti da considerare sin dall'inizio:

i metodi previsti per la cancellazione delle informazioni (vedere 12.9.9);

come saranno trasferiti i dati in modo anche da assicurarne la portabilità, ossia riceverli in un formato tale da poter essere riutilizzati con altri sistemi, interni o di altro fornitore.

Alcuni seguono la pratica di far compilare ai fornitori e potenziali fornitori questionari relativi alle misure adottate per la sicurezza delle informazioni e la privacy. Questi questionari non rappresentano alcuna valutazione del rischio né permettono di dimostrare il reale controllo dei fornitori, anche perché spesso sono accettate risposte generiche. L'approccio corretto prevede che sia il cliente a stabilire le misure di sicurezza e richiedere ai fornitori di applicarle, non chiedere ai fornitori quali misure attuano per poi decidere quali chiedere. Nel caso in cui un fornitore non possa applicare le misure come richiesto, può proporre alternative ed è compito del cliente valutare se sono equivalenti o comunque accettabili.

Un aspetto da valutare riguarda la continuità della fornitura, anche nel caso in cui un fornitore sia vittima di un incidente, chiuda o dismetta parte delle attività. In questi casi si deve verificare la presenza di almeno una delle seguenti alternative:

il fornitore ha un piano di continuità (paragrafo 12.14);

il cliente deve pianificare le opportune strategie come, per esempio:

cambiare fornitore con uno con un piano di continuità;

usarne più di uno contemporaneamente in modo di passare il carico di lavoro a uno quando l'altro non è disponibile;

assicurare la presenza di competenze del personale interno e un numero sufficiente di persone per prendere direttamente in carico le attività del fornitore;

monitorare la disponibilità di altri fornitori per una veloce sostituzione in caso di necessità.

L'uso di fornitori distinti e le valutazioni sulla portabilità dei dati permettono

anche di evitare i rischi relativi al vendor lock-in.

12.12.3 Monitoraggio dei fornitori

Durante l'erogazione dei servizi il cliente può effettuare controlli diretti attraverso audit e il monitoraggio tecnologico e controlli indiretti chiedendo resoconti periodici, per esempio, sulla disponibilità del servizio, sugli incidenti e sui cambiamenti effettuati.

In alcuni casi, quando è usato un sistema di ticketing per le comunicazioni tra cliente e fornitore, il cliente può ricavare autonomamente dei report per analizzare le prestazioni del fornitore.

Da pianificare incontri periodici tra le parti per riesaminare le prestazioni, le eventuali criticità intervenute o previste e modifiche ai servizi e ai processi.

Quando si acquista un prodotto informatico appositamente sviluppato, il cliente potrebbe prevedere verifiche intermedie di quanto prodotto e, al termine dei lavori, eseguire delle code review (paragrafo 12.15.4).

I risultati dei riesami e monitoraggi possono richiedere un cambiamento del contratto e possono essere usati in occasione del suo rinnovo (o usati quando un contratto simile è sottoscritto con un altro fornitore). Per esempio durante la relazione potrebbero esserne emersi elementi non considerati nel precedente contratto e che potrebbero essere inclusi nel successivo. Ovviamente i rinnovi e le modifiche devono assicurare il mantenimento dei livelli di sicurezza.

12.12.4 Cloud computing e fornitori

Negli ultimi anni si è parlato molto del cloud e delle misure di sicurezza da prevedere quando si utilizzano servizi erogati con questa tecnologia; ciò è dovuto anche all'interessamento eccessivo dell'autorità italiana garante per la protezione dei dati personali.

In questa sede non è approfondito il tema perché i servizi offerti via cloud sono uguali a molti servizi erogati con altre tecnologie; l'uso delle tecnologie cloud li ha resi più economici e diffusi anche presso il grande pubblico; per il resto, nulla cambia nella gestione dei fornitori.

Per esempio, oggi si parla del trasferimento di dati attraverso servizi cloud, ma già da anni si usa l'email, peraltro molto insicura, gestita da un fornitore esterno, che potrebbe usare o meno tecnologie cloud.

Purtroppo, i fornitori informatici sono spesso gestiti senza attenzione per la sicurezza: sono loro assegnati diritti di accesso troppo estesi o utenze condivise, non vengono verificati i livelli di servizio concordati, non si hanno garanzie sulla continuità del servizio e così via. Quando si parla di servizi cloud, però, il livello di attenzione e di percezione del rischio improvvisamente aumenta perché è diffuso il falso mito per cui i servizi cloud usano per definizione dei server in luoghi e Paesi indefinibili, ma questa non è una caratteristica dei servizi cloud [97] perché molti di essi sono erogati da siti facilmente identificabili ed esplicitabili sui contratti. Anzi, alcuni servizi “tradizionali”, come quelli di assistenza tecnica, sono spesso condotti da più persone ubicate in diversi Paesi del mondo.

Dall'altra parte, alcuni comprano servizi cloud e non considerano che vanno configurati in modo appropriato. Molte organizzazioni addirittura riducono

ulteriormente i costi mandando via persone competenti perché, erroneamente, pensano che i fornitori di servizi cloud si occupano di tutto. Questo non è vero, come dimostrano molti casi¹⁰⁷.

Alcune pubblicazioni sulla sicurezza dei servizi cloud [18, 20, 96] sono fatte molto bene e dovrebbero essere considerate come linee guida da applicare a tutti i tipi di fornitori di servizi informatici.

Quando si decide di usare servizi cloud, alcuni elementi particolarmente critici, tra quelli già indicati nei paragrafi precedenti, sono:

- i requisiti di sicurezza stabiliti prima di selezionare il fornitore;
- le modalità per chiudere il servizio e come è assicurata la portabilità dei dati;
- il rispetto della normativa privacy;
- la locazione dei server;
- le modalità per raccogliere prove legali dai sistemi;
- la responsabilità dei backup e del disaster recovery e gli strumenti messi a disposizione dei clienti per questo scopo;
- la gestione dei cambiamenti (ossia se e come sono previsti preavvisi per alcuni cambiamenti significativi).

12.12.5 L'acquisizione di prodotti informatici e lo sviluppo affidato all'esterno

L'acquisizione di prodotti informatici e lo sviluppo affidato all'esterno sono due

processi da controllare con attenzione perché ogni sistema informatico può introdurre vulnerabilità perché progettati, sviluppati o verificati in modo non adeguato.

Alcuni elementi specifici da considerare in fase di acquisizione prodotti informatici, oltre a quanto già indicato al paragrafo 12.11:

se il software acquisito è ancora oggetto di manutenzione, quando ne è prevista la fine (EOL, end of life) e quando è prevista la fine del supporto (EOS, end of supporto); questa verifica è da ripetere periodicamente;

il tipo di licenza, in particolare in merito a chi ha la proprietà del software e se l'utilizzatore può apportare modifiche e quali;

possibili certificazioni del software.

Per quanto riguarda lo sviluppo affidato all'esterno, oltre a quanto sopra indicato, vanno stabiliti:

le modalità con cui il fornitore recepisce i requisiti di sicurezza (del software e dell'ambiente di sviluppo) del cliente;

quali strumenti di sviluppo e di ticketing usare, per esempio se sono quelli del cliente o del fornitore;

quali database sono necessari al fornitore per condurre i test richiesti dal cliente;

i test e le verifiche, anche di sicurezza, e chi li deve svolgere; per esempio può essere responsabilità del fornitore svolgere i test, ma deve mettere a disposizione del cliente i rapporti;

il tracciamento dell'origine dei diversi componenti del software e dell'hardware,

in modo da poterne assicurare l'aggiornamento.

Da ricordare che un'organizzazione può essere attaccata proprio attraverso la sua filiera di fornitura ossia i suoi fornitori di software¹⁰⁸ e anche hardware¹⁰⁹. Questi attacchi hanno sollevato molti allarmi¹¹⁰ e sono oggi tra quelli più pericolosi.

Per prevenire tali attacchi, noti come attacchi alla filiera di fornitura (supply chain attacks), non è più solo necessario assicurarsi che il software acquisito abbia le necessarie funzioni di sicurezza e che il fornitore abbia seguito buone pratiche di sviluppo sicuro, ma anche che l'ambiente di sviluppo sia controllato in modo da mitigare la probabilità di intrusione e di inserimento di codice dannoso nel software.

12.12.6 Le assicurazioni

Come già specificato nel paragrafo 9.1.4, la sottoscrizione di una polizza assicurativa è una forma di condivisione del rischio.

È necessario prestare attenzione alle polizze sottoscritte, in quanto il mercato delle assicurazioni in materia di sicurezza informatica è ancora poco maturo¹¹¹. Bisogna aggiungere che, con il passare degli anni, le polizze proposte sono sempre più complete e precise, con anche, per esempio, la copertura delle responsabilità civili, delle spese per il supporto tecnico e per le indagini.

Gli assicuratori, al momento, richiedono alle organizzazioni di concentrarsi soprattutto sulle procedure organizzative e non su quelle tecnologiche. Anzi, spesso richiedono procedure di base e non offrono incentivi reali per investire in sicurezza. Da notare poi che le polizze coprono prevalentemente i costi di

risposta agli incidenti (spesso mettendo a disposizione servizi offerti da società specializzate), ma si tratta di misure post-incidente, meno utili di quelle di mitigazione preventiva (questo anche perché i costi del recupero sono più facili da quantificare)¹¹².

12.13 Gestione degli incidenti

Nel paragrafo 6.2 sono date le definizioni di evento e incidente relativo alla sicurezza delle informazioni. Vanno distinti i due concetti, come illustrato dai tre esempi seguenti.

Esempio 12.13.1. Uno sconosciuto che si avvicina all'ingresso del CED rappresenta un evento relativo alla sicurezza delle informazioni. Potrebbe essere un incidente relativo alla sicurezza delle informazioni se tenta di accedervi per danneggiare i sistemi informatici dell'organizzazione.

Se lo sconosciuto è invece un visitatore in cerca del bagno, l'evento non ha alcuna “probabilità significativa di compromettere le attività e di minacciare la sicurezza delle informazioni” e pertanto non deve essere classificato come incidente, ma analizzato, per esempio, per stabilire se rappresenta una vulnerabilità.

Esempio 12.13.2. Un dipendente cerca di superare i tornelli di ingresso con un badge non valido.

Se si verifica che ha usato per sbaglio la carta fedeltà del supermercato al posto del badge, allora l'evento non deve essere classificato come incidente. Per contro, se si dovesse verificare che il dipendente è stato recentemente licenziato, va classificato come incidente pur in assenza di danni.

Esempio 12.13.3. A fronte di un aumento inatteso di email ricevute, si potrebbe registrare un incidente se causato da un attacco di mass mailing bombing. Viceversa, è da registrare un evento se dovuto a una consegna di numerosi documenti contemporaneamente da parte di un fornitore.

Nel secondo caso si avrebbe un incidente se l'aumento delle email, anche se non proveniente da malintenzionati, avesse causato un rallentamento inaccettabile del traffico della rete informatica.

In questo capitolo si affrontano anche le vulnerabilità tecniche che, se non trattate, possono causare incidenti.

12.13.1 Ruoli e procedure

Le attività da svolgere nella gestione degli incidenti devono essere documentate, in modo da chiarirle a tutte le parti interessate. In particolare la documentazione deve specificare il processo, i livelli di classificazione degli eventi e le responsabilità.

Tra le responsabilità, come si vedrà nei paragrafi successivi, va indicato chi riceve le segnalazioni di potenziali incidenti, chi deve trattare gli eventi da un punto di vista tecnico e chi da un punto di vista relazionale.

12.13.2 Processo di gestione degli incidenti

È importante stabilire un processo ben strutturato di gestione degli incidenti affinché siano rilevati e trattati efficientemente ed efficacemente, con eventuali effetti negativi ridotti al minimo, e attuato il piano di gestione della crisi se necessario (paragrafo 12.13.5), le vulnerabilità valutate e trattate adeguatamente e rapidamente, le conoscenze condivise per prevenire futuri incidenti.

In figura 12.13.1 è presentato uno schema di processo di gestione degli incidenti.

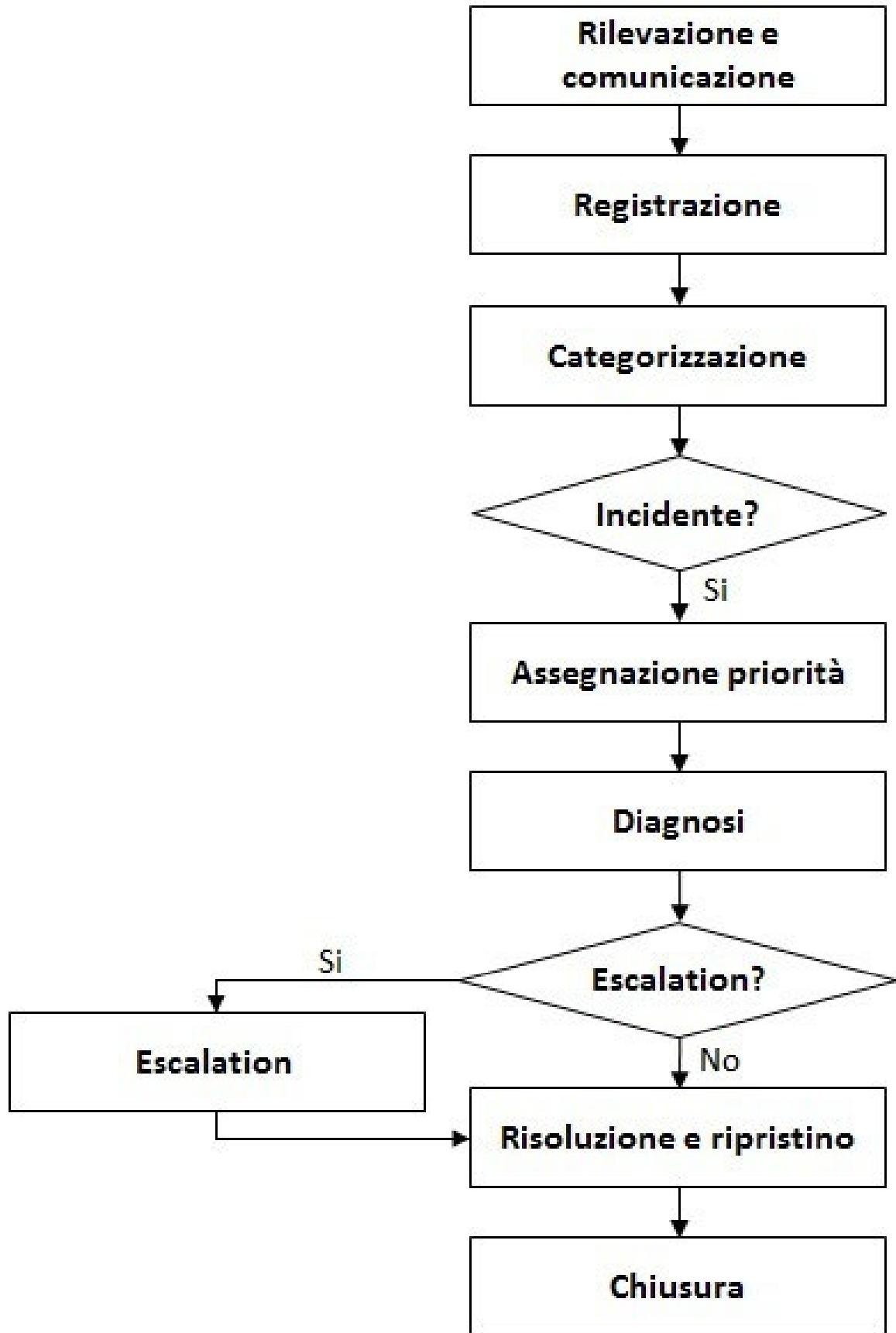


Figura 12.13.1:

Il processo di gestione degli incidenti

12.13.2.1 Rilevazione e comunicazione

La rilevazione riguarda eventi, incidenti e vulnerabilità (anche per il software sviluppato o acquisito e usato da utenti interno ed esterni). Può essere effettuata da: sistemi automatici di monitoraggio, analisi o verifiche manuali da parte degli operatori, segnalazioni da parte del personale, dei clienti, dei fornitori o dei partner, mezzi di informazione.

È importante stabilire a chi segnalare un incidente o vulnerabilità, affinché venga convenientemente trattato. Per gli utenti, si consiglia sempre di istituire un unico punto di contatto (SPOC o single point of contact), con un unico numero di telefono e indirizzo email, a evitare confusioni.

Quando si tratta della gestione di servizi informatici, questo punto di contatto viene chiamato service desk e si occupa di tutte le richieste e segnalazioni degli utenti. I termini contact centre e call centre sono usati come sinonimo di service desk, ma più caratteristici di attività commerciali.

12.13.2.2 Registrazione

Gli eventi devono essere registrati, in modo che sia noto chi li ha segnalati, chi li sta trattando e per conservarne una storia, utile se un caso simile si dovesse ripetere e, se il trattamento richiede molto tempo, per monitorarlo (per esempio, potrebbe essere necessario acquistare apparecchiature non prontamente disponibili sul mercato).

Esistono molti tipi di sistemi di registrazione degli eventi detti sistemi di ticketing. La loro diffusione è tale che alcuni usano il termine “ticket” al posto di “incidente”.

L’evento va registrato anche perché, se si tratta di un incidente con caratteristiche specificate dalla normativa vigente, va notificato alle pertinenti autorità (paragrafo 12.13.2.7).

12.13.2.3 Categorizzazione

Il passo successivo di categorizzazione consiste in poche analisi, con l’obiettivo di comprendere:

se la segnalazione riguarda effettivamente un incidente o una vulnerabilità;

l’impatto attuale o potenziale dell’incidente o della vulnerabilità; l’impatto potrebbe essere più elevato se l’incidente riguardasse le informazioni dei clienti;

quale funzione tecnica è la più adeguata a trattare l’incidente o la vulnerabilità (in alcuni casi può essere il service desk, in altri casi una funzione specializzata in una tecnologia).

12.13.2.4 Assegnazione della priorità

La categorizzazione consente di stabilire la priorità di trattamento: incidenti con impatti elevati (per esempio, tentativi di intrusione o interruzioni di servizi utilizzati da molti utenti) hanno la priorità più elevata. Nell’assegnazione della priorità è anche necessario considerare altri parametri, come eventuali scadenze da rispettare o la possibilità che gli impatti dell’incidente possano aumentare rapidamente, allo stesso modo di un principio di incendio.

È molto importante stabilire i criteri di assegnazione delle priorità per evitare incomprensioni tra chi tratta l’evento, chi l’ha segnalato e quanti ne subiscono le conseguenze. Si può usare una semplice scala di 3 valori (“alto”, “medio” e “basso” oppure “emergenza”, “critico”, “allarme”).

12.13.2.5 Diagnosi

Secondo la priorità assegnata, la funzione tecnica coinvolta dal service desk procede a una diagnosi più approfondita, utilizzando strumenti di diagnosi manuali o automatizzati ed eventualmente coinvolgendo la persona che ha fatto la segnalazione. Le prime cose da individuare sono:

l’ambito di origine dell’incidente, in modo da coinvolgere gli opportuni esperti; se incidenti simili si siano già verificati in precedenza, in modo da prendere in considerazione la medesima soluzione.

12.13.2.6 Escalation

Se la funzione tecnica che ha svolto la diagnosi non può affrontare da sola l'incidente, deve coinvolgere ulteriori strutture, ossia effettuare una escalation. Se coinvolti i fornitori, può essere utilizzato il termine dispatching.

Nell'escalation di tipo tecnico l'operatore coinvolge tecnici interni o fornitori affinché risolvano l'incidente. Questi potrebbero a loro volta scalare l'incidente, ossia coinvolgere altri tecnici.

Un'altra escalation è di tipo gerarchico e non esclude quella di tipo tecnico. Se gli impatti possono avere conseguenze sull'immagine dell'organizzazione, è opportuno coinvolgere strutture addette alla relazione con il pubblico o con i clienti, secondo quanto specificato nel piano di gestione delle crisi (paragrafo 12.13.5).

Per alcuni incidenti, normalmente caratterizzati da tentativi di attacco o da potenziali impatti molto elevati, tra le strutture da contattare, se presente, vi è l'ISIRT (o CERT, dedicato però ai soli incidenti in ambito informatico) composto da specialisti nella gestione di questo tipo di eventi.

Nel caso poi di incidenti che possono bloccare le attività per lungo tempo, potrebbe essere necessario attivare il piano di continuità operativa (o business continuity plan, BCP), descritto nel paragrafo 12.14.

Tutte queste escalation devono essere regolamentate: il service desk inizialmente coinvolge il proprio responsabile che a sua volta, dopo aver valutato gli impatti e gli effetti previsti dell'evento, potrà contattare i livelli gerarchici superiori o il business continuity manager o altre funzioni specificate dalle procedure dell'organizzazione.

12.13.2.7 Notifica

I clienti andrebbero informati il prima possibile, o con un minimo ritardo, in merito agli incidenti che hanno impatti sulle loro informazioni e alle azioni prese per affrontarli.

In alcuni casi la normativa impone di notificare l'incidente a determinate autorità. Tra di esse vi è la normativa sulla privacy, che tratta in particolare di violazioni dei dati personali (data breach) con impatti sui diritti e le libertà delle persone fisiche, quella che riguarda i fornitori di servizi essenziali e i fornitori di servizi digitali (D. Lgs. 65 del 2018) e quella relativa al “perimetro di sicurezza nazionale cibernetica” (DL 105 del 2009). La normativa sulla privacy richiede, in alcune circostanze, di notificare l'incidente anche alle persone interessate.

Deve essere quindi stabilito un processo indicando quando deve essere avviato e chi ha l'autorità per inviare le notifiche richieste.

Un rapporto di incidente dovrebbe riportare:

la data e l'ora dell'incidente;

una descrizione dell'incidente e dei suoi impatti;

le azioni prese per affrontare l'incidente e quando questo è stato chiuso;

le ulteriori attività pianificate e realizzate per ridurre gli impatti dell'incidente e prevenirne il ripetersi.

In alcuni casi è previsto che sia inviato un rapporto, anche se incompleto (per esempio perché l'incidente non è stato ancora chiuso o le ulteriori attività non sono state pianificate), il prima possibile ai clienti e alle autorità. Gli aggiornamenti del rapporto potranno essere inviati con comunicazioni successive.

12.13.2.8 Risoluzione e ripristino

A questo punto, le persone più adeguate a trattare l'incidente sono state coinvolte e provvedono alla sua risoluzione e a documentarla sul sistema di ticketing.

In alcuni casi, con i sistemi informatici sotto attacco, si potrebbe decidere di monitorare l'attività dell'intruso per raccogliere prove da usare in procedimenti legali. Per gestire correttamente questa opzione bisogna essere molto competenti ed essere sempre affiancati da un esperto legale (paragrafo 12.13.6).

Per risolvere l'incidente devono essere seguite le procedure di gestione dei cambiamenti informatici (paragrafo 12.9.3) con i cambiamenti in emergenza da attuare in caso di incidente o di presenza di vulnerabilità gravi.

12.13.2.9 Chiusura

Prima di chiudere definitivamente un incidente è opportuno verificare dopo qualche tempo l'efficacia della soluzione. Se l'incidente è stato segnalato da una o più persone, queste devono essere contattate per verificare se anche dal loro punto di vista l'incidente è stato risolto.

12.13.3 Controllo delle vulnerabilità

Nessun sistema, informatico e non informatico, è immune da vulnerabilità. Vulnerabilità possono essere identificate nei sistemi informatici (sviluppati internamente o acquisiti da entità esterne), nell'ambito della sicurezza fisica, nelle procedure e nei processi dell'organizzazione.

Per tutti i sistemi devono essere attivi dei canali di comunicazione con i loro sviluppatori e produttori (interni o esterni, inclusi quelli dei programmi software free): questi devono garantire notizie tempestive in merito alle vulnerabilità riscontrate nei loro prodotti o servizi e alle soluzioni disponibili; viceversa, ciascun utilizzatore deve poter segnalare al produttore eventuali vulnerabilità o difettosità riscontrate nel prodotto fornito o nel servizio offerto e ricevere una risposta.

Ogni segnalazione di vulnerabilità, come accennato in precedenza, va trattata come segnalazione di incidente. Il produttore deve registrare chi effettua le segnalazioni, in modo da poterlo contattare per chiedergli, se necessario, ulteriori dettagli.

Gli esempi che seguono illustrano alcuni casi realmente accaduti, non tutti relativi a vulnerabilità di tipo informatico.

Esempio 12.13.4. Nel 2013, in un CED della Pubblica Amministrazione, a seguito di un'interruzione della rete elettrica, le UPS, che avrebbero dovuto garantire l'alimentazione delle apparecchiature, non funzionarono e le apparecchiature si spensero.

Questo comportamento anomalo fu comunicato al produttore delle UPS che avviò uno studio per comprenderne l'origine e sviluppare una soluzione. Nel corso delle analisi, produttore e utilizzatore si scambiarono diverse notizie in merito alle configurazioni delle UPS e della rete elettrica del CED.

Questo è un esempio di vulnerabilità, a cui è seguito un incidente, di strumenti non informatici.

Esempio 12.13.5. A metà 2013, la Microsoft pubblicò la versione 8.1 del suo sistema operativo Windows. Alcuni programmi software per Windows presentarono comportamenti imprevisti con la nuova versione.

Gli utenti contattarono i produttori di questi programmi, molti free, e in breve tempo ne fu pubblicato un aggiornamento.

Questo è un esempio di vulnerabilità, a cui è seguito un incidente, di un prodotto informatico.

Esempio 12.13.6. Un dipendente italiano di una filiale locale di una multinazionale riscontrò delle mancanze nell'informativa del trattamento dei dati personali dei dipendenti (paragrafo 12.15.1.9) e prontamente avvisato l'ufficio personale che corresse e pubblicò l'informativa.

Questo è un esempio di vulnerabilità di un processo.

Nei paragrafi successivi si discute delle vulnerabilità dei prodotti informatici, ma alcuni principi possono essere estesi agli altri ambiti.

12.13.3.1 Il patching

Quando la vulnerabilità è dovuta a un errore software, il produttore potrebbe risolverla mettendo a disposizione aggiornamenti correttivi, detti fix o patch. Se non riesce a sviluppare tali aggiornamenti in tempi rapidi, il produttore segnala dei workaround, ossia strade alternative per eliminare o contenere la vulnerabilità¹¹³. Il produttore potrebbe segnalare dei workaround utilizzabili da coloro che non intendono installare le patch pubblicate per particolari caratteristiche dei loro sistemi informatici.

I software più diffusi spesso prevedono come opzione predefinita l'installazione automatica degli aggiornamenti messi a disposizione dal produttore ed è bene lasciarla se si tratta del proprio PC personale. Per i sistemi di una rete più complessa, agli aggiornamenti si applica il processo di gestione dei cambiamenti (paragrafo 12.9.3) e in particolare l'analisi degli aggiornamenti disponibili, i test prima dell'installazione nell'ambiente di produzione e la previsione del rollback in caso di malfunzionamenti dovuti all'aggiornamento.

Per essere aggiornati sulle vulnerabilità dei prodotti in commercio, è utile non limitarsi all'analisi dei bollettini pubblicati dai produttori software, ma abbonarsi anche a newsletter gestite da canali indipendenti¹¹⁴, perché non di rado più complete e tempestive e con un'esaustiva descrizione dei workaround: alcuni attacchi, detti zero-day, sfruttano vulnerabilità appena scoperte, segnalate dai bollettini indipendenti e non da quelli dei produttori dei software coinvolti.

È necessario verificare quando è prevista la fine vita (end of life o EOL) e la successiva fine del supporto (end of support o EOS) di ogni prodotto.

12.13.3.2 Tempestività del patching

La velocità di esecuzione del patching dei prodotti software è argomento dibattuto. Gli idealisti dicono di installare le patch appena sono pubblicate, anche grazie agli aggiornamenti automatici; i pragmatici vedono ogni cambiamento ai sistemi informatici come un rischio perché alcune patch possono essere difettose e, prima di autorizzare il cambiamento, verificano se sono applicabili e necessarie ai sistemi gestiti; altri ancora non installano le patch sui sistemi più critici e, come misure compensative, li collegano a una rete ben protetta da firewall e non li rendono disponibili da Internet.

In alcuni casi, l'atteggiamento pragmatico porta a sottovalutare il problema, come dimostrano i danni provocati da virus che hanno sfruttato vulnerabilità note da tempo¹¹⁵.

Un compromesso consiste nell'installare le patch appena possibile sui sistemi esposti su Internet e intervenire con minore tempestività sugli altri. Questo compromesso deve essere accompagnato da un'attenta progettazione dei sistemi: su quelli esposti su Internet sono installati programmi il più possibile indipendenti tra loro (in modo che un cambiamento a uno di essi non abbia impatto sugli altri) e, per quanto possibile, poco critici (per esempio, i soli moduli di presentazione), lasciando gli altri moduli in ambienti e reti più difficili da raggiungere da parte di malintenzionati.

12.13.3.3 Il mercato delle vulnerabilità

Alcuni malintenzionati ricercano vulnerabilità nei sistemi o prodotti informatici non per sfruttarle, ma per diffonderne la notizia ed esibire le proprie capacità. Le dichiarazioni sono anche accompagnate da frasi come: “Ho cercato di contattare il responsabile del sistema, ma non ho trovato alcuna indicazione sul web”. Il comportamento di certi esibizionisti è senz’altro censurabile, ma le organizzazioni devono stabilire canali di comunicazione per ricevere segnalazioni di vulnerabilità a evitare danni all’immagine e raccogliere quelle originate da persone non malintenzionate.

In questi anni il fenomeno di ricerca delle vulnerabilità ha acquistato una dimensione ancora più inquietante: chi trova una vulnerabilità non la comunica, ma la mette in vendita per chi la volesse usare per accedere abusivamente a sistemi informatici e fare attività di spionaggio [31].

12.13.4 Gestione dei problemi

Nell’ambito dell’informatica, il termine problema, forse per analogia con l’espressione problem solving, è usato per indicare la causa di uno o più incidenti. In altri ambiti si utilizza l’espressione root cause e si dicono azioni correttive o preventive le attività per risolverla (paragrafo 15.10).

Un’organizzazione deve attivare un processo di gestione dei problemi per prevenire il verificarsi o il ripetersi di incidenti. Infatti, normalmente, quando si chiude un incidente, si usa un workaround, ossia una veloce soluzione temporanea, per poi, con maggiore calma, cercare la causa ultima dell’incidente e risolverla in maniera definitiva.

Esempio 12.13.7. L'esaurimento del toner a una stampante può essere un incidente perché impedisce agli utenti di utilizzarla.

Il workaround consiste nel sostituire immediatamente il toner.

Per evitare il ripetersi dell'incidente, si potrebbe monitorare in modo automatico il livello del toner, in modo da ricevere per tempo un allarme quando da sostituire.

Come si vede da questo esempio, l'incidente non ha necessariamente cause tecniche molto complicate. In altri casi, si potrebbero individuare cause tecniche o organizzative molto complesse da trattare.

Esempio 12.13.8. A seguito di un'intrusione nei sistemi informatici, si potrebbe individuare come causa il mancato patching di qualche apparecchiatura.

Però questa non è la causa ultima dell'incidente. Questa potrebbe essere di tipo organizzativo, ossia la mancanza di persone con le competenze adeguate o la non corretta definizione del processo di patching.

Individuare le cause ultime di un incidente o di un potenziale incidente non è compito semplice e sono state proposte tecniche per orientare l'analisi per non renderla dispersiva. Tra queste tecniche si ricordano il brainstorming, l'uso di diagrammi causa-effetto o di Ishikawa, la ricerca dei 5 perché.

Per stabilire quali incidenti analizzare per identificarne e trattarne le cause, si consiglia di partire da quelli più frequenti (analisi di Pareto).

Non sempre conviene attivare un processo di ricerca delle cause di un incidente: potrebbe essere meno oneroso affrontarlo ogni volta che si presenta. Purtroppo questa è spesso l'unica opzione seguita, anche quando la ripetitività del medesimo incidente suggerisce un altro approccio.

Si può verificare il caso per cui la causa di un incidente è nota, ma la soluzione troppo onerosa o troppo rischiosa per applicarla (è un noto atteggiamento degli informatici dire “se funziona, meglio non toccarlo”). In questi casi il workaround deve essere ben documentato e diffuso.

12.13.5 Gestione delle crisi

Il crisis management si occupa degli aspetti strategici conseguenti a un incidente grave. Non viene messo in pratica solo in caso di incidenti relativi alla sicurezza delle informazioni, ma anche, per esempio, di problemi economici, andamenti azionari, scalate ostili, servizi negativi sui mezzi di informazione.

È un processo basato soprattutto su tecniche di pubbliche relazioni nei confronti di clienti, partner, investitori, autorità, altre parti interessate e mezzi di informazione. Deve essere gestito dalla Direzione e dagli uffici addetti alla comunicazione che costituiscono il Comitato di crisi. In alcune organizzazioni, chi presiede il Comitato di crisi svolge il ruolo di Business continuity manager, di cui si parla nel paragrafo 12.14.4. Il personale tecnico potrebbe essere coinvolto solo per fornire informazioni al Comitato di crisi.

Quando la crisi riguarda la sicurezza delle informazioni, il Comitato di crisi interagisce con l'ISIRT (o con il CERT, se la crisi riguarda la sola sicurezza informatica), in modo da ricevere e fornire aggiornamenti tempestivi sulla situazione.

Un piano di gestione delle crisi (crisis management plan) deve indicare innanzitutto chi ha l'incarico di rappresentare l'organizzazione nei mezzi di informazione; a tutto il resto del personale devono essere fornite regole affinché si astengano dal fare qualsiasi dichiarazione sui mezzi di informazione, inclusi i social network, o a entità esterne all'organizzazione, inclusi parenti e amici.

I rappresentanti dell'organizzazione possono essere molteplici, purché tra loro coordinati. Questo in considerazione delle diverse parti da contattare: mezzi di informazione, sindacati, mercati, autorità, clienti, fornitori, partner, eccetera. Si possono avere più rappresentanti anche quando l'organizzazione ha sedi in più Paesi e quindi deve interagire con mezzi di informazione e parti interessate di lingue e culture diverse.

Il piano di gestione delle crisi prevede come mantenere relazioni preventive con le forze dell'ordine (paragrafo 12.3.4) e con i mezzi di informazione per poterle contattare con maggiore facilità ed efficacia quando necessario.

Il piano dovrebbe infine riportare esempi di messaggi da diffondere in caso di crisi. Si consiglia di preimpostarli, visto che nei momenti di crisi non si ha la lucidità necessaria per redigerli al meglio.

È importante diffondere messaggi sufficientemente approfonditi, da redigere anche con l'aiuto del personale tecnico.

Esempio 12.13.9. Nel 2014, la società francese di telecomunicazioni Orange subì un attacco da parte di malintenzionati che ottennero accesso ai dati anagrafici dei clienti. Il danno, apparentemente, non fu elevato.

Nelle comunicazioni al pubblico, purtroppo, Orange dichiarò di non sapere se i dati fossero cifrati o meno¹¹⁶, perdendo così la fiducia di molti suoi clienti.

12.13.6 Digital forensics

Le tecniche di digital forensics sono necessarie quando vanno raccolte prove per azioni legali o disciplinari.

Questa disciplina nasce nel 1984, quando il laboratorio scientifico dell’F.B.I. iniziò a sviluppare dei programmi da utilizzare per raccogliere prove legali dai computer e creò un gruppo di lavoro denominato C.A.R.T. (Computer Analysis Response Team).

Una definizione di digital forensics, seppure limitata al contesto penale e non civile, è la seguente.

Digital forensics: L’uso di metodi scientifici e provati per preservare, raccogliere, validare, identificare, analizzare, interpretare, documentare e presentare i mezzi di prova digitali derivati da dispositivi digitali, allo scopo di facilitare o portare avanti la ricostruzione di eventi criminali o aiutare ad

anticipare azioni non autorizzate [33].

I dispositivi digitali sono di tantissimi tipi: computer personali e server, spazi virtuali (inclusi quelli dei servizi cloud), telefoni (inclusi cellulari, smartphone, VOIP), tablet, macchine fotografiche, memorie USB e altri. Essi possono essere spenti o attivi, collegati a una rete informatica pubblica o privata o essere stand alone. Si tratta quindi di una materia che richiede competenze tecniche assai varie.

La tecnica base per l’acquisizione dei dati da un computer spento è semplice: si effettuano due copie bit a bit (tali da poter individuare e analizzare anche file nascosti, cancellati o corrotti) dell’hard disk. Una viene sigillata, l’altra utilizzata per le indagini.

Le procedure sono più complesse in tutti gli altri casi e comprendono tecniche di live forensics per sistemi che non si possono spegnere, anche per evitare l’alterazione dei mezzi di prova, e le intercettazioni del traffico di rete.

Non tutto si riduce alle competenze tecnologiche perché devono essere conosciute le regole per raccogliere, analizzare e documentare i mezzi di prova affinché siano accettabili da un tribunale. Ogni passaggio tra i diversi operatori coinvolti (la catena di custodia) deve essere documentato e tenuto sotto controllo in modo da dimostrare la corretta gestione dei mezzi di prova.

Molto spesso le prove vengono invalidate perché raccolte in difformità alle procedure applicabili o alla normativa sui diritti delle persone, come quelle relative alla privacy e ai diritti dei lavoratori¹¹⁷.

Per questi motivi bisogna avere competenze legali sulla normativa vigente, sui casi già affrontati presso le aule di giustizia e sulle prassi consolidate in ambito penale e civile. Si ricordi che la procedura penale e quella civile sono tra loro diverse [9]; per esempio nel civile le email sono spesso accettate come prova¹¹⁸.

Esistono molti libri sulla digital forensics [23, 25, 45, 55, 164], ma le regole base da seguire in un’organizzazione quando si ha il sospetto che qualcuno stia compiendo dei reati con strumenti informatici sono due:

consultarsi sempre preventivamente con un legale: è inutile raccogliere prove se poi il legale non sa o non può utilizzarle;

se si vuole agire immediatamente, scollegare il sistema dalla rete, sigillarlo senza spegnerlo e non fare altro, a parte consultare un legale.

Un particolarissimo caso di uso di tecniche di digital forensics riguarda i sistemi informatici quando sono attaccati da malintenzionati. In questo caso, alcune organizzazioni cercano di indirizzare l’attaccante verso sistemi “esca” per studiarne i comportamenti (in questo caso i sistemi sono detti honeypot), per deviarne le mire o per rallentare l’attacco (sistemi detti tarpit). Inutile ricordare che queste tecniche devono essere attuate solo da personale molto preparato.

12.14 Continuità operativa (Business continuity)

La definizione seguente è tratta dalla ISO 22300 [73].

Business continuity (Continuità operativa): capacità di un’organizzazione di continuare a fornire prodotti o servizi a un livello accettabile predefinito, dopo

un incidente di disturbo.

Si sta parlando di “business” e non di “informazioni” o “IT” continuity: è quindi compito di tutte le funzioni e processi dell’organizzazione stabilire come garantire la propria continuità e questo compito non può essere ridotto alla sola disponibilità delle informazioni.



Figura 12.14.1:

Rapporti tra business continuity e IT

Esempio 12.14.1. In una banca, il responsabile delle agenzie deve stabilire quanto tempo un'agenzia può rimanere chiusa o per quanto tempo può operare senza i sistemi informatici. Queste scelte non sono di competenza del responsabile della sicurezza delle informazioni o dell'IT.

L'IT dovrà successivamente decidere come garantire la disponibilità dei sistemi per soddisfare i requisiti delle agenzie.

Esempio 12.14.2. Nel marzo del 2000, un incendio nell'unico sito di produzione dei microchip per cellulari della Ericsson nel Messico ha causato perdite per 2 miliardi di dollari e fatto perdere alla società la leadership nel mercato dei cellulari di quegli anni¹¹⁹.

In questo caso, il problema di continuità non riguardava le informazioni.

Tradizionalmente, il problema della continuità è stato affrontato dai responsabili dei sistemi informatici, ma senza un mandato preciso da parte delle altre aree

dell'organizzazione. Questo potrebbe portare al paradosso di avere sistemi informatici attivi senza utilizzatori.

Questa definizione stabilisce che nell'ambito della sicurezza delle informazioni è necessario occuparsi:

della disponibilità delle informazioni con opportune ridondanze;

della continuità dei processi di sicurezza delle informazioni (informationsecurity during disruption), tra cui: controllo degli accessi, controllo degli archivi fisici e dei sistemi informatici, monitoraggio, gestione degli incidenti.

È quindi escluso da questo ambito l'analisi e la predisposizione delle misure di continuità per gli altri processi.

La continuità operativa prevede i seguenti passi, a cui sono dedicati i paragrafi successivi (per approfondimenti sono disponibili numerosi testi [15, 74, 75, 90, 144]):

realizzare una business impact analysis;

valutare il rischio relativo alla continuità operativa;

stabilire gli obiettivi e le strategie di ripristino;

impostare i piani di continuità;

effettuare i test e mantenere i piani.

12.14.1 La business impact analysis (BIA)

La business impact analysis (BIA) ha la finalità di individuare i tempi massimi accettabili di interruzione delle attività dell’organizzazione (maximum tolerable period of disruption o MTPD) e delle risorse a esse collegate (incluse le informazioni), come sintetizzato nella figura 12.14.2.

Gli MTPD devono essere calcolati sulla base dei requisiti dei clienti e quelli legali applicabili. Il MTPD può anche essere calcolato per momenti particolari, per esempio fine mese per la contabilità.

Processo

Commerciale

MTPD

Max 8 ore



Risorse

Sedi

Persone

Informazioni

Sistemi IT:

- File server
- LAN
- e-mail
- e-mail server
- archivi fisici

Impianti

Tempo massimo indisponibilità

8 ore

Figura 12.14.2:

Relazione processi-risorse per BIA

Nella BIA sono da riportare le prestazioni minime da garantire in fase di emergenza (level of business continuity o LBC), solitamente minori rispetto a quelle disponibili nella normalità. Le risorse necessarie per garantire la continuità delle operazioni devono quindi essere dimensionate per ottenere le prestazioni stabilite.

Per individuare le risorse da rendere disponibili in caso di emergenza, si devono considerare: le sedi dove operare, le persone, le apparecchiature per le attività produttive o di erogazione del servizio (per esempio, in un’azienda casearia, devono essere considerati gli impianti di raccolta e conservazione del latte), le informazioni.

Quando si stabiliscono le informazioni necessarie per garantire la continuità, occorre stabilire il maximum tolerable data loss o MTDL, ossia la massima quantità di dati che si possono perdere, inclusi quelli conservati in formato non elettronico (per esempio, i contratti cartacei con i clienti, fornitori e partner).

Chi si occupa di sicurezza delle informazioni deve considerare i requisiti stabiliti dai diversi processi e:

stabilire gli obiettivi di ripristino delle informazioni necessarie a questi processi (paragrafo 12.14.3);

effettuare una BIA relativa ai processi di sicurezza delle informazioni, in modo

da garantirla in caso di emergenza.

I processi di sicurezza delle informazioni devono avere MTPD inferiori agli obiettivi di ripristino delle informazioni; in caso contrario, queste sarebbero disponibili, ma senza un adeguato livello di sicurezza.

12.14.2 Valutazione del rischio per la continuità operativa

La BIA va accompagnata da un'analisi del rischio relativo alla continuità operativa, che consideri i casi di interruzione dei processi dell'organizzazione allo scopo di decidere come ripristinare i processi.

I rischi di continuità con impatti sulla sicurezza delle informazioni si possono raggruppare nelle seguenti categorie:

indisponibilità della sede o dei locali per distruzione, inaccessibilità o inagibilità, non necessariamente a causa di disastri (una manifestazione in strada o un'azione delle forze di polizia nell'appartamento a fianco possono rendere inaccessibile una sede); questa categoria comprende il caso di distruzione degli archivi di documenti non su sistemi informatici; è anche opportuno considerare l'impossibilità di accedere alla sede a causa di chiusure generalizzate come nel caso dell'emergenza COVID della primavera 2020;

indisponibilità o distruzione degli archivi non informatici;

indisponibilità totale o parziale dei servizi informatici (incluse le applicazioni e la rete interna); gli incidenti con impatto sulla loro disponibilità sono anche detti contingenze (contingency)[144];

indisponibilità totale o parziale della connessione Internet;

indisponibilità del personale (per sciopero, per dimissioni contemporanee, per malattia);

indisponibilità dei fornitori di servizi e prodotti necessari alla produzione e all'erogazione dei servizi dell'organizzazione.

Ulteriori rischi di continuità possono essere identificati, ma solitamente non relativi alla sicurezza delle informazioni. Tra di essi vi sono i rischi di rottura dei macchinari di produzione in un'azienda manifatturiera, la carenza di materie prime o l'indisponibilità dei trasportatori.

Per la sicurezza delle informazioni, questa valutazione del rischio dovrebbe essere parte del rischio relativo alla sicurezza delle informazioni, di cui si è discusso nel capitolo 4 e nei successivi. In questo contesto è importante analizzare la probabilità di accadimento di un evento, per evitare investimenti eccessivi a fronte di eventi molto rari o investimenti insufficienti per contrastare eventi più frequenti o di notevole impatto.

12.14.3 Obiettivi e strategie di ripristino

In questo paragrafo si tratta solo degli obiettivi e delle strategie per la disponibilità delle informazioni, oggetto di questo libro, e non della continuità di processi non collegati alla gestione e sicurezza delle informazioni.

In base alle analisi, chi si occupa della sicurezza delle informazioni si dà obiettivi di cui seguono le definizioni più diffuse accompagnate da alcune considerazioni.

recovery time objective (RTO): tempo massimo per ripristinare la disponibilità delle informazioni; deve essere minore o uguale al MTPD dei processi che le utilizzano; per sistemi o servizi informatici e per archivi non informatici con il medesimo RTO, devono essere stabilite le priorità reciproche;

recovery point objective (RPO): il punto nel tempo nel quale i dati sono coerenti e devono essere ripristinati; per i sistemi informatici corrisponde al tempo tra un backup e un altro, per le informazioni in altro formato corrisponde al tempo necessario alla loro copia e archiviazione in un luogo alternativo e deve essere minore o uguale al MTDL; quando si stabilisce l'RPO, bisogna valutare se i dati persi possono essere ricostruiti e in quanto tempo;

minimum business continuity objective (MBCO): le risorse minime necessarie nella fase di emergenza (per esempio, server meno potenti di quelli normalmente in uso o un numero ridotto di postazioni e persone addette al funzionamento di un processo); questo parametro deve essere maggiore o uguale al LBC; quando si definisce l'MBCO, si deve stabilire la durata prevista per l'emergenza, visto che un ridotto numero di persone non può condurre a tempo indeterminato processi normalmente condotti da più persone.

RTO, RPO e MBCO devono essere stabiliti per ciascun sistema o servizio informatico e per ciascun archivio non informatico.

Per soddisfare gli obiettivi, vanno stabilite strategie di ripristino. Chi si occupa di sicurezza delle informazioni dovrebbe occuparsi delle strategie dei soli processi relativi alla disponibilità e alla sicurezza delle informazioni.

Tra le opzioni si ricordano le seguenti:

in caso di indisponibilità della sede:

trasferimento di parte del personale addetto alla sicurezza delle informazioni in

altra sede dell’organizzazione o di un fornitore (business user recovery site), con disponibilità di spazi compatibili con l’MBCO e distanza tale da essere raggiunta dal personale in tempi minori al RTO e da non avere impatti dal medesimo incidente che ha reso indisponibile il sito primario;

lavoro fuori sede o da casa (smart working);

in caso di distruzione degli archivi non informatici:

uso di copie della documentazione predisposte in una sede alternativa;

uso di copie digitali predisposte preventivamente, in linea con l’RPO;

in caso di indisponibilità dei sistemi informatici:

prosecuzione delle attività con sistemi non informatici;

utilizzo dei sistemi informatici, dimensionati in modo coerente con l’MBCO, con procedure di contingenza locale, da attivare in conformità al RTO e con i dati allineati al RPO (paragrafo 12.14.3.1);

attivazione di sistemi informatici alternativi (sistemi di disasterrecovery), dimensionati in modo coerente con l’MBCO, da attivare in conformità al RTO e con i dati allineati al RPO (paragrafo 12.14.3.2);

nel caso di guasto hardware, uso di pezzi di ricambio da un magazzino interno costituito in precedenza o da un fornitore con tempi di consegna predefiniti;

in caso di indisponibilità della connessione Internet:

attivazione di sistemi informatici in siti alternativi (sistemi di disasterrecovery);

uso di connessioni alternative (se disponibili);

in caso di indisponibilità del personale:

individuazione delle persone necessarie per riattivare ed eseguire i processi, in linea con il MBCO;

coinvolgimento di personale interno con le competenze del personale assente (per questo, è necessario tenere sotto controllo le competenze del personale,

come indicato nel paragrafo 12.4.3);

ricorso a fornitori specializzati;

documentazione di aiuto alle persone non esperte in sostituzione di quelle assenti;

in caso di indisponibilità dei fornitori:

preventivamente, verifica di un loro piano di continuità operativa con RTO, RPO e MBCO compatibili con quelli dell'organizzazione;

preventivamente, utilizzo di due o più fornitori per i medesimi servizi o prodotti e con capacità tali da sopperire alle mancanze di uno di essi, in linea con il MBCO;

preventivamente, individuazione di fornitori alternativi a quelli utilizzati, in modo da poterli utilizzare in caso di necessità, con tempi e prestazioni compatibili con il RTO e il MBCO.

Esempio 12.14.3. La Ericsson, dopo l'incendio del 2000, ha attivato due stabilimenti dove produrre microchip: uno nel Messico e uno in India.

I sistemi informatici si trovano solitamente in un sito principale, detto sito primario.

Le strategie relative al loro ripristino prevedono la duplicazione (o ridondanza) dei sistemi e apparecchiature informatiche o di loro parti, in modo da continuare le operazioni secondo i parametri di RTO, RPO e MBCO. Queste strategie sono di due tipi:

contingenza locale (termine non ufficiale), se i guasti riguardano singole apparecchiature e il ripristino avviene presso il sito primario;

disaster recovery e siti alternativi se il ripristino avviene presso un altro sito perché la sede o il CED sono inagibili o è stata compromessa gran parte dei sistemi informatici.

12.14.3.1 Contingenza locale

Il termine contingenza locale non è ufficialmente condiviso e riguarda guasti locali. I termini alta affidabilità, high reliability, alta disponibilità e high availability sono utilizzati se le strategie sono tali da garantire una disponibilità dei servizi informatici molto elevata, generalmente del 99,999%.

Per la contingenza locale esistono soluzioni che garantiscono tempi di ripristino diversi:

molto brevi se per le normali attività e per distribuire il carico di lavoro sono usati più sistemi contemporaneamente (load balancing o clustering) oppure sono usati componenti duplicati (per i server, sono spesso duplicati CPU, RAM, dischi di memoria, interfacce di rete e di alimentazione); in caso di guasto di uno di essi, gli altri possono garantire la continuità, anche se con prestazioni inferiori e comunque definite in base al MBCO, fino alla riparazione o sostituzione dell'elemento guasto;

lunghi, se l'hardware (spesso meno potente di quello primario, ma in linea con l'MBCO) è disponibile ma deve essere configurato;

molto lunghi, se si prevede di avere copie di backup dei dati e dei programmi software e di acquistare solo in caso di necessità le risorse hardware su cui caricarle.

Nei CED, per garantire la disponibilità dei servizi, sono normalmente realizzate ridondanze di tutti gli impianti: generatori, UPS, aria condizionata, eccetera. Anche le connessioni alla rete informatica, a Internet e all'elettricità sono spesso duplicate e in alcuni casi allacciate a fornitori e reti diverse, affinché l'indisponibilità di uno di essi non abbia impatti sui sistemi. A seconda del tipo di ridondanze, il CED può essere classificato secondo diversi livelli di disponibilità [36, 82, 151].

I sistemi ridondati localmente possono essere utilizzati per prevenire interruzioni a seguito di cambiamenti. Infatti, è possibile effettuare il cambiamento su uno solo di essi, verificarne la correttezza, e poi estenderlo agli altri.

12.14.3.2 Disaster recovery e siti alternativi

Il sito di disaster recovery (o sito di DR) è un sito per i sistemi informatici, alternativo a quello primario e può anche essere usato per ospitare copie della documentazione in formato non digitale.

I principi sono gli stessi di quelli sopra indicati, ma in questo caso i sistemi duplicati si trovano in un altro sito. I tipi di siti di DR sono sotto elencati; i primi garantiscono RTO e RPO più elevati degli ultimi:

siti di backup, dove si trovano unicamente i backup;

siti freddi o cold site, dove si trovano i backup e delle sale con potenza energetica, aria condizionata e connettività predisposte per ospitare l'hardware da acquistare o noleggiare solo in caso di necessità;

siti tiepidi o warm site, dove si trovano solo i backup e i sistemi opportunamente configurati; in caso di necessità occorre accendere i sistemi, aggiornare il software e caricare i dati dai backup;

siti caldi o hot site, dove si trovano le copie esatte dei sistemi di produzione (ma solitamente meno potenti), sincronizzate periodicamente con questi;

mirrored site o, in italiano discutibile, siti mirrorati, ossia siti caldi i cui sistemi sono sincronizzati in ogni momento con quelli di produzione; in alcuni casi i sistemi sono in load balancing tra di loro, pur se molto distanti.

Le soluzioni richiedono diversi livelli di spesa, da bilanciare con le reali necessità dell'organizzazione, determinate da RTO, RPO e MBCO e con la probabilità di accadimento delle minacce alla continuità.

Non vi sono regole precise sulla distanza minima tra sito primario e quello di DR: i progettisti, in fase di valutazione del rischio relativo alla continuità operativa, devono valutare la possibile estensione geografica degli eventi negativi (per esempio terremoti o crisi geopolitiche), insieme ai costi da affrontare. In alcuni casi si creano due siti tra loro in mirroring a poca distanza (in questo caso si parla anche di campus) e un sito di backup, freddo o tiepido a maggiore distanza.

Il sito di DR può essere affittato presso un fornitore e, in questi casi, nell'ambito del contratto devono essere concordate le misure di sicurezza opportune e le modalità da seguire per effettuare i test. Se il fornitore ha più clienti, sono da concordare le procedure da seguire nel caso più organizzazioni contemporaneamente avessero la necessità di utilizzare il sito; abitualmente si dà la precedenza alle organizzazioni coinvolte nella sicurezza pubblica o nella salvaguardia di vite umane.

Il sito di DR può essere utilizzato anche in caso di eventi non catastrofici, per

esempio per effettuare test di cambiamenti particolarmente critici, per mantenere attivi dei servizi quando nel sito primario è in corso un lavoro di manutenzione o un trasloco, oppure nel caso in cui i sistemi del sito primario hanno problemi o sono attaccati.

Per le attività degli utenti dei sistemi informatici sono utilizzati i termini sito di business continuity o business users recovery site per indicare dove svolgere le attività quando è indisponibile il sito primario dove lavorano.

Chi si occupa di sicurezza delle informazioni deve garantire che i livelli di sicurezza dei siti di disaster recovery e di business continuity siano equivalenti a quelli dei siti primari. Anche la sicurezza fisica, non solo quella informatica, deve essere opportunamente garantita: non è raro trovare sulle scrivanie dei siti di business continuity informazioni molto riservate o un controllo degli accessi fisici meno rigido.

Si ricorda che ogni cambiamento effettuato nel sito primario va replicato sui sistemi nel sito di disaster recovery.

12.14.4 I piani di continuità

Dopo aver deciso come garantire la continuità dei servizi informatici, la disponibilità delle informazioni e la loro sicurezza, occorre redigere procedure semplici e schematiche, utilizzabili anche da personale poco preparato o in condizioni di tensione, che descrivano cosa fare in caso di incidente con impatti sulla continuità. Queste procedure sono denominate piani di continuità (business continuity plan o BCP). Va notato che si utilizza il termine “piano”, anche se si tratta di “procedure”.

Una parte del piano di continuità, detto piano di disaster recovery, riporta le azioni tecniche informatiche da compiere nei siti di disaster recovery: avvio dei sistemi, sincronizzazione dei dati, riconfigurazione della rete e così via.

Come già detto, è compito di chi si occupa della sicurezza delle informazioni realizzare i piani relativi alla disponibilità dei sistemi informatici e degli archivi e quelli relativi ai processi di sicurezza delle informazioni. Per i piani relativi ad altri processi, si dovrebbe collaborare con i loro referenti limitatamente alle parti relative alla gestione delle informazioni.

Per l'attuazione di quanto previsto dai piani di continuità sono normalmente previsti diversi gruppi di persone:

gli utenti, che devono riprendere le attività secondo le modalità previste dai piani;

i tecnici, con le competenze necessarie per le attività di ripristino e conduzione dei sistemi informatici e delle apparecchiature tecnologiche;

il comitato tecnico di crisi, con il compito di coordinare i tecnici ed i fornitori da coinvolgere;

il comitato di crisi (paragrafo 12.13.5) con il compito di mantenere i rapporti con i clienti, i partner, gli investitori, le parti interessate e con i mezzi di informazione.

Si deve quindi stabilire quando un incidente deve essere gestito come tale (paragrafo 12.13) o devono essere attivati (o, in italiano discutibile invocati, dall'altrettanto discutibile inglese invoked) i piani di continuità. Per esempio, l'impossibilità di accedere alla sede a causa della neve potrebbe essere trattato come un “normale” incidente se l'accesso può essere ripristinato entro poche ore oppure potrebbe richiedere l'attivazione dei piani di continuità e l'uso dei siti

alternativi se si prevedono interruzioni più lunghe.

Deve essere redatta una lista dei contatti con i riferimenti dei componenti di ciascun gruppo, inclusi i loro possibili sostituti, per contattarli in caso di necessità.

Le procedure devono stabilire chi ha il potere di richiedere l'attivazione di quelle di continuità. La persona con questa autorità è spesso indicata con il termine di business continuity manager. Questa persona ha ulteriori responsabilità: garantire l'aggiornamento dei piani di continuità e delle liste dei contatti, accertarsi che siano effettuati i test (paragrafo 12.14.5) e presiedere il comitato di crisi.

Chiunque rileva un evento per cui si potrebbero attivare i piani di continuità deve segnalarlo al business continuity manager. I piani di continuità e le liste di contatto devono stabilire le modalità con cui il business continuity manager può essere contattato, eventualmente passando attraverso diversi livelli gerarchici predefiniti (escalation).

Il piano di business continuity deve poi indicare i luoghi dove possono riunirsi i vari comitati (da prevedere almeno due siti distinti, in caso uno di essi sia inagibile), quali sono i siti di DR e di business continuity, quali fornitori contattare e per quali motivi (anche per loro è necessario prevedere almeno due riferimenti distinti), eccetera.

I piani devono sempre evidenziare che la priorità è la vita delle persone. Per esempio, in caso di evacuazione di un edificio, sono da seguire delle regole di blocco dei PC e di chiusura degli archivi, ma queste devono essere secondarie se vite umane sono in pericolo immediato.

Il piano di continuità è sovente composto da più piani di continuità relativi a singoli ambiti; per esempio ci possono essere piani dedicati a ciascuna funzione organizzativa, alla salvaguardia del personale, alla gestione dei siti fisici e dei sistemi informatici. È importante che essi siano tra loro coerenti e coordinati e siano chiare le relazioni tra di essi.

I piani di continuità devono prevedere la registrazione di quanto succede quando sono attivati (esempio di log manuale): ogni gruppo deve registrare ogni evento, ogni attività fatta e ogni persona contattata, insieme all'ora e al nome di chi ha svolto l'attività o contattato le persone.

12.14.5 Test e manutenzione

Tutti i piani di continuità vanno verificati: senza un minimo di pratica il panico prende il sopravvento.

Effettuare test pratici dei piani di continuità è oneroso: evacuare gli uffici, fare in modo che il personale dei gruppi tecnici si diriga presso i siti alternativi, farli lavorare in condizioni di emergenza fino alla fine del test e poi farli tornare al sito primario richiede tempo e comporta un forte rallentamento delle attività quotidiane. Quando si tratta di sistemi informatici, lo spegnimento del sistema primario, l'attivazione di quello in disaster recovery e la riattivazione del sistema primario dopo il test comportano il rischio di perdere dati.

Si possono quindi condurre diversi tipi di test. Il più semplice è quello detto a tavolino (desktop) e prevede un riesame collettivo dei piani di continuità da parte delle persone coinvolte. Questo esercizio è molto utile per verificare se i piani sono aggiornati. Ulteriori test più complessi e onerosi, ma anche più efficaci,

prevedono simulazioni con personale preavvertito o no.

Per i sistemi informatici è sempre necessario prevedere test di ripristino dei sistemi presso il sito di disaster recovery e la verifica dell'allineamento dei loro dati a quelli di produzione. Se non si tratta di una simulazione completa con lo spegnimento dei sistemi del sito primario (effettuata raramente), i test possono dare degli errori, per esempio di interfacciamento con altri sistemi. Questi errori devono essere riconosciuti, in modo da valutare correttamente l'esito dei test.

È compito del business continuity manager stabilire quali test devono essere fatti e con quale frequenza e quando effettuare test straordinari a seguito di modifiche significative all'organizzazione o ai sistemi informatici.

Se il test rileva degli errori, vanno corretti. Tra gli errori più comunemente rilevati si riscontra il mancato aggiornamento dei piani, delle istruzioni e delle liste dei contatti. Nulla di male: basta aggiornarli e fare in modo che in futuro siano aggiornati per tempo.

I test possono dare un altro particolare tipo di errore: il mancato rispetto dell'RTO o, più raramente, dell'RPO. In questo caso, è pratica comune, ma scorretta, voler modificare l'RTO (o l'RPO) nella business impact analysis.

Se l'RTO o l'RPO non possono essere raggiunti perché la tecnologia adottata non lo consente, bisogna scegliere se modificare la tecnologia, con i costi consequenti, o accettare il rischio. In questo caso è necessario evidenziarlo, non nasconderlo modificando l'obiettivo iniziale.

12.15 Conformità

Ogni organizzazione deve agire in conformità alla normativa vigente, alle procedure interne, ai contratti stipulati con i clienti e partner, a standard nazionali o internazionali adottati volontariamente.

Per verificare la propria conformità a procedure, requisiti o norme, un’organizzazione deve condurre degli audit che possono essere svolti da personale interno o da organizzazioni esterne. Particolare caso di verifiche sono i vulnerability assessment.

12.15.1 Normativa vigente

Ogni organizzazione deve tenere sotto controllo la normativa applicabile. Il metodo più banale consiste nel mantenerne un elenco e verificarne periodicamente lo stato di aggiornamento.

Ci sono libri [123], mailing list e siti web generici o settoriali per mantenersi aggiornati. Purtroppo quelli istituzionali¹²⁰ non sono sempre di facile consultazione, mentre quelli non istituzionali, dopo qualche anno, attraversano varie vicissitudini e non sono più aggiornati¹²¹.

Quando si utilizzano servizi informatici e non informatici all'estero, è importante capire la differenza tra le legislazioni di Paesi diversi. In particolare, negli USA, il concetto di privacy è diverso da quello europeo: in Europa la normativa privacy serve a tutelare la dignità dell'individuo, mentre negli USA il Governo è autorizzato ad acquisire tutte le informazioni necessarie alle protezione dello Stato a partire da quelle relative agli individui.

12.15.1.1 Standard volontari

Un’organizzazione può decidere di conformarsi a standard, la cui adozione non è richiesta da alcuna legge, ma può essere ritenuta utile per l’immagine dell’organizzazione sul mercato, per partecipare a gare o per avere un riferimento per migliorare il proprio approccio alla sicurezza delle informazioni. Alcune decidono di adottare degli standard e, talvolta, di richiedere un certificato di conformità, perché richiesto dai clienti per poter avviare o continuare il rapporto di affari. Nonostante l’adozione di questi standard sia spesso imposta da clienti o regolamenti, essi sono noti come standard volontari.

Tra di essi vi sono gli standard con requisiti relativi ai sistemi di gestione come la ISO/IEC 27001, la ISO 9001, la ISO/IEC 20000-1 e la ISO 22301. Chi li adotta si impegna a rispettare tutti i loro requisiti. Altri “standard”, come la ISO/IEC 27002, ITIL® e il PMBOK® del PMI, non riportano requisiti da adottare obbligatoriamente e sono utilizzati come riferimenti per la terminologia e per migliorare alcuni controlli di sicurezza delle informazioni.

Sono disponibili moltissime altre norme o linee guida, sia generali (come lo standard dell’Uptime Institute, il CMMI, gli standard TIA, il COBIT), sia settoriali, come le GMP in ambito farmaceutico.

Recentemente sono diventate molto popolari le linee guida del NIST sulla Cybersecurity [113], anche perchè promosse dalla Banca centrale europea, da alcune entità italiane come “Framework Nazionale per la Cyber Security” [6] e dall’Agenzia per l’Italia digitale [3]. Scelta curiosa, visto che queste entità hanno promosso delle linee guida di origine statunitense invece che di livello internazionale, come la ISO/IEC 27001 e la ISO/IEC 27015 (ora abrogata).

Ulteriori schemi sono stati avviati nel tempo. Per esempio, il CyberSecurity

Maturity Model Certification (CMMC), avviato nel 2020 dal Department of Defence USA per i propri fornitori¹²² [?] e il TISAX¹²³ per il settore dell’automotive. Questi, in particolare, prevedono cinque livelli di maturità che possono essere assegnati all’organizzazione che si sottopone a verifica.

12.15.1.2 Normativa sulla criminalità informatica

Il primo dispositivo di legge italiano sulla criminalità informatica (computer crime) è del 1993 e consiste in un’estensione al contesto informatico di alcuni reati già previsti dal Codice Penale (accesso abusivo ai sistemi IT, diffusione di virus, danneggiamento di sistemi IT, eccetera).

Un’organizzazione non deve far nulla per essere conforme a questa normativa. Deve “solo” evitare di compiere i reati indicati.

Ulteriori normative applicabili sono il D. Lgs. 373 del 2000 e la Legge 48 del 2008 (che regolamenta anche la digital forensics).

12.15.1.3 Normativa sul diritto d’autore e sulla proprietà industriale

La normativa in vigore in materia di diritto d’autore è la Legge 633 del 1941 (promulgata dal Re d’Italia e di Albania e Imperatore d’Etiopia!). Questa Legge è stata oggetto di moltissime modificazioni, spesso difficili da consolidare.

È di interesse anche il Codice di proprietà industriale (D. Lgs. 30 del 2005), il suo regolamento di attuazione (Decreto Ministero Sviluppo Economico 33 del

2010) e quanto previsto dal Codice civile in materia di brevetti.

Si osservi che i software e le banche dati sono coperte dal diritto d'autore regolamentato da queste normative. Se in un'organizzazione sono utilizzati software in contrasto con la normativa sul diritto d'autore, l'organizzazione corre il rischio di subire processi e pagare multe.

Devono quindi essere attivati processi per censire le licenze intestate all'organizzazione e verificarne la corrispondenza con i software installati. Ciò richiede una buona collaborazione tra ufficio acquisti e responsabili dei sistemi informatici. Devono essere stabiliti processi per gestire la dismissione delle licenze quando non più necessarie.

Bisogna quindi mantenere un inventario delle licenze (paragrafo 12.5.2), tale da avvertire quando queste sono in scadenza per rinnovarle se necessario. Da prestare attenzione alla varietà di licenze previste dai produttori di software: in alcuni casi dipendono dal numero di computer su cui i software sono installati, in altri dal numero di CPU dei computer stessi, in altri ancora dal numero di utenti, e così via. Insieme all'inventario va stabilito un buon sistema di archiviazione delle prove di licenza, ossia dei documenti in formato elettronico o cartaceo che attestano il possesso della licenza.

Ovviamente questa normativa è importante per gli stessi produttori di software, che dovrebbero prestare attenzione alla sua applicazione per salvaguardare i propri diritti.

Per quanto riguarda la proprietà industriale, le imprese devono almeno specificare in istruzioni scritte quali informazioni sono da classificare segreti industriali (paragrafo 12.5.1) e attuare misure di sicurezza per proteggerle¹²⁴.

Per proteggere il diritto d'autore sui libri, sul software e su altri media prodotti, un'organizzazione può ricorrere alle tecniche di digital rights management. Esse includono segni fisici (detti watermarks) sul supporto (per esempio un DVD), controlli digitali basati su crittografia, firme digitali, chiavi del prodotto, chiavi fisiche collegate al dispositivo e connessioni con server online. Tutte queste tecniche possono creare problemi agli utilizzatori (per esempio se hanno bisogno di una copia a scopo di disaster recovery, se cambiano dispositivo o se vogliono usare il prodotto in viaggio e offline). Per questo devono essere selezionate con attenzione, considerando le esigenze dei potenziali utilizzatori.

12.15.1.4 Responsabilità amministrativa delle imprese

Il Decreto Legislativo 231 del 2001 stabilisce che un'organizzazione e la sua Direzione, e non solo la persona che materialmente li ha perpetrati, sono responsabili per reati commessi nel loro interesse o vantaggio, tra cui concussione, corruzione e truffa.

Negli anni, a questi reati cosiddetti “tradizionali”, si sono aggiunti, tra gli altri: delitti informatici e trattamento illecito di dati, falsità in [...] strumenti o segni di riconoscimento e delitti in materia di violazione del diritto d'autore. Altri reati aggiunti, come gli abusi di mercato o l'omicidio colposo per violazione delle norme antinfortunistiche, sono estranei alla sicurezza delle informazioni propriamente detta.

La normativa stabilisce che l'organizzazione e i suoi organi apicali non sono responsabili se i reati sono commessi contravvenendo a disposizioni impartite o aggirando misure di sicurezza create per impedirli. In altre parole, la Direzione rischia di essere accusata se non ha fatto nulla per impedire tali reati.

È quindi da pubblicare e diffondere un codice etico che stabilisca l'opposizione della Direzione ad avere vantaggi da reati (il codice etico e la politica per la sicurezza delle informazioni possono essere integrati in un unico documento) e un disciplinare con i comportamenti da tenere quando si rilevano reati o se ne riceve segnalazione (caso particolare di gestione degli incidenti, per il quale è anche da stabilire un meccanismo, detto di whistleblowing, per garantire l'anonimato di chi effettua la segnalazione).

Vanno attuate misure di tipo tecnico e di tipo organizzativo per garantire la separazione delle responsabilità e la limitazione degli accessi alle informazioni e agli strumenti dell'organizzazione. Queste misure sono utili anche per prevenire i reati cosiddetti "tradizionali".

Le misure nel loro complesso sono indicate come modello organizzativo 231 ed è opportuno descriverle anche brevemente in un documento; le singole procedure sono solitamente denominate protocolli.

Il modello 231 e la sicurezza delle informazioni, anche se hanno molti punti di sovrapposizione, sono spesso gestiti da persone diverse, che dovrebbero collaborare nella scelta e attuazione di procedure e protocolli e, se possibile, integrarli.

12.15.1.5 Normativa sul commercio elettronico

La normativa applicabile al commercio elettronico (e-commerce) è riportata dai D. Lgs. 70 del 2003, D. Lgs. 206 del 2005 (Codice del consumo) e D. Lgs. 69 del 2012. La Direttiva Europea 2011/83 sui diritti dei consumatori ha introdotto ulteriori modifiche nell'ordinamento italiano.

Vi sono altre normative settoriali, per esempio sulla commercializzazione di servizi finanziari, sui giochi on-line e sulle attività editoriali.

Per la sicurezza delle informazioni propriamente detta, queste normative, tra gli altri adempimenti, richiedono ai fornitori di servizi informatici di essere reperibili per ricevere comunicazioni di attività illegali e bloccare i servizi o cancellare i file pertinenti.

12.15.1.6 Codice dell'amministrazione digitale

Il D. Lgs. 82 del 2005 (Codice dell'amministrazione digitale, CAD) regolamenta le firme elettroniche e digitali e stabilisce come i documenti in formato elettronico debbano essere considerati da un punto di vista legale. Esso non riguarda solo l'amministrazione pubblica, ma tutte le organizzazioni.

Alcune definizioni utili.

Documento elettronico: qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva [dal Regolamento eIDAS].

Documento informatico: il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti [dal CAD].

Documento analogico: la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti [dal CAD].

Il CAD regolamenta anche le modalità con cui gestire le copie (da formato informatico a formato analogico, oppure viceversa, oppure su medesimo tipo di formato) in modo da garantirne l'autenticità.

Le regole tecniche collegate al CAD sono pubblicate come DPCM (Decreti della Presidenza del Consiglio dei ministri) o dall'Agenzia per l'Italia digitale (AgID)¹²⁵.

12.15.1.7 Regolamento eIDAS e servizi fiduciari

Nel 2014 è stato approvato il Regolamento UE 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari. Questo regolamento è in vigore dal 2016.

Esso regolamenta alcuni cosiddetti servizi fiduciari o trusted services: firme elettroniche, sigilli elettronici (assimilabili a firme elettroniche di tipo aziendale e non personale), marche temporali elettroniche, servizi elettronici di recapito certificato (SERC o registered email o REM), in Italia già offerti dalla PEC, certificati di autenticazione di siti web e conservazione di firme, sigilli e certificati elettronici. Sono in fase di analisi le estensioni ad altri servizi, per esempio per la blockchain, la conservazione a lungo termine, il portafoglio di identità digitale.

Il Regolamento europeo, avendo valenza superiore rispetto alle normative nazionali, ha costretto il Governo italiano ad apportare delle modifiche al CAD.

Le aziende che offrono i servizi oggetto del Regolamento eIDAS devono quindi conformarsi a quanto previsto dal Regolamento stesso (questo richiede anche

l'adozione di standard tecnici specifici emessi da ETSI e la certificazione da parte di enti terzi). Le aziende che usufruiscono dei servizi oggetti del Regolamento eIDAS devono accertarsi che i fornitori siano accreditati dall'Agenzia per l'Italia digitale.

In Italia sono offerti ulteriori servizi di tipo fiduciario, oltre a quelli previsti dal Regolamento eIDAS, anche se questo termine non può essere usato. Essi sono quelli di: conservazione a lungo termine dei documenti informatici, lo SPID (sistema pubblico di identità digitale) e la PEC (posta elettronica certificata). I fornitori di tali servizi devono soddisfare regolamenti specifici stabiliti da AgID¹²⁶. Alcuni è probabile che saranno inclusi nel Regolamento eIDAS in suoi futuri aggiornamenti.

12.15.1.8 Conservazione a lungo termine

In Italia la conservazione a lungo termine dei documenti in formato digitale è regolata dall'Agenzia per l'Italia digitale, anche sulla base di alcune disposizioni del CAD. Questo prevede che le pubbliche amministrazioni conservino tutti i documenti seguendo specifiche regole tecniche. Sono stati progettati formati proprio per la conservazione a lungo termine, come il PDF/A descritto dalla ISO 19005.

Fornitori di servizi informatici possono offrire servizi di conservazione alla pubblica amministrazione, purchè rispettino alcuni requisiti.

L'obbligo di mantenere i documenti secondo certi standard si sta sempre più ampliando verso i privati. Inizialmente alcuni usavano i sistemi cosiddetti "a norma", per esempio per conservare le fatture elettroniche, per avere maggiori garanzie in caso di dispute. Successivamente questo approccio prudenziale è stato adottato per altri documenti e anche la normativa (in particolare il CAD,

aggiornate nel 2021 con il DL 76) tende ad estendere gli obblighi di conservazione “a norma” ai soggetti privati.

È importante mantenere la leggibilità dei documenti per tutto il tempo in cui devono essere conservati. Se le informazioni sono su supporti deperibili come la carta, è necessario siano conservate in archivi con le opportune misure di sicurezza e di controllo della temperatura e dell’umidità. Se le informazioni sono in formato digitale, bisogna garantire la disponibilità dei programmi software per leggerle e, se questi non sono più disponibili, stabilire regole per convertirle in altri formati. Un’altra opzione prevede di creare i documenti e le registrazioni direttamente in formati progettati per la conservazione a lungo termine, come il PDF/A descritto dalla ISO 19005.

12.15.1.9 Normativa sui dati personali (Privacy)

Il riferimento principale in materia di trattamento dei dati personali in Italia è il Regolamento europeo 2016/679 (detto General data protection regulation o GDPR). Alcune specifiche italiane sono oggetto del D. Lgs. 196 del 2003, aggiornato con il D. Lgs. 101 del 2018 a seguito dell’entrata in vigore del GDPR.

In questo paragrafo sono fornite solo linee generali su questa normativa, che deve essere approfondita da chi si occupa di sicurezza delle informazioni. Si ricorda che in Italia è disponibile molta letteratura [10, 65, 121, 153]¹²⁷.

La normativa distingue tra dati personali, dati personali appartenenti a categorie particolari (in precedenza, in Italia, erano detti personali sensibili) e dati personali relativi a condanne penali e reati (in precedenza, in Italia, detti dati personali giudiziari). Il loro trattamento deve avvenire su basi legali, elencate dal GDPR.

Per una migliore interpretazione del GDPR, sono da considerare le opinioni, raccomandazioni e linee guida dell’European Data Protection Board o EDPB¹²⁸ (per esempio quelle sull’uso di dispositivi video e in particolare sulla videosorveglianza). In Italia hanno inoltre valore le linee guida, le autorizzazioni e i provvedimenti generali del Garante per la protezione dei dati personali (Garante privacy)¹²⁹, in particolare quelli sulla gestione degli Amministratori di sistema. Sono stati pubblicati anche Provvedimenti per settori specifici come banche e strutture sanitarie.

Anche alcuni documenti di ENISA, l’Agenzia europea per la sicurezza informatica, possono essere utili per approfondire la materia [42].

Quando si progetta e mantiene un sistema di gestione per la sicurezza delle informazioni è necessario considerare i ruoli, le responsabilità e le misure di sicurezza richieste dalla normativa. Queste includono l’autorizzazione delle persone che trattano di dati personali e la gestione dei rapporti con fornitori e partner anche residenti all’estero (titolari, contitolari o responsabili). Per alcune organizzazioni è anche necessario nominare il responsabile della protezione dei dati (o data protection officer o DPO).

Le persone a cui si riferiscono i dati sono detti interessati e devono essere informati delle finalità per cui i dati sono trattati. Questa informativa stabilisce i limiti ai trattamenti che un’organizzazione può fare sui dati; deve essere pertanto attuata. In alcuni casi, il trattamento deve avvenire solo a seguito di esplicito consenso da parte degli interessati.

Tutti i trattamenti svolti vanno riportati in un particolare inventario, detto registro dei trattamenti. Le informazioni da riportare in questo registro sono prescritte dal GDPR.

Gli interessati possono poi esercitare dei diritti (accesso, cancellazione, limitazione e altri), per cui un'organizzazione deve stabilire processi in modo da assicurare la corretta elaborazione delle richieste.

Esempio 12.15.1. Sono molti gli esempi di trattamenti illeciti dei dati personali. I più diffusi sono:

utilizzo dei dati dei clienti per campagne di marketing, quando invece sono stati raccolti per fornire assistenza o per vendere un servizio a distanza (per esempio tramite Internet);

registrazione delle attività dei dipendenti, senza averli informati, per analizzarne la produttività.

Il GDPR richiede che l'organizzazione attui misure di sicurezza “adeguate”, considerando i rischi. Va quindi condotta una valutazione del rischio relativo alla privacy, che potrebbe essere integrata con quella relativa alla sicurezza delle informazioni. In questo caso va ricordato che gli impatti vanno valutati in modo diverso considerando quelli per l'organizzazione e quelli per gli interessati. Alcuni pensano che vadano sempre condotte due valutazioni del rischio distinte. Ogni organizzazione deve stabilire l'approccio da seguire considerando il proprio contesto.

Una misura importante riguarda l'obbligo di comunicare le violazioni ai dati personali al Garante e, nei casi in cui l'impatto potrebbe essere elevato per i diritti e le libertà delle persone fisiche, agli interessati. Un'altra riguarda il diritto di avere i propri dati cancellati, sempre che questi non debbano essere mantenuti per soddisfare obblighi di legge (come, per esempio, le fatture che devono essere

conservate per 10 anni), estesa poi al diritto all’oblio¹³⁰. Devono essere tutte considerate quando si progetta il sistema di gestione per la sicurezza delle informazioni.

Per alcuni trattamenti, ritenuti “rischiosi” dalla normativa, è richiesta una valutazione del rischio specifica, denominata Valutazione d’impatto sulla protezione dei dati o privacy impact assessment o PIA. Qualcuno sostiene che la valutazione del rischio relativo alla privacy (vedere sopra) è l’insieme delle PIA condotte per tutti i trattamenti.

Il GDPR pone limiti al trasferimento dei dati personali al di fuori dello Spazio economico europeo, che vanno quindi rispettati. A questo proposito è significativo il fatto che molti Paesi, inclusa la Cina, hanno approvato normative sulla privacy simile a quella europea.

Vale la pena ricordare che molte società hanno promosso corsi, consulenze e certificazioni sin dalla pubblicazione di una prima bozza del GDPR a inizio 2012. Persone competenti e non avide avrebbero dovuto evitare di fare queste proposte e ricordare che il testo finale sarebbe potuto essere molto diverso dalla bozza, come infatti è stato. Tale fretta, da parte di clienti troppo ansiosi e di consulenti incompetenti o avidi, si è vista anche in altri ambiti (per esempio a fronte di proposte, anche successivamente decadute, di modifica del D. Lgs. 231 del 2001). La sicurezza delle informazioni richiede maggiore prudenza e discernimento negli investimenti.

Il GDPR è accompagnato dalla Direttiva 2016/680 per i dati trattati dalle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali. Tale Direttiva è stata recepita nell’ordinamento italiano con il D.Lgs. 51 del 2018.

12.15.1.10 Normativa sulle infrastrutture critiche e il cybersecurity act

Relativamente alla sicurezza delle infrastrutture critiche, inizialmente, sulla spinta della Direttiva europea 2008/114/CE, fu approvato il D. Lgs. 61 del 2011 per identificare le cosiddette infrastrutture critiche e promuovere strumenti di protezione. Per tanti motivi, nonostante l'importanza di tali normative e l'impegno di tanti professionisti del settore, le disposizioni non trovarono mai un'efficace attuazione.

Successivamente fu quindi approvata la Direttiva europea 2016/1148, detta NIS o Network and information security, per gli operatori di servizi essenziali (OSE) e dei fornitori di servizi digitali (digital service provider o DSP) come mercati, motori di ricerca e cloud. Essa fu recepita in Italia dal D. Lgs. 65 del 2018.

Per meglio attuare la Direttiva NIS, considerando che non copriva tutti i settori critici, in Italia fu approvato il DL 105 del 2019, poi convertito con la Legge 133 del 2019, che stabilisce il “perimetro di sicurezza nazionale cibernetica”¹³¹.

L'impianto normativo, dimostrando l'acquisita importanza della materia, si è arricchito negli anni con:

DM del 12 dicembre 2018 specifico per i fornitori di reti e servizi di comunicazione elettronica;

DPCM 8 agosto 2019 per costituire il CSIRT italiano¹³²;

DPCM 131 del 2020 che stabilisce come vengono identificati i soggetti che esercitano funzioni essenziali e servizi essenziali, ossia i “soggetti inclusi nel perimetro”;

DPR 54 del 2021 per definire le modalità con cui gli enti designati (CVCN e CV) devono valutare i prodotti e servizi informatici acquisiti dai soggetti nel perimetro e pubblicare le caratteristiche per la valutazione di tali prodotti e servizi e i relativi dei test di sicurezza;

DPCM 81 del 2021 che specifica come i soggetti che esercitano funzioni essenziali e servizi essenziali devono comunicare gli incidenti che hanno impatto sui loro sistemi informatici e le misure di sicurezza che devono adottare;

DL 81 del 2021 (convertito con la Legge 109 del 2021) che istituisce l’Agenzia per la cybersicurezza nazionale (ACN) che diventa il punto di riferimento per ricevere le comunicazioni degli incidenti di sicurezza informatica con impatto sugli OSE, i DSP e sui soggetti che esercitano funzioni essenziali e servizi essenziali, assume il ruolo di Autorità nazionale di certificazione della cybersicurezza, incorpora il CVCN, incorpora il CSIRT Italia e diventa punto di riferimento per numerose attività relative alla sicurezza delle informazioni.

Agli OSE, ai DSP e ai soggetti inclusi nel perimetro sono state imposte misure minime di sicurezza, derivate dal CFS del NIST¹³³. Nel caso degli OSE e DSP, le misure richieste non sono pubblicate, mentre per i soggetti che esercitano funzioni essenziali e servizi essenziali, le misure di sicurezza sono specificate dal DPCM 81 del 2021.

12.15.1.11 Il Cybersecurity act

A livello europeo, per sostenere ulteriormente le iniziative di sicurezza, è stato emanato il Regolamento 881 del 2019, detto Cybersecurity Act, che stabilisce le responsabilità per ricevere e analizzare le informazioni in merito agli incidenti registrati presso gli OSE in tutta la UE e per sviluppare schemi di certificazione per la sicurezza dei prodotti e servizi informatici a livello europeo (anche recependo schemi già noti come i Common Criteria).

12.15.1.12 Normativa settoriale

Accanto alla normativa sopra citata e applicabile a tutte le organizzazioni, sono da ricordare alcuni dispositivi specifici:

Legge 124 del 2007 “Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto” e DPCM 4 del 22 luglio 2011 “Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate” (importanti anche il DPCM 5 del 2015 e il DPCM 3 del 2017 per le informazioni classificate);

D. Lgs. 259 del 2003 “Codice delle comunicazioni elettroniche” e D. Lgs. 109 del 2008, con disposizioni per gli operatori di telecomunicazioni (ulteriori disposizioni sono emesse dall’Autorità nazionale per le telecomunicazioni);

vari regolamenti per gli operatori del settore bancario, del credito o assicurativo, spesso rintracciabili presso i siti della Banca d’Italia o dell’IVASS.

Questa lista non è esaustiva. È compito di ciascuno informarsi e tenersi aggiornato sui provvedimenti relativi al settore in cui opera, per esempio attraverso associazioni professionali.

12.15.2 Contratti

Contratti da considerare e che bisogna rispettare, non solo in materia di sicurezza delle informazioni, sono quelli con:

clienti, con anche l’impegno di riservatezza reciproca, poiché i clienti vengono a

conoscenza di informazioni sui prodotti e servizi forniti; fornitori, che devono includere gli obblighi del fornitore (vedere paragrafo 12.12.1) e del cliente (per esempio in materia di proprietà intellettuale del fornitore o delle responsabilità del cliente in caso di incidente); assicurazioni (vedere paragrafo 12.12.6).

È necessario stabilire opportuni processi di comunicazione tra chi vende, chi si occupa degli acquisti, chi progetta i servizi e i prodotti, chi li realizza e chi li tiene in esercizio in modo che sia assicurata l'attuazione di quanto concordato sui contratti.

Per quanto riguarda le attività di vendita, quando possibile, si possono stabilire modelli di contratto, in modo da non dover decidere di volta in volta quali misure di sicurezza includere nei contratti. Vanno anche identificate quali sono le funzioni da coinvolgere nel caso in cui sia necessario deviare dal modello di contratto stabilito.

12.15.3 Audit

In questo paragrafo si esaminano brevemente gli audit e i requisiti di sicurezza da considerare durante gli audit.

12.15.3.1 L'attività di audit

La definizione di audit è fornita da diversi standard internazionali come segue.

Audit: processo sistematico, indipendente e documentato volto all'ottenimento di prove, al fine di valutarle per determinare quanto i criteri di audit sono soddisfatti.

I criteri di audit sono l'insieme di politiche, procedure e requisiti su cui basare l'audit. È necessario definire i tre tipi di audit e i relativi criteri:

interni o di prima parte: sono svolti dall'organizzazione stessa (con personale interno o esterno) e i criteri di audit sono le procedure interne;

esterni di seconda parte: sono svolti da una parte interessata (solitamente un cliente) presso un'organizzazione (solitamente un proprio fornitore) e i criteri di audit sono gli accordi o i contratti tra le parti;

di certificazione o di terza parte: sono svolti da organismi indipendenti e i criteri di audit sono gli standard concordati dall'organizzazione con l'organismo di certificazione.

Il termine audit differisce da quello di assessment perché l'audit è orientato a verificare se sono soddisfatti requisiti completamente stabiliti a priori, mentre l'assessment può fare riferimento a requisiti non completamente predeterminati.

Degli audit interni e ai fornitori, se ne discute nel paragrafo 15.9.2.

Gli audit di terza parte possono essere condotti secondo standard o norme come la ISO 9001 e la ISO/IEC 27001, le specifiche PCI¹³⁴, la SSAE 16 o la ISAE 3402 dell'AICPA. Altri audit importanti sono effettuati dai revisori dei conti o da altri soggetti simili.

Relativamente agli audit di terza parte, in appendice C si trovano alcuni elementi su quelli di certificazione rispetto a norme come la ISO/IEC 27001 o la ISO 9001.

12.15.3.2 La sicurezza durante gli audit

Gli audit possono presentare rischi, visto che gli auditor possono commettere errori o essere malintenzionati. Essi quindi devono essere trattati sempre come visitatori quando accedono ad aree fisiche e sistemi informatici dell’organizzazione. Nel caso in cui l’audit sia condotto da un’entità esterna, devono essere stabiliti rapporti simili a quelli clienti-fornitori, stipulando un accordo con le misure di sicurezza da garantire da ambo le parti.

Gli auditor (in particolare i revisori dei conti) potrebbero richiedere di connettersi ai sistemi per effettuare analisi o raccogliere dati. In questi casi la prima regola è quella di assegnare autorizzazioni di sola lettura ai dati. È anche necessario prestare attenzione agli strumenti utilizzati, visto che sono da garantire le stesse misure di sicurezza stabilite per i sistemi del personale interno (è interessante notare come certi auditor utilizzino personal computer senza antivirus, con attivi software di peer-to-peer o senza un sistema di controllo accessi attivo). In alcuni casi può essere imposto all’auditor l’uso di un computer predisposto appositamente dall’organizzazione.

Gli auditor potrebbero voler verificare i comportamenti dei sistemi e quindi interagire con essi. In questi casi è sempre opportuno che le operazioni vengano svolte dagli amministratori di sistema, non dall’auditor. Nel caso di vulnerability assessment (vedere il paragrafo successivo), per avere maggiori garanzie in merito alla sicurezza delle attività, l’organizzazione dovrebbe anche verificare le competenze del personale addetto.

Si deve concordare con gli auditor esterni, prima dell'inizio dell'audit, se è loro consentito conservare i documenti dell'organizzazione dopo la conclusione dell'audit. Come regola generale, se sono fornite copie dei dati, è opportuno chiederne la cancellazione al termine delle attività.

Un caso speciale è quando le autorità (per esempio la Guardia di finanza) si presenta presso l'organizzazione per indagini. In questo caso, dovrebbero essere state fornite istruzioni a tutto il personale almeno su come accogliere i visitatori (per esempio facendoli accomodare in una sala specifica, vicino all'ingresso), chi contattare (per esempio la Direzione e l'ufficio legale), accompagnarli sempre e prendere nota delle loro azioni e dei documenti a loro consegnati.

12.15.4 Vulnerability assessment

Il vulnerability assessment consiste nell'analisi dei sistemi informatici (solitamente negli ambienti di produzione e test) e nella ricerca e valutazione delle eventuali vulnerabilità presenti. Essi possono riguardare l'infrastruttura (sistemi e rete) o le applicazioni.

I vulnerability assessment possono essere condotti in diverse modalità: si può simulare un attaccante con conoscenza dei sistemi (white box) o senza alcuna conoscenza (black box); oppure un attaccante con ruolo di utente interno, o di utente esterno, o di "normale" utente Internet; il test può essere condotto a tavolino, o direttamente sui sistemi; può essere condotto solo con strumenti automatizzati (vulnerability scanner) o con tecniche di attacco adottate da hacker con diverse competenze e risorse (penetration test); può essere condotto da personale dell'organizzazione o da esterni (normalmente detti ethical hacker o white hat).

Gli strumenti automatici potrebbero non evidenziare vulnerabilità poco diffuse,

ma garantiscono un buon livello di completezza dei test¹³⁵. D'altra parte, i penetration test richiedono un maggiore investimento economico e quindi sono spesso condotti solo sui sistemi più critici.

I penetration test possono essere condotti per analizzare una determinata applicazione informatica prima di renderla disponibile al pubblico e dovrebbero essere sempre effettuati, se possibile, sui sistemi installati nella loro configurazione operativa [11]. Quando un sistema è già in ambiente di produzione, il penetration test deve limitarsi a dimostrare l'esistenza di una via per concludere un attacco, senza concluderlo realmente.

Per verificare la sicurezza delle applicazioni, possono essere usati strumenti di analisi del codice statico (static application security testing o SAST o anche source code security analyzers) o dinamico (dynamic application security testing o DAST). I primi sono più utili nelle fasi di sviluppo, i secondi nelle fasi di test di integrazione e UAT.

Altri test possono essere predisposti per vedere come il personale reagisce a un tentativo di attacco; in questo caso il personale deve essere tenuto all'oscuro del test (bisogna però prestare attenzione a che non interpellino le forze dell'ordine!).

Per completezza, visto che i termini di sicurezza informatica non sono standardizzati e spesso assumono significati diversi in contesti diversi, si riportano le definizioni degli standard pertinenti [24].

Vulnerability assessment (VA): attività volta a determinare l'esistenza e la possibilità di sfruttare security flaws e debolezze dell'oggetto sottoposto a valutazione nel suo ambiente operativo (simulato);

Penetration test (PT): tecnica di test (non di dimostrazione, come la VA) volta a determinare se le potenziali vulnerabilità identificate sono effettivamente sfruttabili nell'ambiente operativo in cui opera l'oggetto sottoposto a valutazione.

L'attività complessiva di identificazione e valutazione delle vulnerabilità è quindi suddivisa in due parti: una teorica (il vulnerability assessment) e una sperimentale (il penetration test).

I test più rigorosi prevedono una prima analisi del codice delle applicazioni (code review) e dell'architettura dei sistemi, poi un assessment white box, quindi uno scanning automatico e infine un penetration test.

Un test rigoroso è molto oneroso. Per questo è sempre necessario stabilire il perimetro da considerare ed, eventualmente, per quali servizi o sistemi limitarsi a verifiche meno approfondite.

I test sono spesso affidati a società (o laboratori) specializzate. In Italia, Accredia ha promosso uno schema di certificazione (o, più propriamente, di accreditamento) per questi laboratori¹³⁶ e ne richiede l'utilizzo da parte dei fornitori di servizi fiduciari (paragrafo 12.15.1.7).

I rischi dei vulnerability assessment

Se si tenta di attaccare l'ambiente di produzione, è necessario che il personale addetto all'assessment sia molto preparato, visto che un errore può compromettere i sistemi. Anche l'utilizzo di strumenti apparentemente innocui come i vulnerability scanner può essere molto insidioso.

Se si usano fornitori esterni, è necessario stabilire contrattualmente le responsabilità reciproche (paragrafo 12.12).

I vulnerability assessment non informatici

Il termine vulnerability assessment è generalmente utilizzato per i sistemi informatici, ma può essere necessario verificare la sicurezza fisica o il comportamento del personale.

Alcuni test prevedono di simulare un attacco di social engineering.

Esempio 12.15.2. Si può simulare un malintenzionato telefonando a un utente dell'organizzazione e dicendo di essere un amministratore di sistema con un problema la cui soluzione necessita la password dell'utente per accedere ai sistemi.

L'utente dovrebbe rispondere di non essere autorizzato a fornire questa informazione. In caso contrario, si riscontra una vulnerabilità.

Ovviamente, il test va effettuato contattando più utenti, per stabilire se si tratta di una mancanza diffusa o relativa a un numero ristretto di persone. Sulla base dei dati raccolti, è possibile stabilire l'azione di trattamento pertinente.

12.15.5 Il riesame del sistema di gestione

Questo controllo è oggetto del paragrafo 15.9.3.

Note

⁶⁹A questo proposito c’è da chiedersi perché si siano diffuse espressioni come “appetito per il rischio”, “rilasciare un software”, “invocare dei piani”, “concludere uno step di progetto”.

⁷⁰Il Garante italiano: www.gpdp.it/; l’European Data Protection Board, EDPB: <https://edpb.europa.eu>

⁷¹Per esempio SANS Newsbyte, www.sans.org

⁷²<https://csirt.gov.it/>.

⁷³punto-informatico.it/3146710/PI/News/aruba-incendio-nella-farm.aspx.

⁷⁴Materiale è disponibile sul sito ENISA:
www.enisa.europa.eu/media/multimedia/material.

⁷⁵<https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19>.

⁷⁶Regio Decreto 11 luglio 1941, n. 1161.

⁷⁷<https://nordpass.com/most-common-passwords-list/>.

⁷⁸Come dimostra un Provvedimento del Garante privacy del 2016:
www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/6032975.

⁷⁹<https://technet.microsoft.com/windows-server-docs/security/securing-privileged-access/securing-privileged-access>.

⁸⁰www.computerworld.com/s/article/9114479/San_Francisco_hunts_for_mystery_city_network.

⁸¹ www.nowsecure.com/blog/2016/07/12/pokemon-go-security-risks-what-cisos-and-security-pros-need-to-know/.

⁸²Un'applicazione di utilità pericolosa: <https://codiceinsicuro.it/blog/quando-la-squia-e-la-tastiera-del-tuo-smartphone-il-caso-flash-keyboard/>. Uno degli esempi più recenti di pulizia dei software distribuiti:
<https://www.republicworld.com/technology-news/apps/google-removes-34-malware-infected-apps-from-play-store.html>.

⁸³Alcune sono <https://letsencrypt.org> e <http://wiki.cacert.org>.

⁸⁴Oggi è l’Agenzia per l’Italia Digitale, www.agid.gov.it.

⁸⁵<https://www.zdnet.com/article/how-to-securely-erase-hard-drives-hdds-and-solid-state-drives-ssds/>.

⁸⁶it.wikipedia.org/wiki/Wiki.

⁸⁷<https://makezine.com/2017/09/07/secure-your-raspberry-pi-against-attackers/> e www.schneier.com/blog/archives/2017/09/securing_a_rasp.html.

⁸⁸<https://nvd.nist.gov/ncp/repository>.

⁸⁹Un caso tra i tanti, anche se non più recente:
<https://krebsonsecurity.com/2010/04/mcafee-false-detection-locks-up-windows-xp/>.

⁹⁰<https://arstechnica.com/information-technology/2015/11/failed-windows-3-1-system-blamed-for-taking-out-paris-airport/>.

⁹¹Uno dei tanti articoli, per cui gli sviluppatori spendono metà del loro tempo a correggere gli errori: www.businessweekly.co.uk/hi-tech/14898-software-bugs-cost-more-than-double-eurozone-bailout.

⁹²Una delle librerie più note è OpenSSL: www.openssl.org.

⁹³Due articoli. Il primo: arstechnica.com/information-technology/2014/04/tech-giants-chastened-by-heartbleed-finally-agree-to-fund-openssl/. Il secondo: www.theregister.co.uk/2014/04/11/openssl_heartbleed_robin_seggelmann.

⁹⁴Un esempio molto buono è quello offerto dal CERT: www.securecoding.cert.org/confluence/display/seccode/SEI+CERT+Coding+Standards.

⁹⁵<https://www.darkreading.com/5-key-takeaways-from-the-solarwinds-breach/d/d-id/1339764>.

⁹⁶<https://www.darkreading.com/application-security/git-some-security-locking-down-github-hygiene/d/d-id/1330511>.

⁹⁷<https://www.nomoreransom.org>.

⁹⁸Tra i più noti in Italia si citano quello dell'INRiM e dell'NTP Pool Project.

⁹⁹Uno dei tanti articoli: <https://www.darkreading.com/attacks-breaches/attackers-wage-network-time-protocol-based-ddos-attacks/d/d-id/1141112>.

¹⁰⁰ <https://medium.com/@kaistinchcombe/decentralized-and-trustless-crypto->

[paradise-is-actually-a-medieval-hellhole-c1ca122efdec.](#)

¹⁰¹Questo caso del 2013 è uno dei tanti:
associazionecindi.wordpress.com/2013/02/28/diffamazione-facebook-giplivorno.

¹⁰²<https://www.varonis.com/blog/the-dangers-of-shared-links/>

¹⁰³Per descrizione dell’attacco: <https://us-cert.cisa.gov/ncas/alerts/aa20-049a>; per la segnalazione della CISA:
www.theguardian.com/technology/2021/may/08/colonial-pipeline-cyber-attack-shutdown.

¹⁰⁴www.petri.co.il/cisco-ios-configuration-mistakes.htm.

¹⁰⁵<https://www.ncsc.admin.ch/ncsc/it/home/cyberbedrohungen/ceo-betrug.html>.

¹⁰⁶Sono numerosi gli esempi; questo è uno dei più gravi:
arstechnica.com/security/2013/01/secret-backdoors-found-in-firewall-vpn-gear-from-barracuda-networks.

¹⁰⁷www.cyberscoop.com/verizon-wireless-s3-bucket-public-access-kromtech.

¹⁰⁸Un famoso attacco è quello a Solarwinds di fine 2020:
<https://www.schneier.com/blog/archives/2020/12/russias-solarwinds-attack.html>.

¹⁰⁹Un attacco famoso, la cui attendibilità è però contestata, è del 2018:
<https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies>.

¹¹⁰<https://www.infosecurity-magazine.com/news/us-warns-of-supply-chain-attacks/>.

¹¹¹<https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem>.

¹¹²https://www.schneier.com/blog/archives/2019/09/on_cybersecurit.html.

¹¹³Un esempio del 2012: www.h-online.com/security/news/item/No-patch-for-critical-Oracle-database-vulnerability-1649106.html.

¹¹⁴Tra le più autorevoli: [www.sans.org/newsletters/risk e seclists.org/fulldisclosure](http://www.sans.org/newsletters/risk/seclists.org/fulldisclosure).

¹¹⁵www.chron.com/disp/story.mpl/front/6250411.html.

¹¹⁶www.bbc.com/news/technology-27322946.

¹¹⁷www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2149222.

¹¹⁸www.altalex.com/documents/news/2017/01/23/email-ammissibile-come-prova-anche-senza-la-firma-elettronica-qualificata.

¹¹⁹<https://www.economist.com/business/2005/10/27/when-lightning-strikes>.

¹²⁰Per esempio, www.normattiva.it, www.agid.gov.it, www.agcom.it, www.garanteprivacy.it.

¹²¹Esempi di siti attivi da anni sono www.filodiritto.com, www.altalex.com e www.agendadigitale.eu; un sito, tra i tanti, chiusi, è www.complianceaziendale.com.

¹²²<https://www.acq.osd.mil/cmmc/index.html>.

¹²³<https://www.vda.de/en/topics/safety-and-standards/information-security/information-security-requirements.html>.

¹²⁴Una sentenza illustra meglio la questione:
<http://www.filodiritto.com/articoli/2017/01/segreto-industriale-l-importanza-delle-misure-di-protezione.html>.

¹²⁵www.agid.gov.it.

¹²⁶www.agid.gov.it/it/piattaforme/spid.

¹²⁷I testi italiani sono solo esemplificativi e non completamente verificati dall'autore di questo libro

¹²⁸<https://edpb.europa.eu>.

¹²⁹www.garanteprivacy.it.

¹³⁰Con spiacibili considerazioni come quelle relative al caso di morte:
<https://inno3.it/2018/07/26/eredita-digitale-che-fine-fanno-i-dati-dopo-la-morte/>.

¹³¹Il termine “cibernetica” è stato usato impropriamente per tradurre l’inglese “cyber”, già a sua volta nato nell’ambito della fantascienza e quindi criticabile. Purtroppo i legislatori e alcuni organi importanti continuano a reiterare l’errore, non osservando, tra l’altro, che, in inglese, la cibernetica (ossia la materia che studia i sistemi di comunicazione e controllo) è indicata con il termine “cybernetics” e nessuno direbbe “cybernetics security”

¹³²<https://csirt.gov.it>.

¹³³<https://www.nist.gov/cyberframework>.

¹³⁴www.pcisecuritystandards.org.

¹³⁵Vedere anche <https://www.linkedin.com/pulse/awesome-truth-vulnerability-scanners-pete-herzog?articleId=7243169196393738733>.

¹³⁶www.accredia.it/servizio-accreditato/vulnerability-assessment/.

Parte IV

I requisiti di un sistema di gestione per la sicurezza delle informazioni

Capitolo 13

Le norme ISO e l'HLS

Together we stand,

divided we fall.

Pink Floyd, Hey you

L'ISO può essere visto come un editore che pubblica libri scritti non da singoli autori ma da gruppi di esperti designati dagli organismi nazionali di normazione. Si ricorda che norme e standard non sono pubblicati solo dall'ISO, ma anche da altri organismi di normazione nazionali, internazionali o privati.

13.1 Specifiche e linee guida

Si distingue tra diversi tipi di norme, definiti come segue.

Standard verificabili: norme con specifiche rispetto alle quali può essere condotto un audit da parte di personale indipendente; si riconoscono perché è utilizzato il verbo ausiliario shall in inglese e deve in italiano;

Linee guida: manuali o raccolte di best practice disponibili per una loro selezione al fine di raggiungere un certo obiettivo; si riconoscono perché sono

utilizzati i verbi ausiliari should, can e may in inglese e dovrebbe, può e potrebbe in italiano.

Le norme possono riguardare: prodotti, servizi, sistemi organizzativi (o sistemi di gestione), competenze delle persone. Possono essere pertinenti a tutti i settori delle attività, come è possibile intuire dalla lettura di alcuni elenchi [104], anche se difficilmente completi a causa della continua evoluzione del mercato.

Le norme spesso nascono dalle cosiddette best practice, molto numerose. Nel tempo, le migliori tra esse diventano standard de facto perché un gran numero di organizzazioni le adotta spontaneamente, ritenendole preferibili ad altre o a soluzioni proprietarie. Il passaggio a norma nazionale o internazionale, in alcuni casi, è particolarmente semplice, dato che l'ISO, International Organization for Standardization, si limita a rimuovere il vecchio identificativo e a darne uno nuovo.

Gli standard verificabili sui sistemi di gestione sono numerosi. La ISO 9001, relativa alla qualità, è quella più famosa e diffusa; a seguire per diffusione sono la ISO 14001 relativa all'ambiente e la ISO 45001 relativa alla salute e sicurezza sul lavoro. La ISO/IEC 27001 sulla sicurezza delle informazioni e la ISO/IEC 20000-1 sulla gestione dei servizi IT sono altri standard di sistemi di gestione abbastanza diffusi e noti. Recentemente sono stati pubblicati e si stanno diffondendo altri standard di sistemi di gestione, tra cui la ISO 22301 sulla continuità operativa, la ISO 28000-1 sulla sicurezza della filiera di fornitura e la ISO 50001 sulla gestione energetica.

13.2 Le norme della famiglia ISO/IEC 27000

La ISO/IEC 27001 è uno standard verificabile; oltre che dall'uso del verbo shall,

lo si capisce dal titolo, che riporta in inglese Requirements e in italiano Requisiti. Possono essere condotti audit di un sistema di gestione per la sicurezza delle informazioni di un'organizzazione e, se questo è ritenuto conforme ai requisiti della ISO/IEC 27001, può essere emesso un certificato di conformità. In appendice C si presenta sinteticamente il processo di certificazione.

La ISO/IEC 27001 è affiancata da linee guida che forniscono supporto all'attuazione dei suoi requisiti o indicazioni per la sua applicazione in settori specifici. L'insieme di queste norme è detto famiglia delle norme ISO/IEC 27000 (ISMS standard family o famiglia di norme dei SGSI) e ne fanno parte:

ISO/IEC 27002, che descrive i controlli di sicurezza; non è possibile dichiarare una conformità rispetto a essa, ma alcune organizzazioni lo fanno e dimostrano quanto poco conoscano questo standard;

ISO/IEC 27003, guida all'interpretazione dei requisiti della ISO/IEC 27001;

ISO/IEC 27004, guida per la misurazione e il monitoraggio di un sistema di gestione per la sicurezza delle informazioni;

ISO/IEC 27005, guida per la gestione del rischio relativo alla sicurezza delle informazioni (purtroppo, anche per questo alcuni chiedono la certificazione o attestati di conformità).

Altre norme della famiglia sono quelle che estendono i controlli della ISO/IEC 27001 (e, nel caso, possono essere citate sul relativo certificato). Ne fanno parte:

ISO/IEC 27011 con controlli di sicurezza per i fornitori di servizi di telecomunicazione;

ISO/IEC 27017 con controlli di sicurezza per i fornitori e gli utilizzatori di

servizi cloud;
ISO/IEC 27018 con controlli privacy per i fornitori di servizi cloud;
ISO/IEC 27019 con controlli di sicurezza per il settore dell'energia;
ISO 27799 con controlli di sicurezza per il settore della sanità.

Se un'organizzazione si certifica ISO/IEC 27001 e include i controlli di questi standard nella sua Dichiarazione di applicabilità (descritta nel paragrafo 15.6.3), può chiedere che siano citati sul certificato.

Esempio 13.2.1. Un'organizzazione che offre servizi cloud IaaS, può includere i controlli della ISO/IEC 27017 nella propria dichiarazione di applicabilità e quindi avere riportato sul certificato il seguente ambito: “Erogazione di servizi IaaS, con Dichiarazione di applicabilità estesa con i controlli della ISO/IEC 27017”.

13.3 ISO/IEC 27701

La norma ISO/IEC 27701, pubblicata a fine 2019, riguarda la certificazione del sistema di gestione per la protezione dei dati personali, e si è ispirata al Regolamento europeo sulla protezione dei dati personali (GDPR). Essa aggiunge alcuni requisiti e alcuni controlli alla ISO/IEC 27001.

È opportuno ricordare che il GDPR promuove la certificazione dei trattamenti (processing activity), seguendo le regole di certificazione di “prodotti, processi o servizi”, stabilite dalla ISO/IEC 17065. La ISO/IEC 27701, estendendo la

ISO/IEC 27001, permette di certificare, invece, un “sistema di gestione” con le regole fissate dalla ISO/IEC 17021 (con le aggiunte fornite dalla ISO/IEC 27006-2).

La differenza può sembrare minimale, ma si tratta comunque di due cose diverse. Molti però ritengono che la certificazione ISO/IEC 27701 avrà un tale successo che questo problema sarà sempre più irrilevante. Altri invece pensano che, quando le autorità garanti si pronunceranno su uno schema secondo quanto previsto dagli articoli 42 e 43 del GDPR, questo offuscherà la ISO/IEC 27701. I tempi sembrano però molto lunghi e il percorso non è del tutto delineato, anche se si sono avviate alcune iniziative a livello europeo.

13.4 L’HLS

Gli standard verificabili relativi ai sistemi di gestione pubblicati prima del 2012 spesso riportavano requisiti tra loro molto simili (in alcuni casi anche uguali), ma posti in paragrafi diversi o scritti in modo differente. In altre parole: mancava standardizzazione negli standard. Questo creò malcontento nelle organizzazioni che ne adottavano più di uno (per esempio, ISO 9001 e ISO/IEC 27001).

Nel 2009, quindi, il Technical Management Board (TMB) della ISO chiese al Joint Technical Coordination Group (JTCG) di stabilire uno schema comune per sviluppare gli standard sui sistemi di gestione. Si cominciò così a sviluppare il Common Structure and Identical Text for Management System Standards, noto anche come HLS o High level structure.

L’HLS contiene il testo di base da adottare per ciascun standard sui sistemi di gestione. Per esempio, quello relativo alla conduzione degli audit interni si trova nel paragrafo 9.2 e tutti gli standard devono riportarlo esattamente nella stessa

posizione e con le parole dell’HLS. Considerando le peculiarità di ciascun standard, è consentita l’aggiunta di testo per ciascuna disciplina.

Nell’ottobre 2010 il testo del HLS fu fatto circolare e successivamente annunciata la sua pubblicazione come ISO Guide 83 nel febbraio 2012.

A sorpresa, l’HLS venne pubblicato nel 2012 nell’Annex SL delle ISO/IEC Directives, Part 1, Consolidated ISO Supplement; in altre parole, fu pubblicato come direttiva, non come guida. Il testo era però immaturo in alcune sue parti e questo creò difficoltà nella redazione della seconda edizione della ISO/IEC 27001, che si concluse nel 2013. La ISO/IEC 27001 si basa quindi sul HLS, a cui fu aggiunto del testo relativo alla sicurezza delle informazioni, in particolare sulla valutazione e sul trattamento del rischio.

Dal 2012 al 2018, tutti gli standard sui sistemi di gestione furono aggiornati per recepire l’HLS.

Per il suo posizionamento nelle ISO/IEC Directives, molti riferimenti all’HLS riportano il termine Annex SL, certamente inappropriato perché dipendente dall’organizzazione del documento.

13.5 Storia della ISO/IEC 27001

La ISO/IEC 27001 nacque nel 1995 come BS 7799, ossia come norma nazionale britannica, dall’esigenza delle organizzazioni inglesi di avere un punto di riferimento comune per i controlli di sicurezza relativi alla sicurezza delle informazioni. Il British Standard Institute (BSI), collaborando con quelle organizzazioni, pubblicò il British Standard 7799 con titolo Information security

management - Code of practice for information security management. Esso riportava un insieme di controlli di sicurezza con linee guida per la loro realizzazione.

Linee guida (ISO/IEC 27002)

1995: BS 7799



BS 7799-1:1999

(ISO/IEC 17799:2000)



ISO/IEC 17799:2005

(ISO 27002:2005 nel 2007)



ISO/IEC 27002:2013



ISO/IEC 27002:2022

Requisiti (ISO/IEC 27001)

BS 7799-2:1998



BS 7799-2:1999



BS 7799-2:2002

(ISO/IEC 27001:2005)



ISO/IEC 27001:2013



ISO/IEC 27001:2022

Figura 13.5.1:

Storia della ISO/IEC 27001

Successivamente nacque l'esigenza di promuovere uno schema di certificazione relativo alla gestione della sicurezza delle informazioni, simile a quello adottato per la qualità con la sempre più diffusa ISO 9001. Per questo nel 1998 fu realizzato lo standard di requisiti BS 7799-2:1998 (con titolo Information security management systems - Specification) e la BS 7799 fu rinumerata BS 7799-1.

La BS 7799-2 era strutturata come l'attuale ISO/IEC 27001: una prima parte con i requisiti di sistema, oggetto del capitolo 15 del presente libro, all'epoca ridotti quasi alla sola richiesta di valutare il rischio, predisporre un piano di trattamento e una Dichiarazione di applicabilità (paragrafo 15.6.3). In una seconda parte, Annex o Appendice A, erano riportati i medesimi controlli di sicurezza della BS 7799-1, anche se molto riassunti e con il termine should sostituito con il termine shall. Alcuni riassunti, fatti evidentemente di fretta, non erano sempre esaustivi o coerenti con il titolo del controllo.

Nel 1999, le BS 7799-1 e BS 7799-2 furono riemesse aggiornate, soprattutto perché i precedenti controlli di sicurezza risultarono obsoleti a fronte dei notevoli progressi tecnologici di quegli anni. L'impostazione rimase la stessa: la BS 7799-1 riportava i controlli di sicurezza e la BS 7799-2, sinteticamente, i requisiti di sistema e una lista di controlli di sicurezza derivata dalla BS 7799-1.

Nel 2000, la BS 7799-1 fu recepita dal JTC1 dell'ISO/IEC attraverso una procedura di "fast track" e pubblicata come ISO/IEC 17799:2000. In sostanza si trattava della BS 7799-1 con un unico cambiamento: la numerazione. La BS

7799-2, a causa dell'eccessiva sintesi dei requisiti di sistema, era troppo dissimile dalle altre norme sui sistemi di gestione (per esempio la ISO 9001 sulla qualità e la ISO 14001 sull'ambiente) per poter essere recepita come standard ISO/IEC.

Purtroppo, la BS 7799-1 lo fu come norma relativa all'information technology, quando invece trattava di sicurezza delle informazioni non solo dal punto di vista informatico. L'orientamento tecnologico si notava in alcune descrizioni dei controlli di sicurezza.

Nel 2002 venne pubblicata una nuova versione della BS 7799-2, più allineata con la ISO 9001 e la ISO 14001: molti requisiti (per esempio, quelli sulle responsabilità della Direzione e quelli sulla gestione dei documenti, delle registrazioni, delle risorse, degli audit interni e delle azioni correttive e preventive) furono copiati direttamente da esse, anche se con qualche refuso. I requisiti relativi alla valutazione del rischio erano molto prescrittivi e specificavano nel dettaglio i passaggi da effettuare. L'Appendice A rimase esattamente come prima perché faceva riferimento alla ISO/IEC 17799:2000, anche se alcuni controlli ripetevano quanto già scritto nei requisiti di sistema, per esempio in merito alle responsabilità della Direzione e alla gestione del personale.

In questo modo si avviarono i lavori per recepire la BS 7799-2 da parte della ISO/IEC e si conclusero nel 2005 con la pubblicazione della ISO/IEC 17799:2005 e della ISO/IEC 27001:2005. La ISO/IEC 27001 non presentava sostanziali differenze rispetto alla BS 7799-2:2002.

Più interessanti le variazioni alla ISO/IEC 17799, soprattutto perché ora i controlli di sicurezza erano organizzati in modo da avere sin da subito quel "riassunto" da riportare nell'Annex A della ISO/IEC 27001 con la sola modifica del termine should con shall. Questo ridusse gli errori nell'Appendice A.

A fine 2008 si avviarono i lavori per una nuova edizione della norma e le discussioni furono soprattutto orientate sui seguenti dilemmi: mantenere o meno l'Appendice A e la Dichiarazione di applicabilità (paragrafo 15.6.3), ridurre o meno le prescrizioni relative alla valutazione del rischio, allineare maggiormente i requisiti alle altre norme ISO. L'adozione del HLS introdusse nuovi elementi di discussione anche per alcune difficoltà di interpretazione dei suoi requisiti, peraltro senza il supporto di altre esperienze di adozione dell'HLS. Infatti, i lavori di aggiornamento di norme più diffuse come l'ISO 9001 e l'ISO 14001 non erano ancora iniziati.

Si arrivò quindi alla nuova norma solo a fine 2013 dopo nove bozze.

Nel 2017, l'EN (European Normalization) adottò la ISO/IEC 27001:2013, ne cambiò solo la copertina e la nominò EN ISO/IEC 27001:2017. In questo modo, si poteva comprare la ISO/IEC 27001:2013 sul sito della ISO e la EN ISO/IEC 27001:2017 sul sito della EN e avere gli stessi identici documenti. Gli enti di normazione nazionali europei dovettero quindi recepire la versione della EN. Così in Italia (dove era già presente la versione UNI CEI ISO/IEC 27001:2014, datata 2014 per ritardi da parte di UNI) si ebbe la UNI CEI EN ISO/IEC 27001:2017, a sua volta uguale (se non per la traduzione e il titolo Sistemi di gestione per la sicurezza delle informazioni: Requisiti) alla ISO/IEC 27001:2013.

Quindi per la ISO/IEC 27001 furono indicati anni diversi, a seconda dell'ente di normazione che l'ha recepita, anche se si trattava dello stesso standard. Per la ISO 9001, invece, per ogni edizione gli enti cercano di adottarla nello stesso anno di pubblicazione da parte della ISO (anche quando questo avviene a dicembre, come accadde per la versione del 2000).

Nel 2022 fu pubblicata una nuova versione della ISO/IEC 27002, che rideuce i

controlli a 93, eliminando molte ridondanze, accorpando quelli troppo simili tra loro, dividendone alcuni e aggiungendone altri diventati necessari a causa dell’evoluzione della sicurezza delle informazioni (come quelli sul cloud) o inspiegabilmente non previsti nella precedente versione (come quelli sulla configurazione dei sistemi informatici). I controlli sono ora organizzati in soli 4 capitoli (o categorie), come approfondito all’inizio del capitolo 12.

Dopo la pubblicazione della nuova edizione della ISO/IEC 27002, nel 2022 fu pubblicato un emendamento (Amendment) della ISO/IEC 27001 per allineare l’Appendice A ai nuovi controlli, ma la norma rimase la ISO/IEC 27001:2013, seppure emendata. Si procedette infine al consolidamento delle due poco significative correzioni pubblicate nel 2014 e 2015 e dell’emendamento nella ISO/IEC 27001:2022.

13.6 Come funziona la normazione

La ISO/IEC 27001 è scritta da un gruppo di lavoro che fa riferimento alla ISO e alla IEC. La ISO (International organization for standardization) si occupa della standardizzazione in tutti i settori, mentre la IEC (International electrotechnical committee) è specializzata nell’ambito elettrotecnico. Fanno parte della ISO e della IEC gli Organismi nazionali (National bodies), uno per ciascuna nazione rappresentata.

La ISO/IEC 27001 è quindi responsabilità di due comitati internazionali e per questo è importante evitare di indicarla solo come ISO 27001.

Le attività congiunte di ISO e IEC, come quelle relative alla ISO/IEC 27001, sono coordinate da un comitato dal poco fantasioso nome di Joint technical committee 1, o JTC 1, a sua volta suddiviso in sottocomitati. Quello addetto alla

ISO/IEC 27001 ha nome sub-committee 27 o SC 27. A sua volta, l'SC 27 si suddivide in più gruppi di lavoro, ciascuno specializzato: il WG 1 (Working Group 1) si occupa dei sistemi di gestione per la sicurezza delle informazioni e quindi della ISO/IEC 27001, il WG2 di crittografia e meccanismi di sicurezza, il WG3 di valutazione, test e specifiche per la sicurezza (si occupa, tra le altre, della ISO/IEC 15408, nota come Common Criteria, di cui si parla brevemente in appendice D), il WG4 di controlli e servizi di sicurezza (in particolare, di norme tecniche sulla sicurezza, la digital forensics, l'IoT, eccetera) e il WG5 di privacy [99].

Ogni norma passa diversi stadi: working draft (WD), committee draft (CD), draft of international standard (DIS), final draft of international standard (FDIS) e può essere pubblicata come International standard (IS), Technical specification (TS) o Technical report (TR) a seconda del consenso necessario per la sua approvazione. La ISO/IEC 27001 è un International Standard ed è stato approvato da almeno il 75% degli organismi nazionali aventi diritto.

In Italia, gli organismi nazionali corrispondenti all'ISO e all'IEC sono l'UNI (Ente nazionale per l'uniformazione) e la CEI (Comitato elettrotecnico italiano), che hanno delegato Uninfo a rappresentarli nell'SC 27. Chiunque, pagando una quota di iscrizione, può partecipare ai lavori dell'SC 27 dell'Uninfo e ogni sei mesi, come delegato, agli incontri internazionali [150].

Va detto che la partecipazione italiana è ancora limitata e la nostra delegazione non riesce a seguire l'insieme dei lavori, soprattutto nel corso degli incontri internazionali plenari semestrali anche se questi, dal 2020, si svolgono online. In particolare, per l'edizione del 2013 della ISO/IEC 27001 parteciparono molto marginalmente l'organismo di accreditamento italiano, nessuno degli organismi di certificazione accreditati in Italia, nessuna delle medie o grandi società di consulenza italiane che vendono servizi relativi alla ISO/IEC 27001, nessuno della Pubblica Amministrazione o delle Autorità collegate come il Garante privacy (anche se poi emettono regolamenti o bandi di gara che fanno riferimento alla ISO/IEC 27001 o alla ISO/IEC 27002), quasi nessuno delle

nostre imprese più rappresentative. Per la versione del 2022, gli unici partecipanti furono due consulenti.

I motivi sono sicuramente tanti e tra di essi si può indicare il disinteresse tecnico per delle norme sfruttate solo per vendere servizi di consulenza o per mostrare il proprio certificato ISO/IEC 27001. Bisogna anche aggiungere il problema economico: i partecipanti devono pagare l'iscrizione a UNINFO, le spese di viaggio e soggiorno per i meeting semestrali nelle più disparate località del mondo (anche se questo non è più vero, almeno dal 2020). Infine, anche se con uno sconto, devono pagare per disporre delle edizioni finali delle stesse norme che hanno contribuito a scrivere.

Capitolo 14

Il miglioramento continuo e il ciclo PDCA

Turn!

Turn!

Turn!

Pete Seeger

Le norme ISO sui sistemi di gestione, tra cui quindi la ISO/IEC 27001, impongono alle organizzazioni che li adottano il miglioramento continuo, oggetto della prima parte di questo capitolo.

Nella seconda parte si tratta dello strumento fondamentale per il miglioramento, ossia il ciclo Plan-Do-Check-Act.

Il concetto di miglioramento e il ciclo PDCA, sebbene possano sembrare semplici, sono invece complessi.

14.1 Il miglioramento continuo

Il concetto di miglioramento continuo è stato introdotto negli anni Ottanta del Novecento in Giappone, nell'ambito del Total quality management o gestione

della qualità totale, ossia delle teorie e delle pratiche relative alle attività gestionali volte a migliorare la qualità dei prodotti e servizi offerti da un’organizzazione e ad accrescere la soddisfazione dei clienti.

Il principio su cui si basa la qualità totale è che ogni processo, più o meno direttamente, contribuisce alla qualità dei prodotti e servizi offerti. Si tratta quindi di migliorare tutti i processi di un’organizzazione. Il concetto sembra banale, ma spesso alcuni processi vengono trascurati e non si fanno investimenti per migliorarli.

Nell’ambito della sicurezza delle informazioni non si parla di soddisfazione dei clienti né del suo miglioramento, anche se gli incidenti potrebbero avere conseguenze sull’immagine. Dovrebbe essere comunque adottato il principio secondo cui la sicurezza delle informazioni migliora solo se migliorano tutti i processi a essa connessi.

Il termine “miglioramento” può sembrare in alcuni casi inappropriato, preferendogli il termine “adeguamento”: si adeguano i processi e i controlli di sicurezza ai rischi individuati e ai requisiti normativi e contrattuali; si migliorano quando si dimostrano inefficaci o si rilevano degli incidenti.

Nella pratica, le organizzazioni tendono a non modificare alcunché, se non quando costrette. Parte di questo atteggiamento è ascrivibile alla propensione di tutto il personale (inclusi i responsabili delle diverse funzioni) a svolgere le attività quotidiane, senza riflettere sull’efficacia di quanto stanno facendo o senza proporre modifiche. Si possono individuare altre ragioni, sovente indicate con l’espressione generale di “resistenza al cambiamento”: pigrizia mentale, paura di perdere potere o controllo a seguito dei cambiamenti, prudenza per evitare di offendere qualcuno, e così via.

Nel corso degli anni sono stati fatti molti studi su come affrontare i cambiamenti; i più noti sono quelli relativi al business process re-engineering (anche se quasi tutte le sue applicazioni sono state fallimentari) e al kaizen, ossia al cambiamento attraverso piccoli passi [49, 50, 100, 106].

È importante evitare di avviare miglioramenti non controllati perché potrebbero introdurre ulteriori rischi. Oltre agli ovvi rischi dovuti al cambiamento di strumenti, è necessario considerare anche quelli dovuti alle inevitabili inefficienze che si presentano almeno nei primi tempi. Sono poi numerosi i casi in cui il cambiamento è talmente male organizzato che le inefficienze e le vulnerabilità permangono anche per lungo tempo.

Esempio 14.1.1. A marzo 2020, quando iniziò l'emergenza COVID, il Ministero dell'istruzione chiese alle scuole di avviare attività di didattica a distanza, suggerendo anche alcuni strumenti per questo fine.

Purtroppo fu fatta molta confusione: non furono fornite istruzioni per utilizzare gli strumenti suggeriti, gli strumenti non furono analizzati in merito ai loro impatti sulla privacy, non furono fornite indicazioni agli insegnanti su come organizzare le video lezioni (che non possono, ovviamente, essere organizzate come quelle dal vivo), non fu considerato l'impatto sulle famiglie con scarse competenze informatiche o con più figli a cui assicurare la connessione anche nello stesso momento.

Problemi simili si presentano nelle organizzazioni che introducono nuovi strumenti senza istruire completamente il personale, che, cercando di sopperire a queste mancanze, potrebbe introdurre nuove vulnerabilità.

Questo esempio dimostra anche che gli strumenti digitali non risolvono i

problemi e, anzi, potrebbero introdurne di nuovi.

Il ciclo PDCA, a cui è dedicato il paragrafo seguente, non è un metodo per gestire i cambiamenti, ma uno schema per identificarli e tenerli sotto controllo.

14.2 Il ciclo PDCA

Il ciclo PDCA o Plan-Do-Check-Act è uno strumento per conseguire il miglioramento e si può applicare a tutte le organizzazioni, processi e attività. È noto come ciclo di Deming, dal nome della persona che lo ha reso noto e popolare prima in Giappone e poi nel mondo.

Il ciclo (figura 14.2.1) è così composto:

pianificare (plan): individuare le attività, i processi e gli strumenti da utilizzare per conseguire i risultati previsti;

realizzare (do) quanto pianificato;

verificare (check) quanto realizzato rispetto a quanto pianificato;

intervenire (act) se a fronte delle verifiche si individuano carenze.



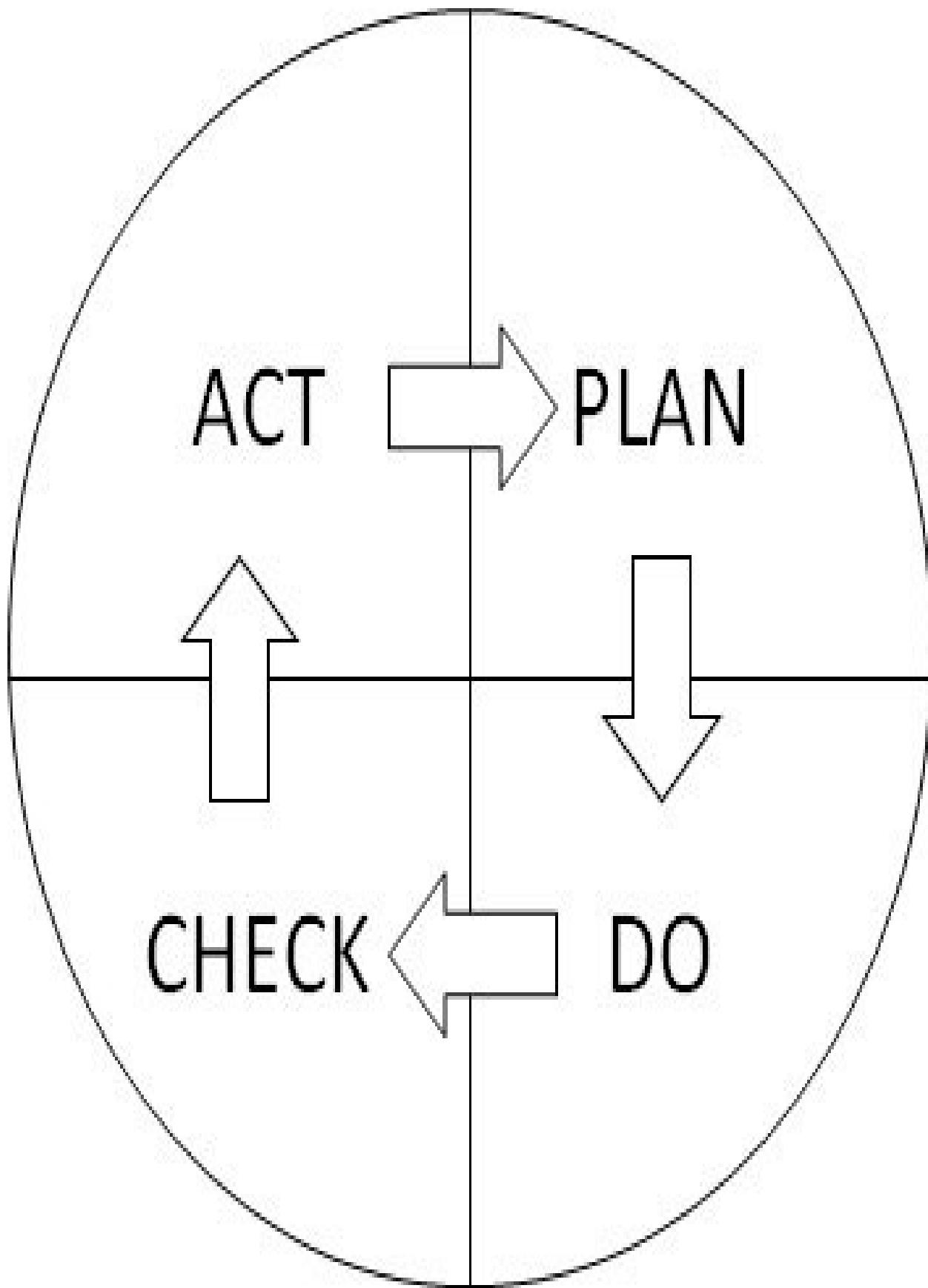


Figura 14.2.1:

Il ciclo PDCA

Sembra si tratti di un ciclo banale. In effetti, è semplice da capire, ma nella pratica è applicato parzialmente oppure frainteso, come illustrato nei paragrafi successivi.

Al termine, si discute brevemente della natura frattale del ciclo PDCA.

14.2.1 Pianificare

Questa fase del ciclo PDCA è spesso fraintesa: quando si chiede di pianificare, non necessariamente si chiede di predisporre piani molto dettagliati con ogni fase da completare. Il dettaglio della pianificazione dipende dalla dimensione e criticità del progetto: in alcuni casi sono utilizzati dei bigliettini su una lavagna, spostati manualmente ogni volta che le attività progrediscono, come si vede nella figura 14.2.2. La pianificazione deve comunque evidenziare tutte le attività da completare e le loro interrelazioni, in modo da non avere conflitti tra di esse.



Figura 14.2.2:

Una lavagna con bigliettini per l'avanzamento delle attività

La pianificazione riguarda tutti i livelli dell'organizzazione (piramide di Anthony, paragrafo 4.2):

a livello strategico si pianificano le attività a lungo termine e le caratteristiche generali dei prodotti e dei processi;

a livello tattico si pianificano i miglioramenti di dettaglio dei processi;

a livello operativo si pianificano le attività quotidiane necessarie alla produzione o all'erogazione dei servizi.

14.2.2 Fare

Questa fase è quella che trova sempre attuazione e consiste nel realizzare quanto pianificato.

In molti casi, quando la pianificazione è carente, la realizzazione risulta a sua volta di scarsa qualità o più costosa di quanto lo sarebbe stata se si fosse prestata maggiore attenzione alla pianificazione.

14.2.3 Verificare

Questa fase consiste nel verificare che quanto fatto sia efficace. Per questo, è opportuno riportare la seguente definizione della ISO/IEC 27000.

Efficacia: grado rispetto al quale le attività pianificate sono realizzate e i risultati pianificati raggiunti.

Le verifiche, nel caso di progetti o produzioni complesse, non andrebbero effettuate solo al termine dei lavori, ma anche in fasi intermedie, per risolvere tempestivamente eventuali difficoltà.

Questa fase è spesso ignorata o sottovalutata: nella pratica si discute spesso su cosa fare, senza analizzare successivamente se quanto deciso è stato attuato efficacemente. Non sono rari i casi in cui sono varati nuovi organigrammi, fornite indicazioni strategiche e richieste modifiche ai processi senza che poi ne sia verificata l'efficacia, salvo quando si evidenziano risultati negativi; a livello operativo, sovente i test sono condotti con superficialità e questo ha come risultato la realizzazione di prodotti e l'erogazione di servizi difettosi.

Le verifiche vanno stabilite nella fase di pianificazione, per decidere quando farle (per esempio, al termine di ogni fase di progetto o attraverso monitoraggi continui) e come farle.

Come già accennato, il motivo principale per cui si sottovaluta questa fase è la continua attenzione al quotidiano e la conseguente difficoltà a trovare il tempo per verificare cose decise tempo addietro. Forse un altro motivo potrebbe essere la paura di mettersi in discussione, nel caso in cui un progetto non abbia portato i benefici desiderati.

Quando si tratta di strategie e di tattiche, i testi dedicati al governo di impresa [68] indicano come la verifica e il monitoraggio siano di responsabilità di coloro che le hanno stabilite, ossia della governance (figura 14.2.3).

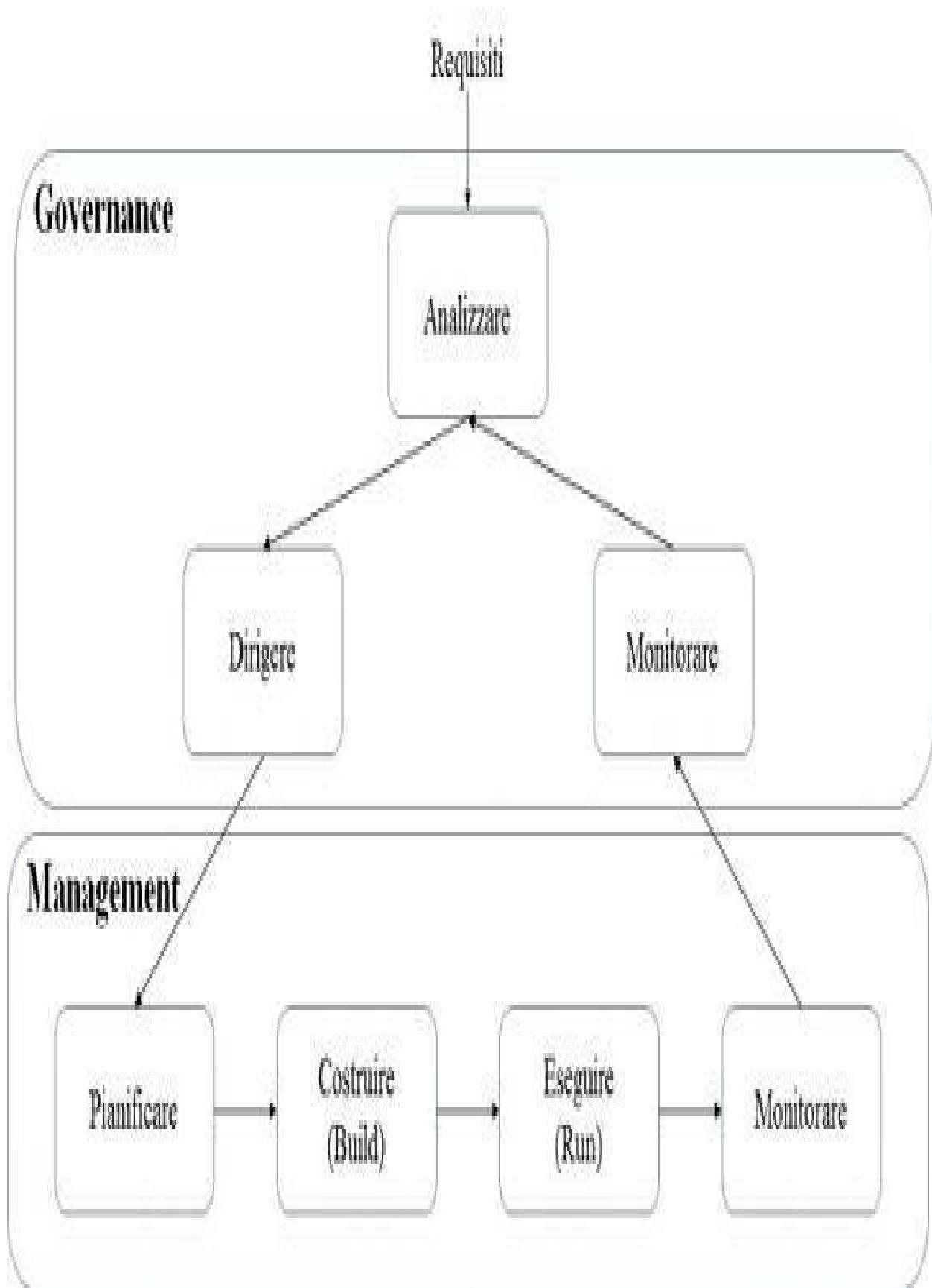


Figura 14.2.3:

Schema di governance e management [68]

14.2.4 Intervenire

Se nella pratica le verifiche sono svolte sporadicamente, gli interventi successivi sono molto più rari, nonostante siano fondamentali.

Alcune volte gli interventi devono essere effettuati quando si individuano errori o situazioni impreviste, altre volte quando si individuano degli elementi da migliorare.

Esempio 14.2.1. A livello strategico, si potrebbero modificare le strategie e gli obiettivi strategici dopo aver analizzato il loro andamento per un certo periodo di tempo.

A livello tattico, dopo aver modificato un processo e verificato se il personale lo esegue in modo efficace, si potrebbe evidenziare la necessità di apportare cambiamenti a: modelli di documento difficili da compilare, modalità di comunicazione tra le funzioni coinvolte, controlli intermedi troppo onerosi, eccetera.

A livello operativo, al termine dei test si potrebbe decidere di: rilavorare parzialmente o totalmente quanto prodotto a causa dei difetti riscontrati oppure, coinvolgendo il livello tattico, modificare alcune caratteristiche del prodotto o servizio.

Gli interventi non devono mai essere orientati a individuare un colpevole. Questo atteggiamento porta a nascondere i problemi. Uno dei principi del miglioramento è che si verificano sempre errori (o non conformità): un'organizzazione virtuosa non è quella senza errori, ma quella che li sa gestire al meglio ed evita di ripeterli.

14.2.5 La natura frattale del ciclo PDCA

Ognuna delle quattro fasi del ciclo PDCA deve essere a sua volta oggetto di un ciclo PDCA, così come illustrato in figura 14.2.4. Essa illustra, seppure molto schematicamente, la natura frattale del ciclo PDCA.

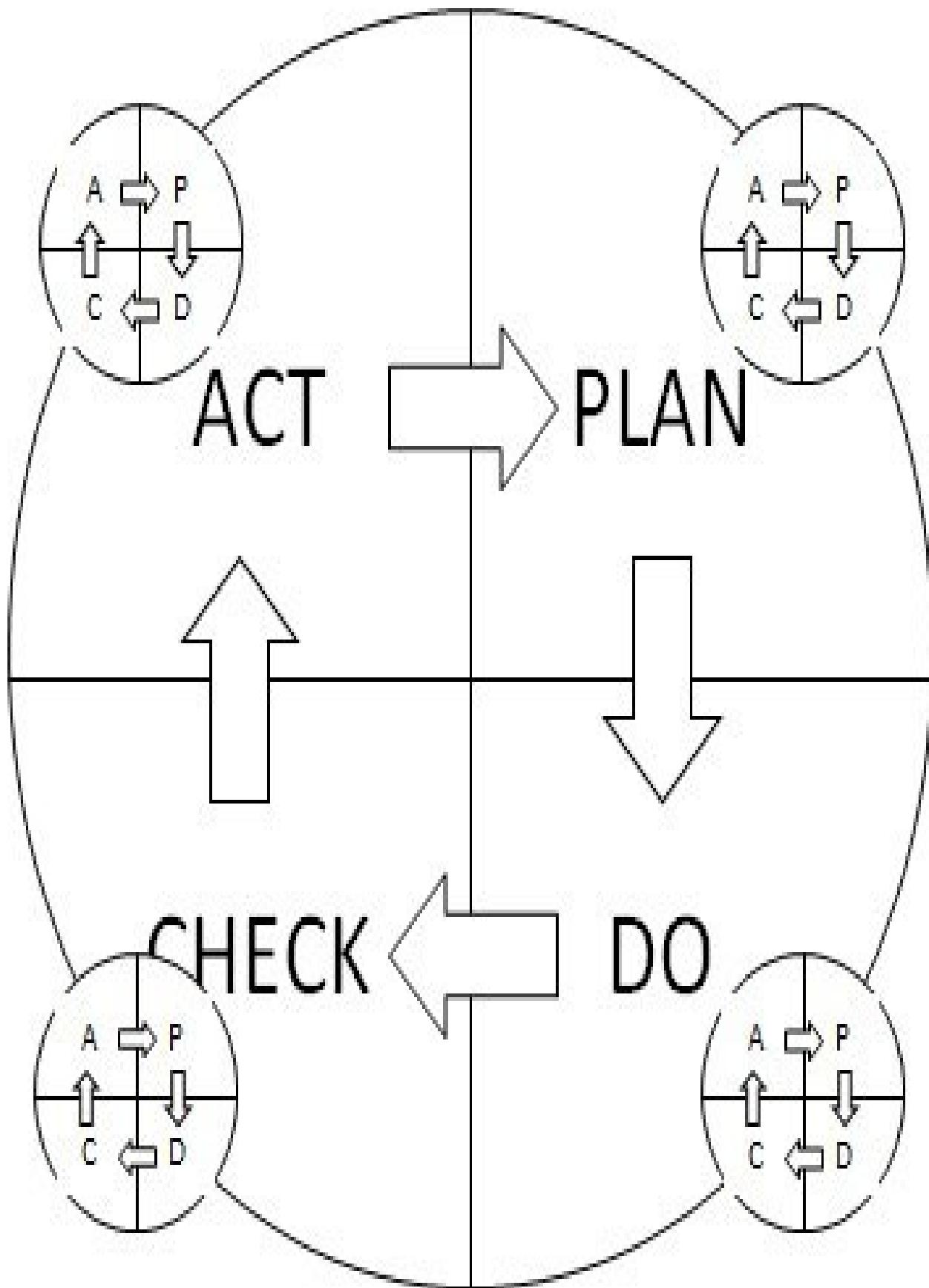


Figura 14.2.4:

Il ciclo PDCA “frattale circolare”

Esempio 14.2.2. La pianificazione di un progetto, attività tipica della fase di plan è a sua volta oggetto del ciclo PDCA. In altre parole, a sua volta deve essere pianificata, attuata, verificata e, se opportuno, oggetto di intervento.

Ecco quindi un ciclo PDCA per la pianificazione di un progetto:

plan: prima di pianificare un progetto, è necessario stabilire quali strumenti utilizzare per tenerne sotto controllo le sue fasi e risorse (per esempio, diagrammi di GANTT su supporto cartaceo o informatico);

do: la pianificazione deve essere realizzata con gli strumenti stabiliti in precedenza;

check: nel corso del progetto, la pianificazione va verificata periodicamente, per vedere se è sempre adeguata o, a causa di diversi eventi, è necessario modificarla;

act: se richieste modifiche alla pianificazione, vanno fatte con interventi mirati; in alcuni casi, può essere necessario ripianificare tutto il progetto, tornando alla fase di plan.

Quanto detto riguarda la natura “frattale circolare” del ciclo PDCA. Accanto a

essa bisogna considerare la natura “frattale gerarchica” del ciclo PDCA lungo i livelli della piramide di Anthony (figura 4.2.1): l’attuazione (Do) di una strategia richiede di pianificare (Plan) la modifica dei processi a livello tattico, la cui attuazione (Do) richiede di pianificare (Plan) quanto necessario a livello operativo.

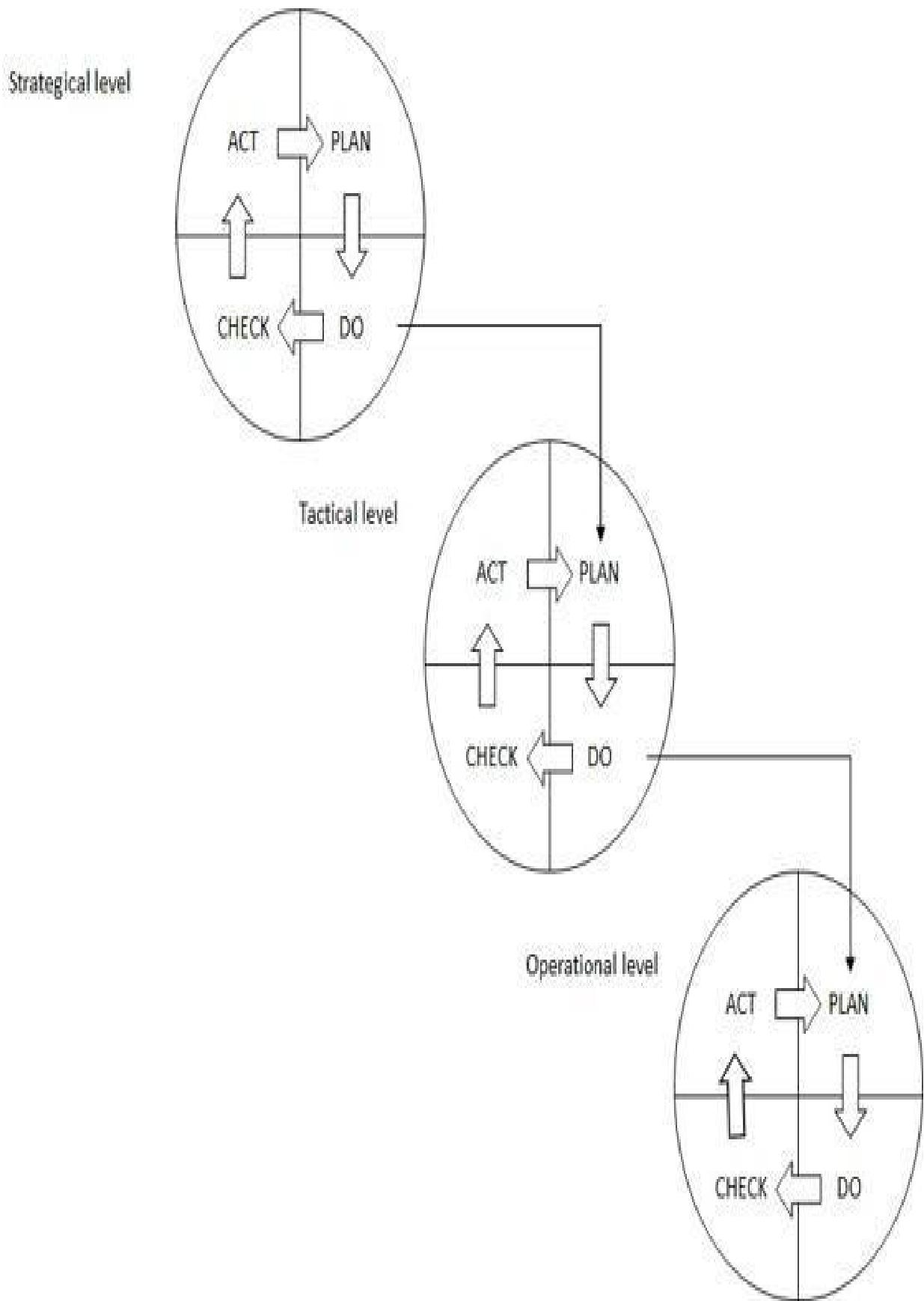


Figura 14.2.5:

Il ciclo PDCA “frattale gerarchico”

Esempio 14.2.3. Un’officina meccanica specializzata nella lavorazione del rame, ha come strategia l’ampliamento delle proprie attività all’acciaio.

Attua quindi questa strategia pianificando, a livello tattico, quali devono essere le macchine da utilizzare, quali devono essere i processi da seguire, quali persone formare o inserire nell’organizzazione per avere le competenze necessarie.

Per attuare queste tattiche, dovranno essere pianificate ed eseguite le attività operative: acquisizione e installazione delle macchine, preparazione e diffusione delle procedure e dei moduli, formazione e reclutamento del personale.

Al termine del progetto si dovranno pianificare ed eseguire le attività operative quotidiane: produzione, test, correzione dei difetti, eccetera.

Questi argomenti, sebbene teorici, permetteranno di comprendere alcune scelte operate nella redazione della ISO/IEC 27001.

Capitolo 15

I requisiti di sistema

Le persone non stupide sottovalutano sempre il potenziale nocivo delle persone stupide

Carlo M. Cipolla, Le leggi fondamentali della stupidità umana

In questo capitolo sono riportati i requisiti della ISO/IEC 27001 e una loro interpretazione, basata anche su quanto discusso durante i lavori preparatori della ISO/IEC 27003:2017. Per ovvi motivi di diritto d'autore, i requisiti non sono riportati tali e quali, anche se ne è mantenuta la medesima divisione dei capitoli. Si raccomanda di leggere la ISO/IEC 27001 nella versione ufficiale perché quanto segue non ha la pretesa di sostituirla.

La lettura della norma non può essere fatta in modo lineare perché i requisiti si richiamano l'un l'altro, spesso in modo non esplicito. Nell'introduzione, la stessa ISO/IEC 27001 dichiara che “l'ordine con cui i requisiti sono presentati in questo standard non riflette né la loro importanza, né l'ordine in cui devono essere attuati”. Nonostante ciò, si cercherà di presentare i requisiti nel loro ordine, pur con qualche eccezione, e di evidenziare i richiami tra di essi.

Nel seguito, seppure impropriamente e per non appesantire il testo, si utilizza l'espressione “sistema di gestione” al posto di “sistema di gestione per la sicurezza delle informazioni”.

15.1 Ambito di applicazione dello standard

Il primo capitolo della ISO/IEC 27001, dopo un'introduzione, chiarisce che i requisiti dello standard sono applicabili a tutte le organizzazioni. Inoltre, per potersi dichiarare conformi allo standard e certificarsi rispetto a esso, è necessario soddisfare tutti i requisiti di sistema riportati nei capitoli dal 4 al 10 dello standard e presentati in questo libro dal paragrafo 15.4 al paragrafo 15.10.

L'Appendice A non riporta requisiti, ma i controlli di sicurezza.

Si segnala che il termine ambito è utilizzato in molte accezioni:

di applicazione della norma, di cui si è appena discusso: la norma è applicabile a ogni tipo di organizzazione, indipendentemente dalla dimensione, natura societaria o settore di mercato;

del sistema di gestione per la sicurezza delle informazioni: quella parte dell'organizzazione a cui si applicano i requisiti della ISO/IEC 27001; può coincidere con tutta l'organizzazione;

della certificazione: un'organizzazione può richiedere a un'entità esterna di verificare il completo soddisfacimento dei requisiti della ISO/IEC 27001 e di emettere un certificato che lo attesti (maggiori dettagli in appendice C); l'ambito della certificazione può coincidere con quello del sistema di gestione o una sua parte.

15.2 Riferimenti normativi della ISO/IEC 27001

L'unico riferimento normativo riportato dalla ISO/IEC 27001 è l'ultima versione della ISO/IEC 27000.

La ISO/IEC 27000, disponibile gratuitamente¹³⁷, riporta le definizioni dei termini tecnici utilizzati dalle norme della famiglia ISO/IEC 27000. È necessario conoscere esattamente le definizioni ufficiali di ciascun termine per poter comprendere appieno i requisiti dello standard.

La ISO/IEC 27002 non è citata in questo paragrafo: trattandosi di una linea guida, non può essere ritenuta normativa e pertanto è solo citata in bibliografia.

15.3 Termini e definizioni della ISO/IEC 27001

Il terzo capitolo della ISO/IEC 27001, previsto dall'HLS, non riporta alcuna definizione perché quelle applicabili sono riportate dalla ISO/IEC 27000, già presentata nel paragrafo precedente.

Nelle future edizioni si prevede di non seguire questo approccio e di riportare le definizioni utili per la ISO/IEC 27001 stessa. Questo per avere un documento il più possibile completo e di facile lettura.

15.4 Contesto dell'organizzazione e ambito del SGSI

Il contesto e l'ambito del sistema di gestione per la sicurezza delle informazioni, oggetto del capitolo 4 dello standard, sono oggetto del capitolo 5 del presente

libro. In seguito sono forniti alcuni elementi di interpretazione della norma.

15.4.1 Il contesto dell'organizzazione

La norma richiede di identificare il contesto dell'organizzazione, ossia:

i fattori interni ed esterni, già elencati nel paragrafo 5.1;

le parti interessate e le loro aspettative, peraltro esse stesse fattori interni ed esterni.

Una nota ricorda che alcune parti interessate si attendono che l'organizzazione rispetti i requisiti legali e i contratti sottoscritti.

La norma non richiede di documentare il contesto, ma andrebbe fatto. Infatti, ne devono essere considerati i cambiamenti in occasione del riesame di Direzione, che a sua volta va documentato (paragrafo 15.9.3).

15.4.2 L'ambito del SGSI

Dal contesto è possibile stabilire l'ambito del sistema di gestione per la sicurezza delle informazioni: ricordando che esso può essere tutta l'organizzazione o parte di essa (paragrafo 5.2), la norma richiede di descriverlo e di fornire le motivazioni per cui è stato scelto. Tali motivazioni devono essere basate sui fattori del contesto interni o esterni, incluse le aspettative delle parti interessate.

Esempio 15.4.1. Un fornitore di servizi informatici di una banca ha deciso di attuare un sistema di gestione per la sicurezza delle informazioni solo per la conduzione dei sistemi informatici e non per lo sviluppo delle applicazioni.

Questo considerando i seguenti fattori:

la disponibilità dei sistemi, garantita in fase di conduzione, è ritenuta fondamentale dalla banca;

le misure di sicurezza sono controllate principalmente dal personale addetto alla conduzione dei sistemi; essi sono anche responsabili di autorizzare l'installazione di nuove applicazioni o di loro modifiche dopo aver esaminato i requisiti e i test elaborati dagli sviluppatori;

si preferisce, in una fase iniziale, concentrare i costi e le energie in un ambito più ristretto ed estenderlo in futuro alle attività di sviluppo.

L'ambito deve essere descritto in un documento riportando quanto è necessario per capire: a cosa si applicano i requisiti e i controlli di sicurezza della ISO/IEC 27001, a cosa si riferisce la valutazione del rischio, quali sono le informazioni da proteggere e gli strumenti che le trattano. La descrizione dell'ambito, di cui è fornito un esempio nel paragrafo 5.1, dovrebbe riportare:

le caratteristiche dei servizi erogati o dei prodotti realizzati;

le informazioni alle quali si vuole garantire la sicurezza e i cui dettagli saranno oggetto dell'identificazione del rischio;

i processi pertinenti, inclusi quelli affidati a entità esterne all'ambito e le loro

interfacce con quelli interni;
la struttura organizzativa a supporto del sistema di gestione;
la tecnologia adottata e uno schema della rete informatica;
le sedi e i locali dove sono trattate le informazioni;
i fornitori più importanti.

La descrizione dell'ambito potrebbe essere nello stesso documento in cui è descritto il contesto. Alcuni elementi dell'ambito potrebbero essere descritti riportando i riferimenti ad altri documenti.

Esempio 15.4.2. In molte organizzazioni, il documento di descrizione dell'ambito non riporta l'organigramma, ma un riferimento a quello ufficiale.

Devono essere inoltre descritti i confini del sistema di gestione, soprattutto se riguarda una parte dell'organizzazione.

Esempio 15.4.3. Il fornitore di servizi informatici descritto nell'esempio 15.4.1 ha riportato nel documento di descrizione dell'ambito, tra l'altro:

aree presenti nell'organigramma incluse o escluse dall'ambito;
funzioni organizzative di controllo del trasferimento delle applicazioni dagli sviluppatori agli addetti alla conduzione (interfacce tra i processi inclusi

nell’ambito e quelli esterni).

L’ambito del SGSI non corrisponde all’ambito scritto su un eventuale certificato: quest’ultimo è solitamente molto sintetico e riporta solo i servizi erogati inclusi nel sistema di gestione; la descrizione dell’ambito del SGSI deve essere invece più esaustiva.

15.4.3 Sistema di gestione per la sicurezza delle informazioni

Il capitolo relativo al contesto e all’ambito si conclude dicendo che, nell’ambito scelto, l’organizzazione deve stabilire, attuare, mantenere e migliorare un sistema di gestione per la sicurezza delle informazioni conformemente ai requisiti dello standard.

Si tratta di un requisito ovvio per chi adotta lo standard.

15.5 Leadership

Le responsabilità della Direzione sono descritte nel paragrafo 12.3.1.1 di questo libro.

La ISO/IEC 27001, anche sulla base di quanto previsto dall’HLS, utilizza il termine leadership, per sottolineare il ruolo della Direzione: non solo di appoggio, ma anche di esempio e guida.

La Direzione deve:

stabilire la politica per la sicurezza delle informazioni (paragrafo 15.5.1) e assicurarsi che siano stabiliti gli obiettivi (paragrafo 15.6.5), allineati con la direzione strategica dell’organizzazione;

garantire la disponibilità delle risorse necessarie al funzionamento del sistema di gestione per la sicurezza delle informazioni; la valutazione delle risorse disponibili e di quelle da reperire è oggetto del riesame di Direzione (paragrafo 15.9.3);

comunicare, attraverso i canali più opportuni, oltre alla politica per la sicurezza delle informazioni, l’importanza del sistema di gestione per la sicurezza delle informazioni e la necessità di adeguarsi ai requisiti stabiliti dalle politiche e procedure dell’organizzazione;

dirigere e sostenere le persone affinché contribuiscano al miglioramento del sistema di gestione per la sicurezza delle informazioni.

Nelle organizzazioni dove l’ambito del sistema di gestione coincide con l’organizzazione stessa, la Direzione è facilmente individuabile ed è il Consiglio d’amministrazione, l’Amministratore delegato o il Direttore generale. Nelle organizzazioni in cui l’ambito ne è solo una parte, per individuare chi ha il ruolo di Direzione, ossia, secondo la definizione riportata nel paragrafo 12.3.1.1, “coloro che dirigono e tengono sotto controllo quella parte di organizzazione”, si potrebbe cercare dove sono i soldi (principio di Sutton): la Direzione è composta da chi decide sulle risorse da allocare per la sicurezza delle informazioni.

15.5.1 Politica per la sicurezza delle informazioni

Questo argomento riguarda la “politica generale per la sicurezza delle informazioni”, esaminata nel paragrafo 12.2, e deve riportare:

uno schema di riferimento per stabilire gli obiettivi di sicurezza delle informazioni; questo schema deve includere cosa si intende per “sicurezza delle informazioni”; infatti è importante per l’organizzazione avere chiari i principi generali da seguire e gli obiettivi strategici generici di cui si parlerà nel paragrafo 15.6.5.1;

la volontà della Direzione di soddisfare i requisiti del sistema di gestione per la sicurezza delle informazioni e di perseguiрne il miglioramento.

La politica deve essere documentata, comunicata all’interno dell’organizzazione e, per quanto appropriato, disponibile alle parti interessate. Se si prevede di comunicare la politica, tutta o in parte, all’esterno dell’organizzazione, essa deve essere scritta evitando di riportare informazioni riservate.

Esempio 15.5.1. Alcune parti interessate esterne all’organizzazione a cui comunicare la politica per la sicurezza delle informazioni:

potenziali clienti che la richiedono per decidere se stipulare un contratto con l’organizzazione;

i fornitori affinché vi si adeguino;

auditor o ispettori esterni.

15.5.2 Ruoli e responsabilità

Dei ruoli e delle responsabilità si è discusso nel paragrafo 12.3.

La Direzione deve stabilire e comunicare, come appropriato, ruoli e responsabilità di primo livello e specificare le necessità di alcuni altri ruoli necessari al sistema di gestione. A loro volta, i ruoli sottostanti devono stabilire ruoli e responsabilità delle persone sotto il proprio controllo.

I ruoli sono spesso specificati in un organigramma, mentre le responsabilità lo sono nei mansionari e nelle procedure.

15.6 Pianificazione

Il capitolo 6 dello standard riguarda la pianificazione del sistema di gestione per la sicurezza delle informazioni da un punto di vista strategico e tattico. È quindi opportuno distinguere tra diversi tipi di pianificazione, facendo riferimento alla piramide di Anthony (paragrafo 4.2):

pianificazione strategica: comprende le scelte generali relative al sistema di gestione, la preparazione e pubblicazione della politica per la sicurezza delle informazioni, la scelta degli obiettivi strategici, l'individuazione dei processi e dei controlli del sistema di gestione, le loro caratteristiche generali e le loro relazioni; essa è oggetto di questo paragrafo;

pianificazione tattica: stabilisce i dettagli dei processi e dei controlli di sicurezza da attuare, i loro obiettivi, le risorse necessarie per realizzare quanto pianificato, le attività che compongono i processi e la loro frequenza o scadenza; essa è parzialmente oggetto di questo capitolo (paragrafo 15.8) e parzialmente oggetto del capitolo 8 dello standard;

pianificazione operativa: stabilisce esattamente quando effettuare le attività, tra cui, per esempio: manutenzione degli impianti, riesami delle utenze, esecuzione delle prove di ripristino, esecuzione dei test di continuità operativa, esecuzione dei vulnerability assessment, acquisizione delle risorse materiali, reperimento delle persone, formalizzazione dei contratti con i fornitori; la pianificazione tattica, nell’ambito dei singoli processi e controlli, deve stabilire quando effettuare queste pianificazioni operative e i loro responsabili.

Il capitolo relativo alla pianificazione è di difficile lettura perché, nelle intenzioni degli autori, dovrebbe essere dedicato alla pianificazione strategica del sistema di gestione. Per questo sono affrontati i requisiti relativi alla valutazione del rischio, alle azioni per il miglioramento e agli obiettivi. Questi elementi, però, hanno impatti anche sulla pianificazione tattica dei processi e questo può generare confusione nella lettura.

15.6.1 I rischi relativi all’efficacia del sistema di gestione

I processi da attuare, le loro caratteristiche generali, i loro obiettivi e le azioni per migliorarli dovrebbero nascere da una valutazione dei rischi relativi all’efficacia del sistema di gestione.

L’HLS, e quindi la ISO/IEC 27001, anche in linea con l’approccio seguito in altri contesti (per esempio nella privacy con il GDPR), riduce i requisiti documentali rispetto al passato, ma chiede di basare le scelte fatte su una valutazione il rischio. Questo approccio, simile a quello della common law anglosassone, anche se più vago, è più flessibile e quindi apprezzabile in caso di nuovi sviluppi tecnici o sociali.

In sintesi, i rischi, originati dai fattori interni ed esterni che compongono il contesto dell’organizzazione, devono essere identificati e valutati

dall’organizzazione per decidere come impostare o migliorare il proprio sistema di gestione per la sicurezza delle informazioni.

In questo libro si sostiene la tesi per cui i rischi relativi all’efficacia del sistema di gestione sono anche rischi relativi alla sicurezza delle informazioni. Infatti, un rischio relativo al sistema di gestione può avere effetti sulla sua capacità di soddisfare i suoi obiettivi ossia, in questo caso, garantire il livello di sicurezza desiderato per le informazioni. Per questo motivo, non sono necessarie due valutazioni del rischio, ma un’unica relativa alla sicurezza delle informazioni che comprenda quella relativa al sistema di gestione.

Gli utilizzatori dello standard sono però liberi di differenziare le due valutazioni del rischio, ricordando che non è specificato come la valutazione dei rischi relativi all’efficacia del sistema di gestione debba essere fatta. Ulteriori considerazioni saranno proposte nel seguito in merito all’integrazione di più sistemi di gestione e al posizionamento della valutazione del rischio relativo alla sicurezza delle informazioni.

La valutazione del rischio relativo alla sicurezza delle informazioni è oggetto del successivo paragrafo 6.1.2 dello standard (paragrafo 15.6.2 di questo libro).

Esempio 15.6.1. Chi vuole differenziare i “rischi relativi all’efficacia del sistema di gestione” rispetto ai “rischi relativi alla sicurezza delle informazioni” propone come esempi:

la mancanza di impegno della Direzione;

la mancanza di risorse;

la mancanza (per malattia, dimissioni o ferie) di competenze in possesso di una sola persona;

l'inadeguatezza delle procedure.

Questi "rischi" sono in realtà delle minacce o delle vulnerabilità relative alla sicurezza delle informazioni.

La norma richiede di pianificare azioni per affrontare i rischi relativi all'efficacia del sistema di gestione. Esse sono oggetto del trattamento del rischio relativo alla sicurezza delle informazioni, i cui requisiti si trovano nel paragrafo 6.1.3 dello standard (paragrafo 15.6.3 di questo libro).

La norma sottolinea la necessità di integrare gli elementi del sistema di gestione per la sicurezza delle informazioni nei processi e nelle attività dell'organizzazione. In altre parole, richiede di non costruire un sistema di gestione per la sicurezza delle informazioni estraneo all'organizzazione, come succede in alcune organizzazioni che intendono certificarsi e realizzano un sistema parallelo con l'unico scopo di mostrarlo agli auditor.

Esempio 15.6.2. Il caso di fine 2013 della Target è emblematico, se la notizia è vera: pagò uno strumento di sicurezza 1,6 milioni di dollari, solo per essere conforme alle regole PCI e non per utilizzarlo¹³⁸.

Le opportunità

Il rischio, come si è visto al capitolo 4, può avere impatti positivi. In questo caso, non si parla di minacce, ma di opportunità. La definizione di opportunità non è fornita dalla ISO/IEC 27000, né da altre norme collegate.

Esempio 15.6.3. Opportunità per il sistema di gestione per la sicurezza delle informazioni possono essere:

l'adozione di tecnologie di virtualizzazione, perché permettono di contenere i costi e realizzare delle ridondanze efficaci;

l'adozione di tecnologie di mobile device management, perché rendono più sicuro l'uso dei dispositivi mobili e il BYOD.

Le opportunità (con impatti positivi) dovrebbero essere valutate con i rischi (con impatti negativi). È quindi consigliabile riscrivere le opportunità come minacce: se un'opportunità non viene colta, allora gli impatti negativi sono i benefici persi.

Esempio 15.6.4. Le opportunità dell'esempio precedente possono essere riscritte come vulnerabilità:

le tecnologie utilizzate per le ridondanze, in confronto con le tecnologie di virtualizzazione oggi a disposizione, sono inefficaci o obsolete;

i dispositivi mobili e il BYOD non sono controllati centralmente.

Le opportunità devono essere valutate insieme ai rischi con impatto negativo. Per evitare di analizzarle separatamente, basandosi sui potenziali benefici, si consiglia di “trasformarle” in minacce e vulnerabilità.

Nota sulla terminologia

La ISO/IEC 27001, a causa di un errore dell’HLS, richiede di analizzare “rischi e opportunità”.

I rischi, però, sono degli “effetti”, positivi o negativi, dovuti a minacce o opportunità. Più correttamente, la norma avrebbe dovuto chiedere di analizzare “minacce e opportunità” oppure “rischi con impatto negativo o positivo”. Intuitivamente il testo è chiaro, ma formalmente non corretto.

Integrazione dei sistemi di gestione

Se un’organizzazione ha attuato più sistemi di gestione per discipline diverse (qualità, ambiente, salute e sicurezza delle persone, energia, eccetera), potrebbe ritenere necessario effettuare una valutazione del rischio per ciascuna.

Esempio 15.6.5. Minacce relative alla qualità possono essere:

indisponibilità delle materie prime;

forniture inadeguate;
errori da parte del personale;
errori dei fornitori;
guasto dei macchinari di produzione.

Un'organizzazione, soprattutto se opera nel mercato informatico, potrebbe trovare più conveniente consolidare in un'unica valutazione del rischio quelle relative ai diversi sistemi di gestione. Altre organizzazioni potrebbero trovare più appropriato, per le loro attività e i risultati da considerare, condurre valutazioni del rischio distinte per ciascuna disciplina e con metodi diversi.

Questo libro si occupa solo di sicurezza delle informazioni e quindi non vengono approfondite queste opzioni.

15.6.2 Valutazione del rischio relativo alla sicurezza delle informazioni

Nella ISO/IEC 27001 i requisiti sulla valutazione del rischio relativo alla sicurezza delle informazioni sono riportati nel capitolo 6, dedicato alla pianificazione del sistema di gestione. Questo perché la valutazione dei rischi relativi alla sicurezza delle informazioni serve a stabilire e pianificare i requisiti dei processi del sistema di gestione. Inoltre, per molti, i rischi relativi alla sicurezza delle informazioni comprendono quelli relativi all'efficacia del sistema di gestione.

La norma richiede di documentare in una procedura il processo di valutazione del rischio adottato. Tale processo deve essere composto dalle fasi di

identificazione, analisi e ponderazione, come visto nella figura 4.0.1.

Altre caratteristiche del processo di valutazione del rischio richieste dalla norma:

individuare i criteri di (accettazione del) rischio (capitolo 8);

in fase di identificazione associare i rischi alla potenziale perdita di riservatezza, integrità e disponibilità delle informazioni;

identificare un responsabile per ciascun rischio (paragrafo 4.4.1);

determinare i livelli di rischio sulla base della valutazione delle loro conseguenze e probabilità;

ponderare i rischi confrontandoli con i criteri di rischio e ordinarli per dare priorità al loro trattamento.

La norma non parla di asset, minacce e vulnerabilità e non richiede di seguire tutti i passi descritti nei capitoli 6, 7 e 8 di questo libro. Questo per lasciare libertà agli utilizzatori nella scelta del metodo da adottare. Come già detto nel paragrafo 4.3.2, esistono altri metodi e se ne raccomanda lo studio prima di decidere quale utilizzare o di svilupparne uno nuovo aderente alle proprie necessità.

La norma impone di assicurare la validità dei risultati, ossia, come riportato in una nota del paragrafo dedicato ai monitoraggi e alle misurazioni e come indicato nel paragrafo 4.3.2: ripetibili, comparabili e coerenti. È sottintesa la completezza.

I risultati della valutazione del rischio, come richiesto nel paragrafo 8.1 dello

standard, devono essere documentati insieme ai rischi identificati e al loro livello.

Periodicità della valutazione del rischio

La norma richiede di stabilire i criteri da seguire per ripetere la valutazione del rischio. Questi criteri devono essere descritti in una procedura che potrebbe essere quella dedicata al processo di valutazione del rischio.

Si raccomanda di rivalutare completamente il rischio almeno una volta all'anno per collegare il piano di trattamento al processo di budgeting e al riesame di Direzione (paragrafo 15.9.3).

La procedura deve anche stabilire a fronte di quali cambiamenti del contesto è necessario rivalutare il rischio, completamente o parzialmente.

Esempio 15.6.6. La rivalutazione completa del rischio potrebbe rendersi necessaria dopo un cambio di tutto il sistema informativo, la modifica dell'organigramma o l'acquisizione dell'organizzazione da parte di un'altra.

La rivalutazione del rischio solo per gli asset coinvolti potrebbe rendersi necessaria dopo un cambio di tecnologia, l'apertura di una nuova sede o l'acquisizione di un'altra organizzazione.

La rivalutazione del rischio solo per una specifica minaccia potrebbe essere originata da una notizia di giornale che la riguarda.

15.6.3 Il trattamento del rischio relativo alla sicurezza delle informazioni

La norma richiede di documentare in una procedura, anche la stessa in cui è descritto il processo di valutazione del rischio, il processo di trattamento del rischio. Questo processo deve prevedere come input i risultati della valutazione del rischio e come output la scelta delle opzioni di trattamento per ciascun rischio, già illustrate nel paragrafo 9.1, dei controlli per attuarle, da descrivere nel piano di trattamento del rischio.

La norma richiede quindi di collegare i rischi ai relativi controlli di sicurezza; anche nel caso di accettazione del rischio, devono essere identificati i controlli che mantengono quel livello di rischio.

Come conseguenza, a ogni controllo di sicurezza si deve poter risalire ai rischi che contrasta, ma questo non è riportato dalla norma perché ritenuto implicito.

Nel caso sia necessario avviare azioni per modificare i controlli di sicurezza già esistenti o per realizzarne di nuovi, devono essere pianificate e attuate delle azioni, oggetto del paragrafo 15.6.4.

I responsabili del rischio, infine, devono approvare le opzioni scelte e le azioni di trattamento proposte.

Dichiarazione di applicabilità

La norma richiede di preparare un documento in cui riportare un elenco esaustivo di controlli di sicurezza e, per ognuno di essi, indicare se è attuato o meno nell'ambito del sistema di gestione, insieme alle motivazioni della scelta o dell'esclusione. L'elenco dei controlli di sicurezza dell'Appendice A della norma stessa è ritenuto "esaustivo" e pertanto quasi tutti usano quello, ma è possibile usarne altri purché altrettanto esaustivo (per esempio la Cloud Controls Matrix della Cloud Security Alliance¹³⁹). L'elenco adottato può essere citato nella descrizione dell'ambito del certificato.

È comunque necessario indicare quali controlli dell'Appendice A della ISO/IEC 27001 sono esclusi e la giustificazione per questa scelta.

Un'organizzazione può anche usare i controlli dell'Appendice A della norma e aggiungerne altri, per esempio perché specifici per le proprie attività o per altre ragioni. Anche in questo caso può citare l'origine dei controlli aggiuntivi sul certificato.

La scelta di inclusione può essere giustificata con un rimando al piano di trattamento del rischio e al collegamento tra rischi e controlli (in questo modo, la ragione per l'inclusione di un controllo è fornita dalle minacce che contrasta). L'esclusione è spesso motivata dall'impossibilità di applicare il controllo all'ambito.

Esempio 15.6.7. Molte organizzazioni escludono il controllo relativo allo sviluppo del software in outsourcing perché non danno a fornitori lo sviluppo del software.

In Italia, quasi tutte le organizzazioni escludono il controllo relativo alla legislazione in materia di crittografia se non offrono servizi informatici per cui questo aspetto è regolamentato per legge.

Questo documento, denominato Dichiarazione di applicabilità in italiano o Statement of Applicability (SoA) in inglese, è poco apprezzato da molti utilizzatori della ISO/IEC 27001 perché sovente si riduce a un esercizio formale di spunta.

Alcuni auditor richiedono di riportare nella Dichiarazione di applicabilità una breve descrizione della modalità di attuazione del controllo di sicurezza o i riferimenti alle procedure in cui è trattato. Questo requisito non è previsto dallo standard e l'organizzazione potrebbe rifiutarsi di ottemperarlo senza conseguenze. Molte organizzazioni trovano però utile questa pratica perché consente di avere una migliore conoscenza dei controlli di sicurezza e delle relative procedure.

Da ricordare che la Dichiarazione di applicabilità era nata nelle prime versioni della BS 7799 proprio allo scopo di condividere facilmente, e con un indice condiviso, la descrizione delle misure di sicurezza tra le parti interessate, per esempio nelle relazioni tra cliente e fornitore.

Posizionamento della valutazione e del trattamento del rischio relativo alla sicurezza delle informazioni

Una consistente minoranza degli utilizzatori della ISO/IEC 27001 non condivide la scelta di posizionare i requisiti relativi alla valutazione e al trattamento del

rischio relativo alla sicurezza delle informazioni nel capitolo dedicato alla pianificazione del sistema di gestione.

Ritengono infatti che i processi di valutazione e trattamento del rischio dovrebbero essere descritti nel capitolo dedicato alla pianificazione di dettaglio dei processi, ossia il capitolo 8 dello standard (descritto in questo libro nel paragrafo 15.8).

Questo punto di vista, peraltro non scorretto, non è risultato vincente perché, come già osservato, la valutazione e il trattamento del rischio relativo alla sicurezza delle informazioni contribuiscono alla pianificazione del sistema di gestione per la sicurezza delle informazioni allo stesso modo della valutazione del rischio relativo al sistema di gestione.

Inoltre, una divisione delle due valutazioni del rischio avrebbe potuto avere come conseguenza un'interpretazione scorretta dello standard: applicare la valutazione del rischio relativo alla sicurezza delle informazioni solo su servizi e prodotti informatici, visti come operativi, e non su tutto l'ambito e su tutti i processi del sistema di gestione per la sicurezza delle informazioni.

Come compromesso, la norma richiama la valutazione del rischio relativo alla sicurezza delle informazioni anche nel capitolo dedicato alle attività operative, dove richiede di mantenerne la registrazione. Altre norme, come la ISO 22301, hanno raccolto tutti i requisiti per la valutazione del rischio relativa alla specifica disciplina nel capitolo 8.

15.6.4 Le azioni

La ISO/IEC 27001 non fornisce esplicitamente requisiti relativi alle azioni, malgrado richieda di pianificarle per trattare i rischi, acquisire le competenze necessarie, mitigare effetti indesiderati dei cambiamenti, correggere le non conformità e prevenire il ripetersi di non conformità. Non esiste quindi un paragrafo dedicato alle azioni, ma a ogni azione deve essere collegato almeno un obiettivo (in caso contrario non si avrebbe la necessità di agire), per il quale devono essere soddisfatti dei requisiti precisi di cui si tratta al successivo paragrafo 15.6.5.

Quindi per ogni azione bisogna pianificare: le risorse necessarie, le persone responsabili dell'azione, le scadenze e le modalità con cui ne verrà valutata l'efficacia. Devono essere inoltre indicate le minacce o le opportunità per cui si è stabilita l'azione: se non ci fossero, l'azione sarebbe inutile.

Le azioni possono essere pianificate e attuate per modificare il sistema di gestione per la sicurezza delle informazioni o alcune sue componenti (processi, strumenti, metodi e procedure).

Un'azione può essere molto semplice e comportare un piccolo cambiamento a una procedura, oppure essere un progetto che richiede settimane, mesi o anni per essere completato.

Le azioni non devono essere tutte stabilite e monitorate dalla Direzione, ma dal giusto livello gerarchico e funzionale (strategico, tattico e operativo).

Quando un'azione può avere impatti su più aree dell'organizzazione, dovrebbe essere pianificata, attuata, controllata e verificata coinvolgendo diverse funzioni attraverso opportuni coordinamenti (paragrafo 12.3.1.5).

15.6.4.1 L'efficacia delle azioni

La valutazione dell'efficacia di un'azione prevede di analizzare se è stata realizzata come pianificato e ha raggiunto i risultati previsti.

Esempio 15.6.8. Un'organizzazione ha deciso di creare una funzione dedicata al monitoraggio della normativa applicabile e alla segnalazione delle sue modifiche alle funzioni interne. Per valutare l'efficacia di questa azione si potrebbe osservare se la nuova funzione:

ha attivato meccanismi per ricevere prontamente gli aggiornamenti normativi da fonti affidabili;

ha attivato canali di comunicazione con tutte le altre funzioni dell'organizzazione potenzialmente coinvolte dagli aggiornamenti normativi;

ha segnalato l'opportunità di avviare dei progetti a fronte di cambiamenti normativi e li ha tenuti sotto controllo.

L'efficacia non dovrebbe essere valutata al momento del completamento dell'azione, ma:

se applicabile, a intervalli pianificati durante le fasi di pianificazione e attuazione, per poter intervenire se necessario;

dopo qualche tempo dalla sua conclusione, quando se ne possono esaminare i benefici o eventuali effetti indesiderati.

Esempio 15.6.9. Proseguendo l'esempio precedente, l'efficacia dell'azione dovrebbe essere valutata dopo qualche mese dalla creazione della nuova funzione. Questo per lasciarle il tempo di attivare i meccanismi di ricezione degli aggiornamenti e i canali di comunicazione con le diverse funzioni.

Una completa valutazione può essere fatta solo al completamento dei progetti di adeguamento ai cambiamenti normativi. Si osservi che questi progetti sono a loro volta delle azioni di miglioramento e quindi la valutazione dell'efficacia di un'azione può essere subordinata alla valutazione dell'efficacia di un'altra azione.

Esempio 15.6.10. A seguito della formazione di una persona sulla gestione dei progetti, non sarebbe significativo valutare l'efficacia di questa azione al termine del corso, ma dopo la conclusione di un progetto di cui è stata responsabile.

Esempio 15.6.11. Nel caso di introduzione di un nuovo strumento software per registrare e tenere sotto controllo le attività di gestione degli incidenti, l'efficacia dell'azione dovrebbe essere valutata al momento della scelta dello strumento, a seguito della sua installazione e dopo un paio di mesi dal momento in cui gli utenti hanno iniziato a usare lo strumento.

Si osservi che la norma richiede quindi l'applicazione di un ciclo PDCA e sottintende la fase di Act: quando l'azione si rivela inefficace è necessario intervenire. Come già detto nel paragrafo 14.2.3, questa attività è spesso sottovalutata.

Esempio 15.6.12. Nel caso dell'esempio 15.6.2, se la notizia fosse vera, la Target, come azione di miglioramento, aveva introdotto un nuovo strumento di rilevazione di malware, ma il processo di rilevamento, segnalazione e trattamento degli allarmi non era stato completamente attivato. Una corretta attuazione del ciclo PDFCA avrebbe probabilmente permesso di rilevare e affrontare il problema.

15.6.4.2 Registro delle azioni di miglioramento

È opportuno, anche se non richiesto dallo standard, creare un registro delle azioni di miglioramento, dove descrivere le azioni in fase di pianificazione e in corso. Questo permetterebbe di tenere informate tutte le parti interessate, in modo che azioni con impatto su più funzioni siano seguite da tutte le persone interessate.

In alcuni casi questo registro può servire a condividere le esperienze: se un'area dell'organizzazione dovesse accorgersi che un'altra area ha avviato un'azione simile a una già attuata, potrebbe mettere a disposizione le proprie esperienze e condividere degli strumenti (per esempio, programmi software) già sperimentati.

15.6.5 Obiettivi

La ISO/IEC 27000 fornisce la seguente definizione.

Obiettivo: risultato da raggiungere.

Nota 1: un obiettivo può essere strategico, tattico o operativo.

Nota 2: gli obiettivi possono [...] essere applicati a diversi livelli (per esempio, di strategia, di organizzazione complessiva, di progetto, di prodotto, di processo).

Nota 3: un obiettivo può essere espresso in molti modi; per esempio come risultato atteso, una finalità, un criterio operativo, un obiettivo di sicurezza delle informazioni; possono essere utilizzati altri termini con significato simile come, per esempio, aim, goal, target.

Nota 4: nel contesto di un sistema di gestione per la sicurezza delle informazioni, gli obiettivi di sicurezza delle informazioni sono impostati dall'organizzazione, coerentemente alla politica di sicurezza delle informazioni, per raggiungere specifici risultati.

Tutti gli obiettivi devono seguire il principio cosiddetto SMART, ossia:

Specifici: riguardare un ambito preciso ed essere coerenti con la politica di sicurezza delle informazioni;

Misurabili: come si vedrà in seguito;

Raggiungibili (Achievable): l'organizzazione e le risorse assegnate sono tali da

permetterne il conseguimento;

Pertinenti (Relevant): applicabili all'ambito di lavoro della persona o funzione o processo a cui sono assegnati;

Con scadenza (Time-bound): relativi a un periodo di tempo specificato.

La misurabilità degli obiettivi richiede di aver stabilito processi di misurazione, affrontati dallo standard al capitolo 9 (paragrafo 15.9.1). Qui si fanno solo pochi accenni a qualche aspetto relativo alle misurazioni, per rendere la lettura il più possibile sequenziale.

La norma richiede di stabilire gli obiettivi relativi alla sicurezza delle informazioni ai diversi livelli funzionali, di documentarli, di comunicarli alle parti interessate secondo necessità e aggiornarli come appropriato. Inoltre, per ogni obiettivo devono essere documentati:

cosa fare; eventualmente pianificando azioni o mantenendo procedure e controlli di sicurezza già stabiliti;

le risorse necessarie;

le persone responsabili del raggiungimento dell'obiettivo;

quando sarà valutato il raggiungimento dell'obiettivo;

le modalità con cui i risultati saranno valutati.

Direzione per obiettivi

Le norme relative ai sistemi di gestione dell'ISO promuovono alcuni elementi

della direzione per obiettivi (management by objective), ossia una pratica gestionale che prevede di assegnare obiettivi alle funzioni dell'organizzazione per poi valutarle in base al loro raggiungimento.

Nella forma più deteriore di questa pratica gestionale, la Direzione assegna degli obiettivi e poi non contribuisce in alcun modo al loro raggiungimento, per esempio non fornendo supporto o risorse o non adeguandoli in base ai cambiamenti di contesto [156].

Ulteriore rischio è che le funzioni dell'organizzazione potrebbero cercare di raggiungere i propri obiettivi senza occuparsi dell'impatto delle loro azioni sugli obiettivi altrui o su quelli complessivi.

Va quindi evitato di ridurre le capacità di analisi ai soli obiettivi misurabili senza osservare con attenzione la realtà, la cui complessità non può essere ridotta a un insieme di numeri. Deming affermò: “Eliminate la direzione per obiettivi (objectives), eliminate la gestione per numeri e per obiettivi (goals); sostituiteli con la leadership (direzione e guida)”. Ulteriori considerazioni in merito ai falsi miti delle misurazioni si trovano nel paragrafo 15.9.1.5.

La norme ISO richiedono di fissare obiettivi e tenerli sotto controllo ed esplicitamente alla Direzione di fornire supporto e risorse e adeguarli in base al contesto.

15.6.5.1 Misurazione degli obiettivi

Tutti gli obiettivi sono misurabili e il tipo di misurazione può essere:

per attributi, se basata su alcuni valori discreti;

per variabili, se la misura riguarda variabili continue.

Sono presentati alcuni esempi in merito e si rimanda al paragrafo 15.9.1 per ulteriori considerazioni.

Qui si propone uno schema di classificazione degli obiettivi, non riferito in alcun testo, ma utile per introdurre l'argomento:

obiettivi generici strategici;

obiettivi di azione;

obiettivi di rischio;

obiettivi di conformità;

obiettivi di prestazione.

La ISO/IEC 27004 [88] preferisce distinguere tra misure di prestazione e misure di efficacia.

Obiettivi generici strategici

Gli obiettivi generici strategici sono quelli espressi in termini imprecisi e sono riportati nella politica generale di sicurezza delle informazioni (paragrafo 15.5.1)

come “schema di riferimento per impostare gli obiettivi”.

Esempio 15.6.13. Esempi di obiettivi generici e strategici sono:

“ridurre le spese”;

“garantire un elevato livello di disponibilità dei sistemi informatici”;

“dare sul mercato un’immagine di affidabilità”;

“garantire la riservatezza delle informazioni”.

Gli obiettivi generici strategici possono essere raggiunti grazie a diverse attività e iniziative, a cui dovrebbero essere assegnati, ai pertinenti livelli dell’organizzazione, obiettivi di azione, di rischio, di conformità e di prestazione.

Esempio 15.6.14. L’obiettivo “garantire la riservatezza delle informazioni” può essere soddisfatto da diversi obiettivi:

obiettivo di azione: ottenere la certificazione ISO/IEC 27001 per tutta l’organizzazione;

obiettivo di rischio: ridurre a livello accettabile i rischi relativi a minacce con impatto sulla riservatezza;

obiettivo di conformità: applicare correttamente tutte le misure previste dalla normativa in materia di privacy;

obiettivo di prestazione: aggiornare nei prossimi tre anni tutti i contratti con i fornitori affinché sia sottoscritta la clausola di riservatezza; il primo anno, non meno del 60% dei fornitori deve aver ottemperato.

Gli obiettivi generici strategici possono essere misurabili per attributi: “soddisfatto”, “parzialmente soddisfatto”, “non soddisfatto”.

Obiettivi di azione

Gli obiettivi di azione riguardano azioni e progetti (paragrafo 15.6.4); il risultato da raggiungere è il loro completamento secondo quanto pianificato in termini di tempi, costi e requisiti.

Gli obiettivi di azione possono essere misurati per:

attributi: “azione completata secondo quanto pianificato” o “azione non completata secondo quanto pianificato”;

variabili: si calcola di quanto non siano stati rispettati i tempi, i costi e i requisiti, oppure la percentuale di quante azioni sono state completate secondo quanto pianificato.

Esempio 15.6.15. Un obiettivo di azione può essere: realizzare una procedura relativa ai backup e attuarla.

Questo obiettivo può essere documentato riportando:

cosa fare: realizzare la procedura e attuarla;

risorse necessarie: una persona per una settimana per realizzare la procedura e il personale addetto ai backup per configurare i sistemi;

responsabile: il responsabile dell'IT;

scadenza: due mesi;

valutazione dei risultati: verificare la corretta applicazione della procedura entro la scadenza prefissata.

Obiettivi di rischio

Gli obiettivi di rischio sono quelli collegati ai livelli di rischio e oggetto del paragrafo 9.3.1.1.

Le azioni di trattamento del rischio dovrebbero, ovviamente, essere collegate agli obiettivi di azione.

Obiettivi di conformità

Gli obiettivi di conformità si possono ridurre a tre:

“le procedure devono essere applicate”;

“le procedure e i processi devono essere conformi alla normativa vigente e agli standard adottati”;

“i prodotti e i servizi devono essere conformi a quanto stabilito dalle loro specifiche e dagli standard adottati”.

Gli obiettivi di conformità possono essere misurati per attributi: “conforme” e “non conforme”.

Si potrebbero anche misurare per variabili, se la valutazione avviene su un numero significativo di campioni, per esempio calcolando la percentuale di quante procedure non sono applicate correttamente, quanti processi e controlli non sono conformi alla normativa o agli standard pertinenti, quanti prodotti o servizi non sono conformi rispetto alle specifiche.

Si osservi che, per soddisfare gli obiettivi di conformità, spesso non è necessario pianificare alcuna azione, se non lavorare come previsto dalle procedure in vigore.

I requisiti riportati nei regolamenti, nelle politiche e nelle procedure sono obiettivi di conformità.

Esempio 15.6.16. Un obiettivo di conformità può essere il rispetto della procedura relativa ai backup e documentato riportando:

cosa fare: nulla di diverso rispetto al solito;

risorse necessarie: quelle già impiegate nella gestione dei backup;

responsabile: il responsabile dell'IT;

scadenza: ogni sei mesi si riesaminano i rapporti di esecuzione dei backup e delle prove di ripristino;

metodo di valutazione dei risultati: verificare la completa e corretta applicazione della procedura secondo le scadenze fissate.

Questo obiettivo è solitamente presentato in una “Procedura di gestione dei backup”.

Obiettivi di prestazione

Gli obiettivi di prestazione sono quelli correlati alle misurazioni oggetto del paragrafo 15.9.1.

In sintesi, a fronte di certe misurazioni (come quelle relative alla disponibilità dei sistemi) si dovrebbe attribuire un valore limite (per esempio, il 99.8% minimo di disponibilità dei sistemi) o dei valori di accettabilità.

Si osservi che, a rigore, tutti gli obiettivi sono degli obiettivi di prestazione, in quanto relativi a misurazioni (per variabili o per attributi).

Esempio 15.6.17. Un obiettivo di prestazione può essere: effettuare prove di ripristino dei backup per almeno il 40% dei sistemi ogni anno. Può essere documentato riportando:

cosa fare: realizzare un programma delle prove di ripristino da effettuare ogni anno e seguirlo;

risorse necessarie: i sistemisti già attualmente coinvolti nella conduzione dei diversi sistemi, stimando il loro impegno dopo aver completato il programma;

responsabile: il responsabile dell'IT;

scadenza: fine anno;

valutazione dei risultati: verificare i rapporti delle prove di ripristino e il completamento del programma annuale.

Gli obiettivi di prestazione potrebbero anche essere concordati a livello contrattuale con i clienti.

15.6.5.2 Obiettivi e organizzazione

Gli obiettivi devono essere assegnati ai pertinenti livelli dell'organizzazione e adeguati alla sua dimensione e finalità.

Obiettivi e livelli dell'organizzazione

La ISO/IEC 27001 utilizza il solo termine obiettivi, mentre altri testi [68, 94]

utilizzano termini, solitamente inglesi, come vision, mission, goal e target per differenziare diversi livelli di dettaglio, come sintetizzato nella figura 15.6.1.

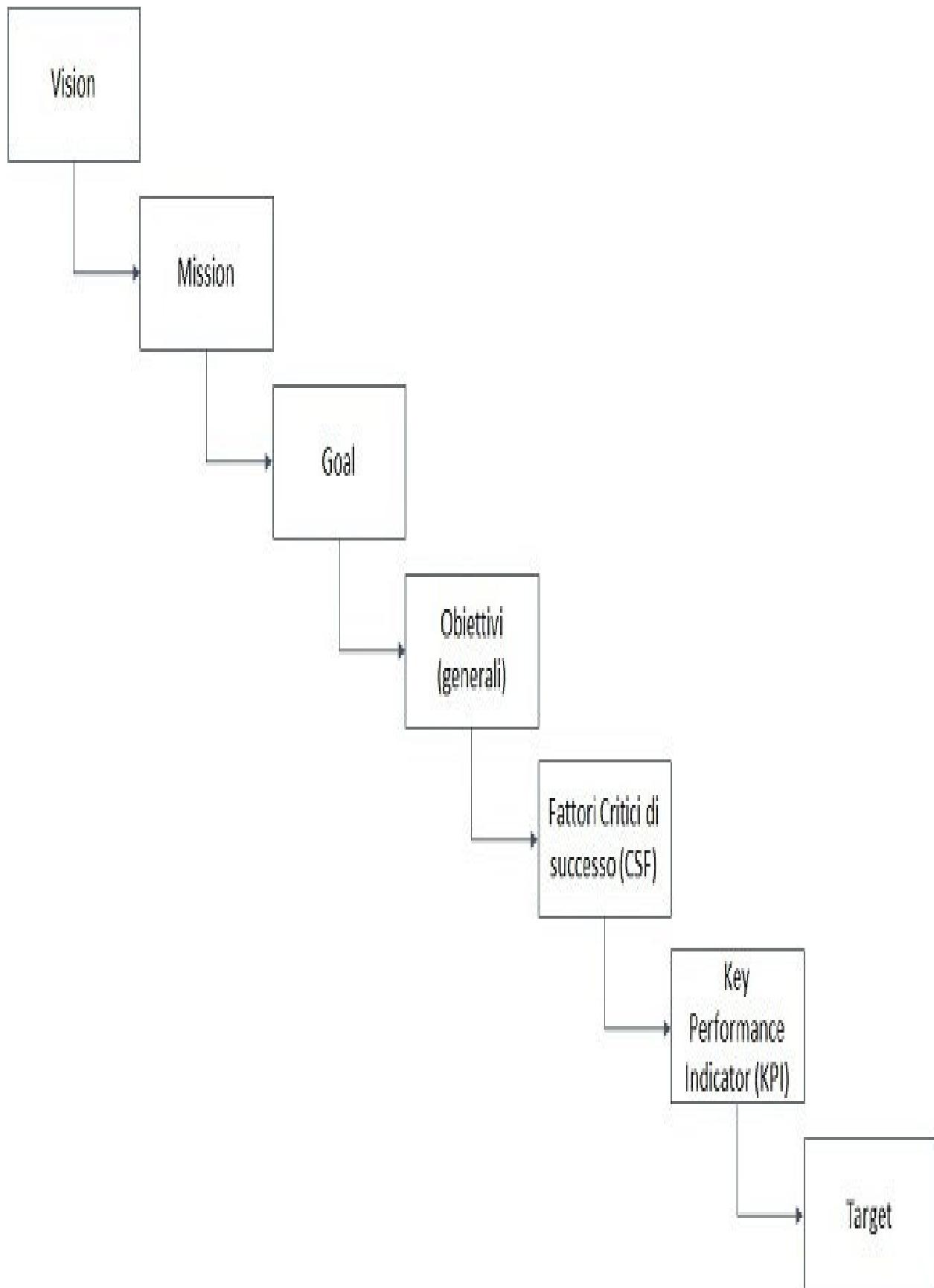


Figura 15.6.1:

Diversi livelli di obiettivi

Gli obiettivi devono essere adeguati a ciascun livello gerarchico: l'alta Direzione stabilisce obiettivi strategici per tutta l'organizzazione e controlla solo dati aggregati; i livelli sottostanti hanno obiettivi tattici coerenti con quelli strategici e da essi derivati. Spesso, per ogni obiettivo strategico si hanno più obiettivi tattici.

Esempio 15.6.18. Nell'esempio 15.6.14 si è visto come l'obiettivo strategico “garantire la riservatezza delle informazioni” abbia originato diversi obiettivi tattici:

l'obiettivo di conformità relativo alla corretta applicazione di tutte le misure previste dalla legislazione, da attuare da parte di tutte le funzioni dell'organizzazione;

l'aggiornamento dei contratti con i fornitori, da attuare da parte della funzione addetta agli acquisti.

Un altro obiettivo strategico, “garantire un elevato livello di disponibilità dei sistemi informatici” deve dare origine a obiettivi per tutte le funzioni coinvolte.

Per esempio:

agli sviluppatori obiettivi sul numero di errori di programmazione che possono bloccare i sistemi;

agli addetti alla conduzione dei sistemi e della rete informatica obiettivi relativi alla disponibilità dei sistemi da loro gestiti.

Obiettivi e dimensione dell'organizzazione

Gli obiettivi devono essere adeguati all'organizzazione e alla sua dimensione.

Esempio 15.6.19. Nelle piccole e medie organizzazioni, l'obiettivo “effettuare audit su tutta l'organizzazione almeno una volta all'anno” è un obiettivo di conformità.

In un'organizzazione di grandi dimensioni, un obiettivo simile può essere espresso in modo diverso: “effettuare audit su tutta l'organizzazione almeno ogni tre anni”. Ogni anno, questo obiettivo potrebbe essere declinato come obiettivo di prestazione: “sottoporre ad audit almeno il 33% dell'organizzazione”.

Il cruscotto degli obiettivi

Gli obiettivi devono essere tenuti sotto controllo dai loro responsabili. Per questo, alcuni realizzano un cruscotto (dashboard) degli obiettivi (alcuni utilizzano il termine indicatori) che dovrebbe mostrare le misurazioni effettuate per ciascun obiettivo e di quanto il valore registrato si scosta dall'obiettivo, in

positivo o in negativo. Ciò dovrebbe permettere ai responsabili degli obiettivi di agire per tempo quando opportuno.

La norma non richiede la presenza di questi cruscotti, ma possono essere utili soprattutto se, per gli obiettivi di prestazione, mostrano i dati in tempo reale.

Si osservi che ogni funzione, compresa la Direzione, deve disporre di analisi relative ai propri obiettivi e non necessariamente a quelli di responsabilità altrui. Quando un obiettivo dipende da altri (per esempio, la disponibilità dipende dai sistemi informatici dalla disponibilità delle applicazioni, dei sistemi e della rete), i risultati di sintesi devono essere coerenti con i risultati di dettaglio. Il responsabile dell'obiettivo generale non deve necessariamente avere a disposizione in tempo reale i dettagli degli obiettivi, ma, in caso di necessità, poterli analizzare.

Esempio 15.6.20. Il responsabile dei sistemi informatici di una grande struttura ha come obiettivo la disponibilità del 99,5% di certi servizi informatici. Ha quindi dato come obiettivo ai responsabili dei sistemi e della rete obiettivi di disponibilità pari al 99,7%.

Solo in caso di scostamenti rilevanti rispetto alla disponibilità complessiva del 99,5% è tenuto a informarsi sui dettagli relativi alle prestazioni dei sistemi e della rete.

I responsabili dei sistemi e della rete non sono tenuti a conoscere l'obiettivo generale, ma potrebbe essere utile comunicarlo per dare un senso al loro obiettivo.

15.7 Processi di supporto

I processi di supporto richiesti dallo standard sono quelli di gestione delle risorse, delle competenze, della consapevolezza, della comunicazione e dei documenti.

15.7.1 Risorse

Il requisito relativo alle risorse si riduce alla richiesta di garantire le risorse necessarie per soddisfare l'obiettivo di stabilire, attuare, mantenere e migliorare il sistema di gestione per la sicurezza delle informazioni.

Tra le risorse sono comprese quelle economiche e quelle materiali (siti, sistemi informatici, eccetera). Il personale, interno ed esterno, è visto come una risorsa e a esso sono dedicati i due paragrafi successivi.

Questo requisito deve essere attuato seguendo un ciclo PDCA: stabilire quali sono le risorse necessarie, reperirle, monitorarne l'adeguatezza e intervenire quando sono insufficienti.

Per reperire le risorse deve essere seguito un processo di budget economico, sottinteso dalla norma.

15.7.2 Competenze e consapevolezza

La gestione del personale è oggetto del paragrafo 12.4. Si ricorda che il requisito non si applica al solo personale dipendente.

Qui è importante osservare l'applicazione del ciclo PDCA richiesto implicitamente dalla norma, soprattutto per la gestione delle competenze.

15.7.2.1 Competenze e formazione

Questo argomento è trattato nel paragrafo 12.4.3 di questo libro.

Le competenze relative alle politiche, alle regole di sicurezza delle informazioni e alle procedure da seguire sono argomento del paragrafo successivo dedicato alla consapevolezza. Il paragrafo dedicato alle competenze riguarda quelle tecniche come a esempio la conoscenza di: ISO/IEC 27001, legislazione in materia di privacy, sistemi UNIX, firewall CISCO, regole di programmazione sicura.

La norma richiede di:

documentare le competenze necessarie per garantire l'efficacia del sistema di gestione per la sicurezza delle informazioni;

documentare le competenze in possesso delle persone impiegate dall'organizzazione, inclusi eventuali consulenti, considerando l'istruzione, la formazione, l'addestramento e l'esperienza (alcune organizzazioni mantengono curriculum vitae aggiornati delle singole persone);

pianificare e realizzare azioni per disporre delle competenze mancanti (corsi di formazione, affiancamenti, assunzioni o inserimento di consulenti);

valutare l'efficacia delle azioni intraprese (nel caso di piccole organizzazioni, questo può avvenire attraverso una breve relazione annuale).

15.7.2.2 Consapevolezza

Di questo argomento si tratta nel paragrafo 12.4.3.3.

Le attività di sensibilizzazione devono riguardare quanto meno:

la conoscenza della politica di sicurezza delle informazioni;

come ciascuno può contribuire all'efficacia del sistema di gestione per la sicurezza delle informazioni (questo include, quindi, la conoscenza delle procedure applicabili, da ottenere attraverso appropriate attività di sensibilizzazione);

i benefici di un sistema di gestione per la sicurezza delle informazioni efficace;

le conseguenze (da gestire secondo un processo disciplinare prestabilito) del mancato adeguamento ai requisiti del sistema di gestione per la sicurezza delle informazioni.

15.7.3 Comunicazione

La norma richiede di individuare quando è necessario comunicare verso l'interno o verso l'esterno e di stabilire, per ogni tipo di comunicazione:

cosa comunicare;
quando comunicare;
chi deve comunicare;
chi sono gli interlocutori interni ed esterni all'organizzazione con cui comunicare.

Questo requisito può riguardare molti aspetti del sistema di gestione per la sicurezza delle informazioni. Le comunicazioni possono infatti riguardare processi direzionali o di pubbliche relazioni esterne (e hanno come oggetto politiche, incidenti, crisi) o interne (con oggetto politiche, incidenti, procedure, ruoli e responsabilità) o processi operativi (comprendendo la gestione degli aggiornamenti ai sistemi informatici, degli incidenti, degli audit).

Esempio 15.7.1. Il processo di gestione dei cambiamenti software presenta molti elementi di comunicazione, tra cui:

la richiesta del richiedente il cambiamento;
il coinvolgimento del personale più appropriato per valutare la richiesta;
il coinvolgimento del personale più appropriato per attuare la richiesta;
la segnalazione agli addetti ai test di effettuarli;
la comunicazione agli addetti alla conduzione dei sistemi informatici di installare in ambiente di produzione gli oggetti cambiati;
la comunicazione preventiva agli utenti del cambiamento;

la comunicazione al richiedente dell'avvenuto cambiamento.

La norma non richiede di documentare questo aspetto, ma le comunicazioni sono parte integrante dei processi e quindi andrebbero descritte nelle relative procedure.

15.7.4 Informazioni documentate

Un'organizzazione deve disporre delle informazioni documentate utili al proprio funzionamento e a dimostrare la conformità alla ISO/IEC 27001. Per comprendere meglio questo argomento, se ne fornisce la definizione.

Informazioni documentate: informazioni da tenere sotto controllo e mantenute da un'organizzazione, insieme con il mezzo che le contiene.

Nota: le informazioni documentate possono essere in ogni formato e mezzo ed essere originate da qualunque sorgente.

Nota: le informazioni documentate possono riferirsi al sistema di gestione, inclusi i suoi processi, o a informazioni necessarie all'organizzazione per funzionare (documentazione) o a prove dei risultati ottenuti (registrazioni).

La precedente edizione della ISO/IEC 27001, così come altre norme, trattava di documenti e registrazioni. L'HLS ha preferito non distinguere propriamente tra questi due concetti e ha introdotto le informazioni documentate. Di questo

argomento si tratta nel paragrafo 12.1.

È qui importante ricordare un punto molto chiaro e importante della norma, ossia che la quantità di informazioni documentate da prevedere dipende:

dalla dimensione dell'organizzazione (se è molto grande, può essere più utile disporre di più documenti perché necessari a coordinare un elevato numero di persone);

dai tipi di attività e processi del sistema di gestione;

dai prodotti realizzati o dai servizi offerti, anche in virtù della normativa applicabile e dei requisiti delle parti interessate;

dalla competenza delle persone (se sono molto competenti, alcune procedure possono ridursi a delle check list, oppure essere inutili).

15.8 Attività operative

Il capitolo sulle operations è breve e si limita a richiedere di effettuare la pianificazione operativa e attuare quanto stabilito.

15.8.1 La pianificazione e il controllo dei processi operativi

Nel capitolo 8 dello standard si chiede espressamente di pianificare nel dettaglio i processi, di attuare le azioni pianificate e quanto necessario per realizzare gli obiettivi.

Questo richiamo alla pianificazione può essere fuorviante rispetto alla pianificazione del capitolo 6 dello standard (paragrafo 15.6). Inoltre, il titolo “attività operative” per un capitolo che tratta di attività tattiche, ossia di pianificazione dei controlli e dei processi, è inadeguato.

La norma, sempre in questo capitolo, richiede di tenere sotto controllo le modifiche pianificate; questo è equivalente a monitorare le azioni e valutarne l’efficacia (paragrafo 15.6.4.1). Richiede inoltre di riesaminare le conseguenze dei cambiamenti volontari, al fine di pianificare e attuare delle azioni per mitigare eventuali effetti negativi; questo è equivalente a gestire le non conformità e le azioni correttive, oggetto dei paragrafi 15.10.1 e 15.10.2.

Un ulteriore requisito riportato nell’ambito delle attività operative, più pertinente alla pianificazione del sistema di gestione, richiede di individuare, determinare e tenere sotto controllo i processi affidati all’esterno. Tra questi vi sono quelli affidati ai fornitori e agli outsourcer i cui controlli di sicurezza applicabili sono oggetto del paragrafo 12.12.

15.8.2 Valutazione e trattamento del rischio relativo alla sicurezza delle informazioni

Nel capitolo 8 dello standard si trova un richiamo alla valutazione e trattamento del rischio relativo alla sicurezza delle informazioni, esaminato nei paragrafi 15.6.2 e 15.6.3.

Qui è aggiunto il requisito di mantenere registrazioni dei risultati della valutazione e del trattamento del rischio relativo alla sicurezza delle informazioni.

15.9 Valutazione delle prestazioni

Nel capitolo 9, la norma tratta di monitoraggio, misurazione, analisi, valutazione, audit interni e riesami di Direzione, a cui sono dedicati i paragrafi successivi.

15.9.1 Monitoraggio, misurazione, analisi, valutazione

La norma richiede di valutare le prestazioni della sicurezza delle informazioni e l'efficacia del sistema di gestione per la sicurezza delle informazioni mediante monitoraggi e misurazioni relativi a processi e controlli di sicurezza.

La norma non richiede di monitorare e misurare le persone perché l'accento è posto sui processi e sui controlli di sicurezza; questo non impedisce però di effettuare valutazioni sulle capacità e prestazioni di ciascuno, sui possibili percorsi di crescita professionale o gerarchica. Si ricorda che in Italia tali monitoraggi e misurazioni sono da limitare in accordo con lo Statuto dei lavoratori (Legge 300 del 1970, che nel 2016 è stato modificato per ammettere controlli “per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale”).

Nei paragrafi successivi sono descritti i monitoraggi, le misurazioni e il processo che li riguarda e successivamente alcuni falsi miti relativi alle misurazioni e si esamina la scelta di cosa monitorare e misurare.

15.9.1.1 I monitoraggi

Di monitoraggio si discute parzialmente nel paragrafo 12.9.6. La definizione della ISO/IEC 27000 è la seguente.

Monitoraggio: Determinazione dello stato di un sistema, di un processo o di un'attività.

Nota: per la determinazione dello stato, potrebbe essere necessario verificare, sovrintendere o osservare.

I monitoraggi non devono essere limitati a quelli tecnologici, ma essere estesi ai processi; possono quindi venire effettuati attraverso l'osservazione diretta o, quando possibile, con strumenti automatici.

Esempio 15.9.1. Esempi di strumenti per il monitoraggio sono:

ticketing per monitorare l'avanzamento della gestione degli incidenti e dell'esecuzione dei cambiamenti;

programmazione delle attività (audit, verifica dei ripristini dei backup, test di continuità, eccetera) per monitorare se sono svolte come previsto;

rilevazione degli eventi sui sistemi informatici.

15.9.1.2 Le misurazioni

La ISO/IEC 27000 fornisce le seguenti definizioni.

Misurazione: processo per determinare un valore.

Metodo di misurazione: sequenza logica di operazioni [...] usate per quantificare un attributo rispetto a una scala specificata.

Nota: [...] si possono distinguere due tipi di metodi di misurazione: soggettivo (che include un giudizio umano) e oggettivo (basato su regole numeriche).

Alcuni usano il termine indicatore al posto di misura, perché ritenuto più evocativo.

Come accennato nel paragrafo 15.6.5.1, il termine misurazione è utilizzato per variabili e per attributi.

Per quanto riguarda la nota, la soggettività (o percezione) dovrebbe intervenire solo in fase di valutazione dei risultati delle misurazioni, come approfondito nel paragrafo successivo. La raccolta e l'analisi dei dati dovrebbe essere il più oggettiva possibile, anche se, come nell'analisi del rischio (paragrafo 7.1), alcune misurazioni includono elementi soggettivi.

Le misurazioni sono comunemente effettuate con strumenti automatici o fogli di calcolo.

La norma richiede di garantire:

la ripetibilità delle misurazioni: in condizioni uguali, i risultati delle misurazioni devono essere uguali;

la comparabilità delle misurazioni: misurazioni condotte in momenti diversi devono permettere una valutazione di tendenze o cambiamenti.

Questo non vieta di modificare i monitoraggi e le misurazioni: è possibile aggiungere o eliminare misurazioni a seconda di mutate esigenze.

Si noti infine che la ISO/IEC 27001 pone l'attenzione soprattutto sugli obiettivi e quindi le misurazioni non dovrebbero essere fini a sé stesse, ma dettate dalle esigenze e dagli obiettivi dell'organizzazione.

15.9.1.3 Cosa monitorare e misurare

Quando si tratta di sicurezza delle informazioni, poche misure sono significative e tra esse vi sono:

i tempi di indisponibilità dei sistemi e delle loro componenti;

i tempi di risoluzione degli incidenti in funzione della loro gravità;

il livello di rischio.

Altre misure possono dipendere dall'organizzazione e dalla capacità di utilizzo dei sistemi di ticketing; tra di esse vi potrebbero essere:

i tempi di patching calcolati dalla segnalazione della vulnerabilità;

il numero di difetti (bug) rilevati nei software sviluppati;

i tempi di correzione delle non conformità di produzione;

il numero di reclami dei clienti e pertinenti la sicurezza delle informazioni e l'incidenza delle penali sul fatturato.

Alcune misurazioni non significative riguardano il numero di intrusioni o di altri attacchi, dato che non sempre sono rilevati e sono molto rari; stabilire una misurazione di questo tipo potrebbe dare un falso senso di sicurezza.

Ovviamente, ogni attacco deve essere oggetto di monitoraggio.

Nonostante le critiche alle misurazioni presentate nel seguito, è comunque utile disporne perché possono aiutare a prendere alcune decisioni. La ISO/IEC 27004 [88] riporta molti esempi e sono disponibili altre proposte, anche se spesso riferite alla sola informatica [44, 68, 140]; se ne raccomanda la lettura per ampliare il numero di esempi a disposizione.

15.9.1.4 Il processo di monitoraggio, misurazione, analisi e valutazione

I monitoraggi e le misurazioni possono riguardare prodotti, sistemi, processi, attività e controlli di sicurezza.

Esempio 15.9.2. Il processo di gestione delle utenze può essere valutato attraverso:

monitoraggi: mediante un'analisi puntuale degli utenti registrati sui sistemi rispetto a quelli previsti, intervenendo quando si osservano degli scostamenti;

misurazioni: calcolando ogni anno quanti sono gli scostamenti tra gli utenti registrati sui sistemi e quelli previsti, intervenendo, se è il caso, sul processo al fine di migliorarlo.

Il processo relativo ai monitoraggi e alle misurazioni descritto dalla norma è composto dalle seguenti attività, secondo il ciclo PDCA:

plan: identificazione di:

cosa monitorare e misurare e, quindi, degli stati da monitorare o delle variabili da misurare;

parametri di confronto (soglie di accettabilità, schemi di comportamento, eventi specifici);

metodi di misurazione e monitoraggio tali da garantire risultati validi (comparabili e ripetibili) e con il livello di accuratezza atteso;

frequenze con cui effettuare i monitoraggi e raccogliere i dati delle misurazioni;

responsabili della raccolta dei dati di monitoraggio e di misurazione e della loro valutazione;

metodi di presentazione dei risultati;

frequenze con cui analizzare e valutare i risultati e relative responsabilità;

do: raccolta dei dati secondo quanto pianificato;

- check: analisi e ponderazione (giudizio) per spiegare la natura di quanto monitorato o misurato;
- act: scelta e attuazione degli interventi per trattare eventi specifici o modificare andamenti.

Quando il ciclo PDCA viene ripetuto è possibile modificare gli stati da monitorare, le variabili da misurare, i metodi di raccolta e i parametri di valutazione dei dati, a seconda degli obiettivi dell'organizzazione.

La ISO/IEC 27001 richiede di documentare i monitoraggi e le misurazioni, conservando, per un tempo adeguato, le presentazioni dei risultati e le loro valutazioni.

15.9.1.5 I falsi miti relativi alle misurazioni

Nel paragrafo 9.3.1.1 si accenna al falso mito del miglioramento continuo e di come questo possa rappresentare un problema quando si vuole migliorare il livello di rischio. Nel paragrafo 15.6.5 si accenna inoltre alla direzione per obiettivi e delle relative critiche. Nel seguito si parla di altri falsi miti.

Se non lo misuri, non puoi gestirlo

Questo falso mito è sostenuto riportando la seguente frase di Lord Kelvin pronunciata nel 1893:

Se puoi misurare ciò di cui parli e puoi esprimerlo con un numero, allora conosci

qualcosa del tuo soggetto; ma se non puoi misurarlo, allora la tua conoscenza è scarsa e insoddisfacente.

Lord Kelvin era un grande fisico e ingegnere e si riferiva alle grandezze fisiche. Quando si parla di sistemi di gestione, si parla soprattutto di organizzazione e di scienze sociali, ed è quindi errato utilizzare concetti delle scienze naturali. Si aggiunga che in fisica è molto difficile misurare le relazioni tra più di due oggetti, mentre le scienze sociali, incluse quelle relative all'organizzazione del lavoro, studiano le relazioni tra una moltitudine di persone.

Si osservi infine che la sicurezza delle informazioni è difficilmente misurabile. Importante, per la sicurezza è “conoscere” e monitorare, non misurare.

Esempio 15.9.3. All'inizio del 2014, fu scoperto The Mask, un malware di tipo advanced persistent threat (APT): da almeno 7 anni serviva a entità sconosciute a spiare agenzie governative. Nessuna misura avrebbe potuto rilevarlo, solo un attento monitoraggio dei sistemi.

Questo falso mito è sostenuto da chi promuove la (falsa) credenza secondo cui “un buon manager lo è in qualunque tipo di organizzazione”. La conoscenza di un’organizzazione, elaborando il pensiero di Deming (paragrafo 15.6.5) si ottiene soprattutto comprendendone la cultura, i punti di forza, le relazioni personali tra i diversi responsabili e i processi. Ma questi parametri sono difficili da comprendere e da misurare, come sanno i veri buoni manager.

Numerosità delle misurazioni

Il secondo falso mito riguarda la numerosità delle misurazioni da riportare alla Direzione e ai diversi livelli gerarchici, solitamente promosso da consulenti e auditor. Questo ha come effetto una produzione sovrabbondante di cruscotti e report, non necessari nella pratica e non utilizzati.

Esempio 15.9.4. In un'organizzazione, negli anni Novanta, il responsabile dei servizi informatici interni individuò un'elevata produzione di report da parte del reparto dedicato alle stampe (a quei tempi, alcune organizzazioni avevano questi reparti).

Decise quindi di interrompere questo servizio di stampa e di riprenderlo solo per i report per i quali avesse suscitato lamentele da parte dei destinatari. Non ricevette quasi alcuna lamentela, dimostrando così che quei report non erano necessari.

Nella pratica, i responsabili di un'organizzazione hanno la necessità di disporre periodicamente dei risultati di poche misurazioni. Solo in caso di eventi straordinari potrebbe essere necessario disporre di ulteriori dettagli.

Esempio 15.9.5. Un automobilista, normalmente, ha bisogno di poche misurazioni: velocità, chilometri percorsi e livello della benzina; ha anche bisogno di pochi monitoraggi, come il livello dell'olio.

Altre misurazioni, peraltro fondamentali, non sono verificate periodicamente dal guidatore: pressione degli pneumatici e livello dell'acido delle batterie. Questi parametri sono verificati periodicamente dai meccanici.

Allo stesso modo, un responsabile di un'organizzazione ha bisogno di pochi dati da verificare periodicamente e da riportare in un report. Ovviamente, questi dati devono essere raccolti in modo tale che, in caso di necessità, si possa risalire ai dati elementari e alla loro origine.

Un obiettivo per ogni misurazione

Alcuni richiedono di attribuire un obiettivo a ciascuna misurazione. Non sempre questo è necessario, perché le misurazioni possono servire solo per fare confronti tra momenti diversi o per rilevare delle situazioni anomale. Sarebbe invece opportuno individuare valori di riferimento delle misurazioni.

Un eccessivo numero di obiettivi, così come di misurazioni, non è utile all'organizzazione, che può concentrarsi solo su un numero ridotto di essi.

Esempio 15.9.6. Per alcuni servizi informatici è utile sapere quanti utenti li utilizzano per poter fare previsioni in merito alla capacità dei sistemi e alle risorse da impiegare. A questi numeri, spesso, non è associato alcun obiettivo, né è interesse dell'organizzazione monitorarlo.

Esempio 15.9.7. In un'organizzazione, il sistema di controllo automatico degli accessi fisici basato sulla lettura di una tessera a microprocessore tiene traccia di quante volte nella giornata è negato l'accesso alle persone a causa

della non validità della tessera.

Alla sede in questione hanno accesso molti fornitori e collaboratori che spesso, per errore e automatismo, provano ad accedere con una tessera abilitata per un'altra sede perché lì normalmente impiegati.

Il numero dei tentativi di accesso falliti è quindi una misurazione ritenuta inutile, così come l'assegnazione di obiettivi a essa collegati.

15.9.2 Audit interni

Gli audit sono introdotti nel paragrafo 12.15.3. Gli audit interni dovrebbero essere condotti secondo quanto previsto dalla norma ISO 19011, alla quale si ispirano i paragrafi successivi.

Si ricorda che i criteri di audit per gli audit interni sono le procedure interne. Gli audit interni possono richiedere audit a fornitori; per questi, i criteri di audit sono quelli stabiliti sul contratto o accordo stipulato.

15.9.2.1 Il programma di audit

La prima cosa da fare è predisporre un programma di audit, individuando le aree da sottoporre ad audit; tra di esse vi sono i processi, i controlli di sicurezza e i fornitori critici.

Per garantire la sistematicità dell'audit, devono essere considerate tutte le aree che compongono l'ambito del sistema di gestione per la sicurezza delle informazioni. Per ciascuna area o processo bisogna quindi stabilire il tempo necessario alla conduzione dell'audit, includendo quello per i trasferimenti e la preparazione del rapporto.

A questo punto è possibile valutare quante singole verifiche è possibile condurre in uno o più anni e quindi stabilire le frequenze con cui verificare ciascuna area.

Nelle piccole organizzazioni, dove il tempo complessivo di audit è di poche giornate, si programma un audit completo ogni anno. Nelle grandi organizzazioni, dove un audit di tutte le aree può richiedere molto tempo e il coinvolgimento di più auditor, è possibile suddividere le attività in più anni. In questo caso, le aree più critiche (a causa della loro complessità, dei risultati degli audit precedenti o di cambiamenti che le hanno coinvolte) devono essere verificate più di frequente, mentre quelle meno critiche anche una volta ogni 3 o 5 anni (per esempio, se il sito di disaster recovery non è presidiato, non subisce cambiamenti e una prima visita ha dimostrato la sua adeguata gestione, potrebbe essere necessario sottoporlo raramente ad audit). È importante documentare le scelte fatte e dimostrare che tutte le aree sono state considerate.

Esempio 15.9.8. In tabella 15.9.1 è presentato, come esempio, un estratto di un programma triennale di una grande impresa.

La sigla “gu” indica le giornate uomo necessarie a ciascun audit; queste sono calcolate considerando il tempo di spostamento tra le sedi, il tempo di redazione e condivisione del rapporto di audit e il tempo per verificare l'efficacia delle azioni correttive pianificate a fronte di eventuali non conformità rilevate dagli auditor.

AREA	2022	2023	2024	Criteri
Funzioni interne				
Sicurezza fisica della sede	2 gu			Frequenza: triennale. Procedura "Sicurezza fisica"
Sicurezza fisica del CED		2 gu		Frequenza: triennale. Procedura "Sicurezza CED"
Gestione dell'infrastruttura: sistemi informatici dedicati ai clienti (database Oracle)	1 gu			Frequenza: triennale. Procedure: <ul style="list-style-type: none">- "Gestione dei cambiamenti";- "Gestione degli utenti e delle autorizzazioni (clienti)";- "Conduzione dei sistemi";- ...
Gestione dell'infrastruttura: sistemi informatici dedicati ai clienti (database SQL Server)		1 gu		...
Gestione dell'infrastruttura: sistemi informatici dedicati ai servizi interni	3 gu			Frequenza: triennale. Procedure: <ul style="list-style-type: none">- "Gestione dei cambiamenti";- ...
Gestione dell'infrastruttura: rete informatica		2 gu		Frequenza: triennale. Procedure: <ul style="list-style-type: none">- "Gestione dei cambiamenti";- ...
Progettazione e acquisizione applicazioni IT per i servizi erogati ai clienti	3 gu			Frequenza: triennale. Procedure: <ul style="list-style-type: none">- "Gestione dei cambiamenti";- "Sviluppo sicuro";- ...
Progettazione e acquisizione applicazioni IT per i servizi erogati all'interno		3 gu		Frequenza: triennale. Procedure: <ul style="list-style-type: none">- "Gestione dei cambiamenti";- "Sviluppo sicuro";- ...
Service desk e SOC: Gestione degli incidenti	2 gu	2 gu		Frequenza: annuale. Procedure: <ul style="list-style-type: none">- "Gestione dei dispositivi personali";- "Gestione degli incidenti";- ...
Business continuity Management	2 gu			...
Ufficio acquisti		1 gu		...
Ufficio personale		1 gu		...
...				
Fornitori				
Fornitore hosting - Milano	3 gu			Contratto
Fornitore hosting SAP - Roma		3 gu		Contratto
...				
TOT GIORNATE	16 gu	15 gu		

Tabella 15.9.1:

Esempio di programma di audit

Devono essere stabilite le caratteristiche degli auditor, in particolare riguardanti la loro competenza ed esperienza, come tutto il personale con responsabilità relative alla sicurezza delle informazioni. Gli auditor devono essere indipendenti dalle aree che verificano, come previsto dalla separazione dei ruoli (paragrafo 12.3.2): non devono essere impiegati in quelle aree o esserne responsabili; potrebbero però aver collaborato alla scrittura delle procedure utilizzate come criteri dell'audit.

Il programma deve riportare i metodi da adottare per l'audit: se fare uso o meno di check list, se effettuare test pratici, se a sorpresa o no.

Il programma di audit dovrebbe essere preparato e aggiornato valutandone i rischi (non solo di sicurezza delle informazioni). Tra questi rischi vi sono, per esempio, quelli originati da: tempi, strumenti e formazione insufficienti per condurre gli audit programmati; competenze degli auditor insufficienti; problemi di coordinamento tra gli auditor; errori nella protezione delle registrazioni di audit; mancato monitoraggio dei risultati degli audit; mancanza di disponibilità o cooperazione delle persone da coinvolgere durante l'audit; metodi di campionamento inadeguati.

Il programma di audit deve essere soggetto al ciclo PDCA ed essere quindi modificato a seconda delle esigenze che si dovessero presentare: cambiamenti all'ambito del sistema di gestione, ai controlli di sicurezza, ai processi e così via. Le opportunità (per esempio condurre più audit nel corso di un singolo incontro o ridurre i tempi e le distanza degli spostamenti) dovrebbero essere valutate.

15.9.2.2 Il piano di audit

Una volta stabilite le aree da verificare, deve essere inviato un piano di dettaglio alle persone da coinvolgere o al loro responsabile e con gli orari ben specificati, come si vede dalla tabella 15.9.2.

Piano di audit: Gestione dell'infrastruttura: sistemi informatici dedicati ai clienti (database Oracle)		
Orario - giorno 1	Area	Auditor
09.00 - 09.30	Riunione di Apertura	Auditor A e B
09.30 - 10.30	Analisi documenti e organizzazione	Auditor A e B
10.30 - 12.00	Controllo accessi: processo e configurazione sistemi	Auditor A
10.30 - 12.00	Gestione dei cambiamenti: change minori e progetti	Auditor B
12.00 - 13.00	Gestione dei media	Auditor A
12.00 - 13.00	Patching	Auditor B
13.00 - 14.00	Pausa Pranzo	
14.00 - 15.30	Configurazione dei sistemi: regole e verifiche	Auditor A
15.30 - 17.00	Inventario degli asset	Auditor A
14.00 - 15.30	Monitoraggi e gestione degli eventi	Auditor B
15.30 - 16.30	Gestione dei backup e dei ripristini	Auditor B
16.30 - 17.00	Antivirus	Auditor B
17.00 - 17.30	Riunione Gruppo di Verifica	Auditor A e B
17.30 - 18.00	Riunione di Chiusura giorno 1 e condivisione rilievi	Auditor A e B
Orario - giorno 2	Area	Auditor
09.00 - 09.30	Riunione di Apertura e sintesi dei risultati del giorno 1	Auditor A e B
09.30 - 10.30	Monitoraggio fornitori	Auditor A
10.30 - 12.00	Competenze del personale	Auditor A
09.30 - 12.00	Continuità, ridondanze e test	Auditor B
12.00 - 12.30	Riunione Gruppo di Verifica	Auditor A e B
12.30 - 13.00	Riunione di Chiusura giorno 1	Auditor A e B

Tabella 15.9.2:

Esempio di piano di audit

Il piano è importante affinché sia garantita la presenza delle persone da intervistare e queste non restino a disposizione degli auditor per più tempo del necessario.

Nella preparazione del piano di audit, vanno considerati i rischi di non raggiungimento degli obiettivi di audit (per esempio se il tempo per le attività critiche è insufficiente o l'auditor assegnato per condurle non ha le adeguate competenze) e per l'organizzazione (per esempio se un auditor compromette informazioni critiche).

15.9.2.3 Conduzione di un audit

L'auditor deve verificare il rispetto dei criteri di audit, ossia delle procedure interne o, nel caso di audit ai fornitori, del contratto o accordo, ricercando delle evidenze di audit attraverso la lettura di documenti e registrazioni, interviste verbali, osservazioni e analisi degli strumenti utilizzati.

Il termine evidenza di audit è utilizzato come traduzione non letterale e scorretta (cosiddetta “pigra”) dell’inglese audit evidence; la traduzione corretta sarebbe prova di audit, ma è poco utilizzato.

A inizio audit è sempre opportuno riesaminare la documentazione per verificare

se è adeguata alla normativa vigente, agli standard adottati e agli obiettivi dell’organizzazione. Obiettivo dell’audit interno richiesto dalla ISO/IEC 27001, infatti, è verificare se il personale segue le procedure interne e se queste sono aderenti alla ISO/IEC 27001. Non è corretto pretendere dal personale il rispetto della ISO/IEC 27001, mentre è corretto pretendere il rispetto delle procedure interne.

Esempio 15.9.9. Durante un audit, un operatore si allontanò dal proprio computer senza attivare lo screen saver. A fronte di questa pratica scorretta, l’auditor rilevò anche che l’organizzazione non aveva comunicato al personale alcuna regola relativa agli strumenti informatici incustoditi.

Per questo, l’auditor segnalò una non conformità per la mancanza di regole sul blocco dei computer, non per il comportamento dell’operatore.

L’audit deve essere normalmente condotto presso gli operatori. Condurre gli audit solo con interviste ai dirigenti non è una buona scelta: solo osservando direttamente come operano le persone e gli strumenti che utilizzano è possibile rendersi conto delle pratiche seguite. I dirigenti conoscono quali sono i processi e le politiche generali applicabili, ma spesso, a loro insaputa, non sono seguite completamente. È proprio uno degli obiettivi dell’audit verificare se le procedure sono correttamente e completamente applicate.

Uno dei principi degli audit di un sistema di gestione è che non è necessario analizzare tutte le prove relative a un certo requisito per comprendere quanto è attuato, ma solo un numero sufficiente per avere un giusto grado di fiducia. In altre parole, si procede per campionamento.

Il metodo del campionamento, ovviamente, può condurre a valutazioni scorrette. È quindi necessario prendere atto della possibilità di effettuare un campionamento inadeguato e dei suoi impatti; in altre parole, è sempre necessario essere consapevoli del rischio di audit (ossia dei rischi relativi al programma di audit).

Esempio 15.9.10. Per il principio del campionamento, non è necessario verificare tutte le configurazioni di tutti i firewall per comprendere se sono adeguati: potrebbero bastarne uno o due scelti casualmente.

Il rischio risiede nella possibilità di scegliere l'unico firewall correttamente configurato.

Altri rischi di audit sono relativi alle interferenze degli auditor sui processi. Oltre a quanto già accennato nel paragrafo 12.15.3.2, si osserva che un auditor può rallentare le attività e attivare involontariamente dei meccanismi creando situazioni inattese.

Esempio 15.9.11. Durante un audit in un CED di disaster recovery, la persona intervistata decise di verificare il sistema di continuità dell'energia e, senza che l'auditor lo chiedesse, simulò un blackout. Inutile dire che il sistema non funzionò come previsto.

Fortunatamente, l'azione non ebbe impatti significativi perché il sito di disaster recovery era inattivo.

L'auditor deve segnalare immediatamente se rileva delle mancanze, soprattutto perché potrebbe non aver capito correttamente la situazione e le persone intervistate potrebbero chiarirla meglio. Un approccio diretto consente all'auditor di spiegare le motivazioni per cui una certa prassi o procedura non è corretta.

Ogni mancanza prende il nome di non conformità, oggetto del paragrafo 15.10.1, e può essere classificata come grave o non grave (gli organismi di certificazione hanno spesso due o tre livelli di classificazione, riconducibili a “grave”, “non grave”, “lieve”).

L'auditor non deve verificare solo il rispetto formale dei documenti scritti, ma valutarne l'adeguatezza. Nel caso della sicurezza delle informazioni, controlli di sicurezza formalmente conformi allo standard o alle procedure interne ma palesemente inadeguati possono portare a non conformità gravi. L'auditor può inoltre rilevare mancanze documentali nella valutazione del rischio (per esempio non identificazione di un rischio o valutazione suffragata da insufficienti considerazioni).

Tutte le non conformità devono essere scritte in un rapporto ed essere accompagnate dal riferimento preciso alla politica o procedura o contratto o accordo non rispettato.

A fronte di non conformità gravi è possibile concordare una verifica straordinaria per verificarne il trattamento.

Alcuni auditor promuovono l'uso di check list per condurre le attività. Prima di realizzarle e usarle bisognerebbe chiedersi perché le procedure già in uso non

sono sufficienti e non possono fungere da check list. Troppo spesso le procedure sono difficili da seguire per gli audit (e, quindi, probabilmente anche per gli utilizzatori) o non riportano tutti gli elementi che un auditor vorrebbe verificare. In questo caso, anche per seguire il principio di trasparenza, sarebbe meglio che l'auditor chiedesse dei miglioramenti alle procedure esistenti, piuttosto che crearne di parallele sotto forma di check list.

15.9.2.4 Conclusione di un audit

I risultati degli audit devono essere riferiti ai responsabili delle diverse aree coinvolte nell'audit e ai livelli gerarchici superiori, inclusa la Direzione.

Al termine di ogni audit, come già detto, può essere necessario aggiornare il programma di audit al fine di migliorarlo.

15.9.3 Riesami di Direzione

Il riesame di direzione è un'attività tra le più importanti per un sistema di gestione, ma anche la più sottovalutata.

Il riesame dovrebbe presentare una previsione di spesa per la sicurezza delle informazioni e quindi dovrebbe costituire parte del budget annuale complessivo dell'organizzazione.

Come per ogni previsione di spesa, bisogna analizzare quanto successo nell'anno precedente, le necessità emerse e cosa potrebbe succedere l'anno successivo.

Più nel dettaglio, la norma richiede di analizzare:

lo stato di avanzamento dei progetti e delle azioni stabilite nel riesame precedente (è interessante osservare quanto spesso questo elemento venga ignorato, come se le decisioni prese in precedenza non fossero degne di un controllo da parte di chi le ha decise);

i fattori interni ed esterni del contesto cambiati rispetto al riesame precedente e riguardanti la sicurezza delle informazioni;

le non conformità emerse dal riesame precedente e le azioni correttive avviate nello stesso periodo, per quanto appropriato al livello delle persone coinvolte nel riesame;

i risultati dei monitoraggi e delle misurazioni, per quanto di interesse della Direzione;

i risultati degli audit interni o condotti da parti esterne, tra cui organismi di certificazione, clienti e autorità;

lo stato di completamento degli obiettivi di sicurezza delle informazioni;

le segnalazioni dalle parti interessate, tra cui i reclami;

i risultati della valutazione del rischio e lo stato del piano di trattamento del rischio relativo alla sicurezza delle informazioni;

le opportunità di miglioramento, sia procedurale che tecnico, di interesse per il livello delle persone coinvolte nel riesame.

Ogni elemento va presentato a un livello di sintesi utile ai partecipanti al riesame (per esempio, la Direzione necessita di un elevato livello di sintesi), in modo che sia possibile trarre delle conclusioni, ossia:

una valutazione complessiva sull’adeguatezza ed efficacia del sistema di gestione per la sicurezza delle informazioni;

quali miglioramenti pianificare e attuare, in particolare quali azioni di riduzione del rischio avviare;

le risorse necessarie per attuare quanto deciso e mantenere la conformità allo standard: persone, competenze, risorse materiali e, conseguentemente, risorse economiche; questo punto è implicito nella norma perché le decisioni della Direzione corrispondono a obiettivi a cui è necessario allocare delle risorse (paragrafo 15.6.5).

Quanto analizzato e deciso va verbalizzato.

Se la Direzione non ha completa autonomia di spesa, il riesame dovrebbe corrispondere alla richiesta di budget per la sicurezza delle informazioni da inoltrare ai livelli pertinenti dell’organizzazione.

La norma richiede di effettuare un riesame a “intervalli pianificati”. La frequenza dovrebbe essere almeno annuale e collegata al processo di budget complessivo dell’organizzazione. In molti casi può essere opportuno prevedere ulteriori riesami parziali più frequenti o riesami straordinari quando si verificano cambiamenti significativi.

15.10 Miglioramento

Il capitolo 10 dello standard è dedicato al miglioramento e si occupa delle non conformità, delle azioni correttive e del miglioramento continuo. Qui si trattano

anche le azioni preventive, presenti nella norma precedente, ma non nella nuova edizione.

15.10.1 Non conformità

Iniziamo con la definizione proposta dalla ISO/IEC 27000.

Non conformità: mancato soddisfacimento di un requisito.

Un requisito non completamente soddisfatto è pertanto una non conformità.

Esempio 15.10.1. Sono esempi di non conformità:

le prove di ripristino dei backup sono effettuate ogni 2 mesi quando le procedure richiedono un mese;

il mancato completamento dei vulnerability assessment su tutti i sistemi previsti.

Le non conformità si possono riscontrare in molti ambiti, trattati nei paragrafi successivi:

mancato rispetto delle procedure e della ISO/IEC 27001, spesso rilevate durante un audit (non conformità di processo);

prodotti e servizi non realizzati come previsto o progetti che non rispettano la pianificazione o gli obiettivi prefissati (non conformità di produzione o progettazione);

prodotti e servizi consegnati ai clienti non in linea con quanto concordato (reclami e segnalazioni dei clienti);

prodotti e servizi consegnati dai fornitori non in linea con quanto concordato (non conformità di fornitura).

La norma richiede di reagire alle non conformità e, se applicabile, eliminarle con una correzione e affrontarne le conseguenze. L'organizzazione deve anche valutare se intraprendere delle azioni correttive, di cui si parla nel seguito, per evitare che la non conformità si ripeta. La gestione delle non conformità e delle azioni correttive è molto simile alla gestione degli incidenti e dei problemi (paragrafi 12.13.2 e 12.13.4).

Tutte le non conformità vanno registrate insieme alle successive azioni di correzione o contenimento. Le non conformità non devono necessariamente essere registrate da un'unica persona e in un unico modo. Deve però essere scelto un metodo per effettuare delle sintesi e delle statistiche sulle non conformità, in modo da consentire ai diversi livelli gerarchici dell'organizzazione di valutare se sia opportuno intraprendere ulteriori azioni di miglioramento. Per esempio, potrebbe essere utile, come misurazione, conteggiare il numero di non conformità per tipo e ambito e il loro costo.

Il processo di gestione delle non conformità dovrebbe essere documentato in una o più procedure. Per esempio, potrebbe essere prevista una procedura distinta per ciascun tipo di non conformità (di prodotto, di progetto, da reclami dei clienti, di fornitura, eccetera). Inoltre, in organizzazioni che effettuano diverse attività (per esempio, hosting ed erogazione di servizi cloud), potrebbe essere necessario prevedere procedure distinte per ognuna di esse.

15.10.1.1 Non conformità di processo

Le non conformità di processo sono normalmente individuate nel corso degli audit interni o degli audit di organizzazioni esterne come, per esempio, un organismo di certificazione. Le non conformità di processo dovrebbero essere tenute sotto controllo dal responsabile del sistema di gestione per la sicurezza delle informazioni, se presente, o dai coordinamenti pertinenti (paragrafo 12.3.1.5).

La correzione di una non conformità di processo potrebbe richiedere un cambiamento di procedura, non necessariamente un adeguamento delle persone alle procedure.

Spesso, a meno che non si tratti di piccoli errori, una non conformità di processo, per evitare che si ripeta, richiede di intraprendere un'azione correttiva.

Per alcuni, solo questo tipo di non conformità è oggetto della ISO/IEC 27001. Questo punto di vista non è quello proposto da questo libro.

15.10.1.2 Non conformità di produzione o progettazione

Le non conformità di produzione o progettazione riguardano progetti, prodotti e servizi non realizzati come previsto e si verificano spesso nell'ambito della qualità quando si individuano prodotti o semilavorati difettosi o errori nell'erogazione di un servizio (per esempio, al cliente di un'agenzia di viaggi viene consegnato un biglietto aereo per un giorno diverso da quello richiesto). Ciò nonostante, queste non conformità potrebbero avere impatti sulla sicurezza delle informazioni (per esempio, un difetto in un prodotto software o il ritardo di

un progetto).

Esempio 15.10.2. Esempi di non conformità di progettazione o produzione sono:

mancanza di requisiti di sicurezza per le interfacce di input degli utenti di un'applicazione informatica;

mancata connessione di un nuovo servizio informatico ai sistemi di monitoraggio degli eventi e delle vulnerabilità;

mancata previsione di un adeguato controllo accessi a una nuova sede dell'organizzazione;

un backup non riuscito;

un difetto nel software di un'applicazione dovuto a un errore di programmazione;

un errore di configurazione di un prodotto informatico;

il ritardo nella conclusione di un progetto di installazione di una nuova applicazione informatica;

la non completa esecuzione dei test di disaster recovery pianificati.

Quando si parla di sicurezza delle informazioni, alcune non conformità di produzione o progettazione sono incidenti o vulnerabilità.

Malgrado la norma richieda di registrare tutte le non conformità, molti non registrano quelle di progettazione e sviluppo individuate e corrette prima della

conclusione del progetto e se non hanno impatti economici rilevanti.

In caso di mancato rispetto dei piani stabiliti, la non conformità dovrebbe essere trattata analizzandone le cause e ripianificando le attività dove necessario.

Come è intuibile, ciascuno di questi tipi di non conformità è sovente gestito da persone con diverse competenze e con strumenti diversi (fogli di calcolo, verbali di riesame dei progetti, sistemi di ticketing).

15.10.1.3 Reclami e segnalazioni dei clienti

I reclami dei clienti sono anch'essi delle non conformità e dovrebbero essere gestiti prevedendo sempre una risposta alle segnalazioni.

In alcuni casi, i reclami potrebbero essere infondati e ritirati dopo che il cliente è stato contattato. È comunque opportuno tenere traccia anche dei reclami infondati poiché dovrebbero essere registrati sin dal loro ricevimento ed essere tenuti sotto controllo fino a quando non se ne è stabilita la causa.

Esempio 15.10.3. Nel caso del cliente che si lamenta perché il biglietto aereo non è stato emesso dall'agenzia di viaggi con la data corretta, si potrebbe scoprire che la data del biglietto corrisponde a quella richiesta del cliente ed, evidentemente, l'errore è suo.

Nell'ambito della sicurezza delle informazioni, un cliente potrebbe lamentare

delle anomalie di un servizio Internet. Un'analisi potrebbe rilevare che sul suo computer è installato del malware a causa della disattenzione del cliente stesso.

Accanto ai reclami è necessario considerare le segnalazioni dei clienti perché, anche se effettuate senza acrimonia, potrebbero rivelare errori commessi dall'organizzazione.

Esempio 15.10.4. Un utente di un sistema informatico potrebbe chiedere l'installazione di uno specifico programma. Se si dovesse scoprire che quel programma avrebbe già dovuto essere installato sul suo computer, la sua richiesta deve essere registrata come non conformità.

Come le non conformità di produzione e di progettazione, anche i reclami e le segnalazioni dei clienti sono più materia della qualità che della sicurezza delle informazioni, ma potrebbero essere causate da vulnerabilità e incidenti relativi alla sicurezza delle informazioni e quindi essere analizzate con attenzione.

15.10.1.4 Non conformità di fornitura

Le non conformità di fornitura sono quelle relative a prodotti e servizi non corretti consegnati dai fornitori (per esempio il superamento dei tempi massimi di indisponibilità di un servizio informatico).

Come le altre non conformità discusse in precedenza, sono spesso di competenza della qualità, ma potrebbero avere impatti sulla sicurezza delle informazioni e,

pertanto, vanno gestite con attenzione.

Spesso queste non conformità sono gestite dal personale tecnico insieme con l'ufficio acquisti e, nei casi più gravi, l'ufficio legale.

15.10.2 Azioni correttive

Le azioni correttive sono definite come segue nella ISO/IEC 27000.

Azione correttiva: azione per eliminare la causa di una non conformità e prevenirne il ripetersi.

Esse vanno affrontate come i problemi descritti in 12.13.4.

Quando si verifica una o più non conformità, si può decidere di analizzarle con attenzione per determinarne le cause e stabilire se è necessario intraprendere azioni per fare in modo che non si ripetano. Tali azioni (paragrafo 15.6.4) potrebbero richiedere modifiche al sistema di gestione per la sicurezza delle informazioni, ossia a processi, procedure o strumenti utilizzati per attuarli.

Non per tutte le non conformità occorre avviare il processo di gestione delle azioni correttive. Per altre, dopo una prima analisi si potrebbe decidere di non intraprendere alcuna azione a causa dei potenziali impatti, per esempio economici o sul livello di rischio relativo alla sicurezza delle informazioni.

Il processo di gestione delle azioni correttive dovrebbe essere documentato, eventualmente sullo stesso documento in cui è descritto il processo di gestione delle non conformità.

Tutte le azioni correttive devono essere registrate insieme alle non conformità a esse associate, alle analisi effettuate e alle successive pianificazioni e valutazioni dei risultati. Se presente, dovrebbe essere usato il registro di miglioramento descritto nel paragrafo 15.6.4.2.

15.10.3 Azioni preventive

La definizione seguente non è più presente nella ISO/IEC 27000, ma è importante.

Azione preventiva: azione per eliminare la causa di una potenziale non conformità o altre situazioni indesiderabili.

In altre parole, un'azione preventiva riguarda non conformità non ancora manifestate, ma potenziali. Per esempio, un decadimento delle prestazioni, seppure entro limiti accettabili, potrebbe richiedere un'azione preventiva per evitare che raggiunga livelli inaccettabili; oppure un caso avvenuto in altre organizzazioni potrebbe essere analizzato per evitare che si manifesti anche nella propria organizzazione.

La gestione delle azioni preventive è molto simile a quella delle azioni correttive (analisi, pianificazione, attuazione e verifica con il supporto di procedure e registrazioni) e pertanto non è discussa nel dettaglio.

Esempio 15.10.5. Un semplice esempio di azione preventiva è il seguente: per evitare un ritardo di un progetto, si sostituisce una persona con poca esperienza con una persona con maggiore esperienza.

È opportuno sottolineare la differenza tra azioni correttive e preventive: le prime sono finalizzate alla prevenzione del ripetersi di una non conformità, le seconde alla prevenzione del loro manifestarsi.

Spesso, in ambienti accademici e professionali, si accendono animate e profondissime discussioni in merito a queste differenze, soprattutto se applicate a casi reali, non sempre facilmente discernibili. Per questi motivi nell'HLS non si tratta di azioni preventive e si fa riferimento alle azioni volte ad affrontare i rischi relativi all'efficacia del sistema di gestione, di cui si è parlato nel paragrafo 15.6. Infatti, un'azione preventiva è un'azione necessaria ad affrontare il rischio che si manifesti una non conformità.

15.10.4 Miglioramento continuo

La norma si conclude con un breve paragrafo: “L’organizzazione deve migliorare continuamente l’idoneità, l’adeguatezza e l’efficacia del sistema di gestione per la sicurezza delle informazioni”.

Questa è una frase generica, e forse inutile, visto che il miglioramento del sistema di gestione è attuato con azioni conseguenti la valutazione del rischio relativo al sistema di gestione, oggetto del capitolo 6 dello standard (paragrafo 15.6 di questo libro).

Si ricorda quanto detto al paragrafo 15.6.2: le azioni di miglioramento non devono essere solo conseguenti a una valutazione del rischio completa di tutto l'ambito, ma possono essere originate da rischi identificati, analizzati e valutati puntualmente come, per esempio: modifiche alla normativa vigente, nuove richieste dei clienti, eventi e incidenti rilevati nell'organizzazione o in altre. Questo vuol dire che il contesto deve essere costantemente oggetto di osservazione, in modo da cogliere i segnali di rischi da valutare e trattare.

15.11 Appendice A della ISO/IEC 27001

L'Appendice A della ISO/IEC 27001 riporta i controlli di sicurezza a cui fare riferimento quando si realizza un sistema di gestione per la sicurezza delle informazioni.

Come precisato nel paragrafo 15.6.3, chi intende certificarsi rispetto alla norma ISO/IEC 27001 deve compilare una Dichiarazione di applicabilità, ossia un'analisi dei controlli attuati. Solitamente questa analisi si basa sui controlli dell'Appendice A. Nel caso in cui alcuni controlli dell'Appendice A non siano attuati, la Dichiarazione di applicabilità deve riportarne la giustificazione.

L'Appendice A comprende, similmente a quanto riportato nel capitolo 12:

controlli tecnologici informatici (per esempio, sull'uso dei programmi di utilità e sulla gestione delle chiavi crittografiche);

controlli tecnici non informatici (per esempio sui controlli di accesso fisico alle sedi);

controlli tecnici parzialmente informatici (per esempio sul trasferimento dei dispositivi di memorizzazione delle informazioni);

controlli organizzativi (per esempio sulla classificazione delle informazioni);

processi di sicurezza, tra cui la gestione degli asset, delle persone, delle utenze, delle autorizzazioni, dei fornitori, della capacità, dei cambiamenti, delle configurazioni, degli incidenti, della disponibilità, della continuità operativa.

Questa impostazione è tipica della ISO/IEC 27001 e deriva dalle sue origini (come detto nel paragrafo 13.5). Altre norme riportano i processi specifici del sistema in questione nel corpo principale della norma.

15.12 Bibliografia della ISO/IEC 27001

L'ultima parte della norma è dedicata alla bibliografia dove, oltre alla ISO/IEC 27002, è riportata la ISO 31000, dedicata alla gestione del rischio in generale: a essa sono allineati i concetti e le definizioni della ISO/IEC 27000 e della ISO/IEC 27001.

Altre linee guida da considerare sono la ISO/IEC 27003, per l'interpretazione della ISO/IEC 27001, la ISO/IEC 27004 sulle misurazioni e la ISO/IEC 27005 sulla valutazione del rischio relativo alla sicurezza delle informazioni.

Note

¹³⁷standards.iso.org/ittf/PubliclyAvailableStandards.

¹³⁸<https://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data>.

¹³⁹[https://cloudsecurityalliance.org/research/cloud-controls-matrix/.](https://cloudsecurityalliance.org/research/cloud-controls-matrix/)

Parte V

Appendici

Appendice A

Gestire gli auditor

*Amor, ch'a nullo amato amar perdona,
mi prese del costui piacer sì forte,
che, come vedi, ancor non m'abbandona.*

Dante Alighieri, Inferno Canto V

Questo libro non approfondisce come programmare, pianificare e condurre un audit, né come riportare le evidenze e le risultanze di audit. Per comprendere veramente come si gestiscono gli audit si consiglia di leggere libri dedicati a questo argomento [35], partecipare a corsi di formazione e, soprattutto, affiancare persone esperte durante gli audit.

Il rapporto con le persone da intervistare è spesso complesso perché vi è sempre un mix di timore e cautela da parte sia dell'auditor sia delle persone dell'organizzazione oggetto dell'audit. Raramente si tratta di un rapporto conflittuale, ma richiede comunque cautela.

Un auditor si trova spesso in imbarazzo a dover affrontare persone sconosciute, nei confronti delle quali deve erogare un servizio che richiede una certa durezza. Ciascun auditor impara con il tempo a gestire questi rapporti, anche in funzione del proprio carattere e delle proprie attitudini; alcuni si dimostrano molto distaccati, altri più amabili, altri molto rigorosi.

Quando un'organizzazione incontra un auditor, il timore, la curiosità, il rispetto professionale e i dubbi sulle sue competenze sono elementi tra loro conflittuali che rendono non sempre semplice il rapporto e, anzi, molto stancante, anche quando l'audit si svolge in modo sereno e senza che siano rilevate non conformità o punti di attenzione.

Questo è vero anche per l'auditor: tutto il giorno è seguito da persone attente a ogni suo movimento e a ogni sua domanda, ha sempre il dubbio di essere inadeguato e timoroso delle reazioni degli intervistati se venissero rilevate delle non conformità.

Il timore di inadeguatezza dell'auditor è determinato dalla consapevolezza di non essere pienamente competente su tutti i campi di indagine, mentre le persone intervistate sono invece molto competenti nel loro settore. Un auditor di sicurezza delle informazioni deve poter discutere di sicurezza fisica, sicurezza dei sistemi, sicurezza della rete, sicurezza delle applicazioni; non può conoscere in modo approfondito tutti questi temi, anche considerando le numerose tecnologie disponibili.

Spesso, soprattutto agli inizi di un audit, le persone intervistate possono avere dei dubbi sulle competenze dell'auditor perché fa domande o affermazioni non sempre pertinenti. Può anche far sorridere quando chiede spiegazioni su argomenti ritenuti banali da parte degli operatori. Si deve però tener conto che un auditor, se non è interno, ha rapporti con tante organizzazioni, ciascuna con il proprio gergo e le proprie tecnologie.

Questa appendice tratta di come gestire un auditor, tema quasi mai trattato da testi, convegni o altro. Si fa riferimento agli auditor esterni, ma alcune regole sono applicabili anche a quelli interni. Inoltre, quanto detto non è sempre applicabile quando l'auditor è un rappresentante di un'Autorità pubblica o delle Forze dell'ordine.

Per illustrare come gestire un auditor, si considerano le sue quattro nature: ospite, partner, fornitore e... auditor.

A.1 L'auditor è un ospite

Come per ogni ospite dell'organizzazione, è buona norma offrire all'auditor caffè e acqua e chiedere se ci sono problemi in merito al condizionamento o riscaldamento dell'eventuale stanza messa a sua disposizione.

L'auditor, quando opera presso l'organizzazione, non è nel proprio ufficio e quindi, se questo non presenta conflitti con le regole dell'organizzazione, è comune cortesia mettergli a disposizione una connessione a Internet (oltre alle regole da seguire, come per ogni altro ospite) e permettergli di fare qualche fotocopia, purché pertinente lo scopo della visita.

Per gli auditor devono essere osservate le misure di sicurezza applicabili agli ospiti e, per esempio, devono essere sempre accompagnati.

Se l'auditor è un esterno, in particolare di un organismo di certificazione, ed è da solo, è buona norma organizzare un pranzo. Se l'attività è lunga, si può ridurre questo impegno alla prima giornata; se l'attività è di uno o due giorni, è opportuno organizzare il pranzo tutti i giorni.

Si consiglia di chiedere a metà mattinata se vuole “accompagnarci per pranzo”, in modo che tutti possano organizzarsi convenientemente. Alcuni auditor rifiutano per evitare conflitti di interesse (anche se spesso sono in trasferta con

rimborso spese), altri accettano volentieri. Spesso un pranzo permette all’auditor di cogliere meglio il lato umano dell’organizzazione e la sua cultura.

L’organizzazione non deve pagare per forza il pasto, soprattutto se vi sono regole o codici etici da applicare. In ogni caso, è meglio chiarire subito con l’auditor la cosa. È anche opportuno chiedere all’auditor se ha problemi particolari, in modo da non andare in un posto “solo pesce” se non può mangiarlo.

Il pranzo non deve essere troppo lungo, perché si è lì per ragioni di lavoro, ma neanche un panino al bar in piedi. Un posto veloce, decoroso e vicino alla sede dove si sta svolgendo l’audit permette di non perdere tempo e di rendere piacevole il pasto.

Si evitino posti lontani o “da provare” proprio per il giorno dell’audit. Alcuni, in particolare se normalmente devono osservare una dieta, colgono l’occasione dell’audit per una mangiata pantagruelica: anche questo va evitato.

Ogni perdita di tempo la pagano tutti: l’audit deve essere completato e se il pranzo è lungo, l’audit si concluderà più tardi, senza soddisfazione per alcuno.

Se l’auditor è in trasferta, si dovrebbe aiutarlo a trovare un buon hotel e segnalargli il modo migliore per raggiungere la sede dell’audit. Può anche essere organizzata una cena con le stesse regole di cui sopra. Non è però obbligatorio. Certamente, se alcuni rappresentanti dell’organizzazione sono in trasferta e devono cenare al ristorante, allora è una buona idea coinvolgere anche l’auditor.

A.2 L’auditor è un partner

Una delle cose più pericolose è raccontare bugie a un auditor, soprattutto perché potrebbe accettare la verità e poi mettere in discussione qualunque altra successiva affermazione.

Quelle più comuni riguardano l'impossibilità tecnica di fare qualcosa (per esempio, sui sistemi Linux creare utenze personali con gli stessi privilegi di root), con il risultato che l'auditor potrebbe anche sentirsi offeso se invece conosce la tecnologia in questione.

È anche importante evitare scuse come “non abbiamo risorse”: l'auditor potrebbe riportare la lamentela alla Direzione, con potenziali ricadute negative su chi l'ha fatta perché ritenuto incapace di gestire i processi con le risorse messe a disposizione. Inoltre questa scusa è nota per essere la più diffusa; un auditor ha avuto modo di rispondere “è un vostro problema di organizzazione” e di scrivere una non conformità.

È meglio evitare contestazioni, inventando scuse improbabili, quando l'auditor ha ragione. In questi casi, l'atteggiamento corretto è: accettare il rilievo ed, eventualmente, cercare di dimostrare che si tratta di cosa non grave.

L'auditor è un partner e quindi è sempre possibile segnalargli aree su cui potrebbe contribuire maggiormente. È necessario tuttavia stare attenti e non segnalare aree di non conformità tali da compromettere il risultato dell'audit. Per esempio, gli si può chiedere di affrontare argomenti su cui la consapevolezza e attenzione delle persone coinvolte è ridotta.

È sempre una buona tecnica, se adottata con sincerità, chiedere chiarimenti su come interpretare alcuni requisiti oggetto dell'audit: l'auditor si sente coinvolto

per le sue competenze e può metterle a disposizione di qualcuno.

Altra buona tecnica è fargli vedere le novità rispetto all'ultimo audit o i progetti innovativi, purché gestiti in modo adeguato: spesso gli auditor vedono sempre le stesse cose, seppure differenti e in ambienti diversi; le novità fanno sempre piacere.

Una cortesia riguarda la documentazione: se è molta e in formato elettronico, è opportuno stamparne qualche esempio, oppure permettergli di consultarla con un PC dedicato. È sempre molto frustrante dover esaminare delle procedure (anche numerose o molto lunghe) senza poterlo fare in autonomia.

Per la pianificazione dell'audit è opportuno cercare di collaborare con l'auditor, soprattutto se l'organizzazione è grande e gruppi diversi si occupano di cose simili (per esempio, per la conduzione dei sistemi Windows e Unix) o le attività sono svolte in sedi diverse e lontane tra loro (molte grandi organizzazioni sono il frutto di acquisizioni e incorporazioni, con il risultato di avere molte sedi e gruppi di lavoro diversi). Si dovrebbe quindi indicare all'auditor le potenziali difficoltà relative al tempo da dedicare ad alcuni spostamenti o alla scorretta pianificazione delle attività.

Esempio A.2.1. Un auditor potrebbe pianificare due ore per la verifica della conduzione dell'infrastruttura informatica. Se questa è effettuata da più funzioni dell'organizzazione, bisognerebbe segnalaraglielo, in modo che possa modificare il piano in modo appropriato. In caso contrario, l'auditor potrebbe trovarsi in difficoltà a chiudere l'audit nei tempi previsti.

Alcuni ritengono che una pianificazione scorretta possa essere utile a perdere

tempo. In realtà si rischia di costringere l'auditor e le persone coinvolte nell'audit a fare tardi e non poter affrontare serenamente l'impegno.

Se l'auditor lo permette, è possibile collaborare alla scrittura del rapporto, in modo che i termini utilizzati e alcuni riferimenti siano facilmente comprensibili a tutte le parti interessate, inclusa la Direzione. Ovviamente, questo non implica l'opportunità di modificare il risultato finale dell'audit.

A.3 L'auditor è un fornitore

L'auditor, se esterno, è veramente un fornitore. Anche l'auditor interno può essere visto come fornitore interno. Per questo, è giusto pretendere la qualità del servizio.

Il primo parametro riguarda il rispetto dei tempi: bisogna chiedere di ricevere con congruo anticipo il regolamento dell'audit e il piano di audit, in modo da garantire la presenza delle persone da coinvolgere senza doverle bloccare oltre il necessario. Inoltre, se non ci sono contrattempi e il piano è stato concordato tra le parti in modo collaborativo e non sono emerse non conformità, se l'auditor prolunga gli incontri oltre l'orario stabilito, deve essere invitato a terminarli.

Durante l'audit, al termine di ogni incontro è opportuno chiedere di esplicitare se ha rilevato qualcosa, in modo che la illustri e fornisca i necessari chiarimenti. Bisogna chiedere chiarimenti fino a quando non si è capito il rilievo, ovviamente evitando di prendere in giro l'auditor e manifestare una falsa incapacità di comprensione per perdere tempo.

Non bisogna aver paura di contraddirsi un auditor. Per esempio, se vuole che

siano verificati i PC dei visitatori all'ingresso della sede e si ritiene inutile questa misura, bisogna spiegargli le proprie motivazioni (spesso collegate alla valutazione del rischio) e non accettare passivamente ogni sua richiesta.

Può essere necessario pretendere il rispetto dei tempi anche dopo la conclusione dell'audit, in particolare relativamente ai tempi di consegna del rapporto. Spesso, quando si riceve il rapporto dopo molto tempo la conclusione dell'audit, se è scritto in modo molto sintetico, è difficile interpretarlo correttamente e avviare le opportune azioni correttive a fronte delle non conformità rilevate.

Bisogna evitare di fare da segretario dell'auditor, per esempio prenotando treni o aerei come potrebbe fare autonomamente via web.

A.4 L'auditor è un auditor

La raccomandazione di essere sinceri deve essere bilanciata con la necessità di non dire proprio tutto.

Regola base: fare in modo che tutto il personale, compresa la Direzione, sia preparato all'audit, anche grazie a simulazioni svolte in precedenza.

Le simulazioni vanno fatte con largo anticipo rispetto all'audit, in modo da condividere i punti da evitare o da adeguare. Le persone che parteciperanno all'audit dovranno essere molto collaborative in questa fase. Alcuni, anche se non hanno mostrato interesse durante le fasi preparatorie, presi da entusiasmo, raccontano all'auditor cose mai segnalate in precedenza ai consulenti o agli auditor interni, con ovvi effetti negativi.

D'altra parte bisogna evitare di falsificare le attività: se durante l'anno non si è fatto nulla per essere conformi ai criteri di audit bisognerebbe chiedersi se non si sono fatti degli errori nella progettazione e pianificazione del proprio sistema di gestione. È pratica comune riesaminare e correggere in anticipo i documenti che l'auditor, presumibilmente, analizzerà, esattamente come si riassetta la casa prima di ricevere degli ospiti. Ma non è ammissibile trovarsi nella necessità di creare dal nulla procedure e registrazioni come dei villaggi Potëmkin o delle ombre cinesi azionate da Fantozzi.

Esempio A.4.1. Una forma interessante di falsificazione delle attività è l'attuazione di misure di sicurezza solo per l'auditor: controllo del computer all'ingresso, indisponibilità della wi-fi, eccetera. Spesso queste false misure sono evidenti perché l'auditor vede altri visitatori trattati in modo diverso e, a quel punto, è costretto a scrivere una non conformità.

Quando si affronta un audit è anche necessario comprendere le esigenze degli auditor: devono vedere esempi delle attività oggetto di audit e quindi bisogna evitare di raccontare processi e controlli di sicurezza solo a voce. È imbarazzante per l'auditor dover continuare a chiedere delle evidenze e continuare ad ascoltare solo parole (anche se il termine auditor deriva proprio dal latino “ascoltare”); in questi casi l'incontro potrebbe concludersi in ritardo o con delle non conformità.

Da evitare frasi come “Questo documento l'ho messo da qualche parte nella e-mail”: le registrazioni vanno tenute sotto controllo e opportunamente archiviate; il fatto che siano reperibili solo in una casella di posta rappresenta una non conformità.

L'auditor non conosce in modo approfondito le mansioni di ciascuno e potrebbe

cercare di affrontare un argomento con la persona sbagliata. In questo caso è bene imparare a rispondere “Vorrei non rispondere su questo argomento perché di competenza di altri” e indicare a chi rivolgersi. Alcuni cercano di rispondere come se fossero interrogati a scuola su un argomento che non hanno studiato, con prevedibili risultati negativi.

Se qualcuno è in difficoltà a capire o rispondere a una domanda, deve chiedere aiuto ai colleghi o collaboratori: l’audit è una valutazione dell’organizzazione ed è la “organizzazione” a dover rispondere, non una singola persona. Questa regola ha le sue eccezioni: è previsto che ciascuno sappia reperire e interpretare la politica per la sicurezza delle informazioni e le procedure applicabili alle sue mansioni (non è però previsto che siano recitate a memoria).

Molti accompagnatori tendono ad assumersi la responsabilità dei risultati dell’audit e a intervenire su tutti gli argomenti. Anche questo è un atteggiamento da evitare: se l’audit è stato preparato correttamente, è giusto che dimostrino fiducia nelle persone e le lascino rispondere. In alcuni casi, però, la persona intervistata potrebbe cedere al panico, anche se ingiustificato, e in questo caso l’accompagnatore dovrebbe intervenire per aiutare. Un’altra occasione di aiuto si presenta quando l’auditor e gli intervistati hanno difficoltà a comprendersi a vicenda perché utilizzano gerghi tra loro diversi.

Bisogna ricordare che l’auditor pone molte domande perché soprattutto intende capire i processi e non ha alcuna intenzione di affliggere i propri interlocutori.

Purtroppo, alcune organizzazioni assegnano al personale obiettivi sul numero di rilievi dell’audit. Questa è una pratica scorretta perché, oltre a rendere gli audit conflittuali, prevede di assegnare obiettivi al lavoro dell’auditor e quindi si potrebbe avere una non conformità perché gli obiettivi non sono appropriati.

Appendice B

I primi passi per realizzare un SGSI

La filosofia è scritta in questo grandissimo libro, che continuamente ci sta aperto innanzi agli occhi (io dico l'universo), ma non si può intendere se prima non s'impura a intender la lingua e conoscere i caratteri ne' quali è scritto.

Galileo Galilei, Il Saggiatore

In questa breve appendice si vogliono riportare i primi passi per realizzare un sistema di gestione per la sicurezza delle informazioni.

I punti qui proposti sono in ordine di importanza e di realizzazione e rappresentano una proposta personale dettata dall'esperienza. Ciascuno può seguire strade diverse a seconda della propria esperienza e delle proprie competenze.

In questo libro si è accennato solo marginalmente alla gestione dei progetti (project management), ma si tratta di una materia da studiare prima di avviare un progetto complesso come la realizzazione di un sistema di gestione per la sicurezza delle informazioni.

B.1 Individuare l'ambito

Il primo passo è sempre quello di individuare l'ambito dove realizzare il sistema di gestione per la sicurezza delle informazioni. In particolare devono essere individuati i servizi e le attività dell'organizzazione da includere.

Alcune volte si può avere il dubbio se includere o meno un servizio o un'attività. Se questi hanno impatti sulle informazioni già nell'ambito, è solitamente meglio includerli: è inutile perdere troppo tempo per ragionare sulle possibili e future difficoltà conseguenti all'inclusione. Se e quando queste si dovessero manifestare, sarà semplice escluderli, mentre potrà essere più difficile includerli in un secondo tempo se invece dovessero risultare necessari.

D'altra parte bisogna prestare attenzione a non voler affrontare un ambito troppo ampio, perché può portare a una dispersione di energie.

B.2 Coinvolgere i manager

Il secondo passo è ben noto a tutti e forse è banale ricordarlo: coinvolgere la Direzione e i responsabili delle funzioni comprese nell'ambito. Pochi però ricordano l'importanza di comunicare l'avvio del progetto a tutti i livelli gerarchici dell'organizzazione con le scadenze previste.

È anche bene fissare incontri periodici con la Direzione e i responsabili delle funzioni comprese nell'ambito. Questi incontri, solitamente brevi, sono utili per rispondere a eventuali dubbi e coordinare le iniziative. In tutti si deve aggiornare il piano di progetto e concordare le scadenze delle attività.

B.3 Gestire i documenti

La gestione dei documenti è sempre intesa come un passo formale, ma essi (politiche, regole, procedure, istruzioni, eccetera) riportano le regole che ciascuno deve seguire. Per questo è bene stabilire chi ha l'autorità di approvare e pubblicare queste regole e chi deve comunicare la disponibilità di nuovi documenti o di loro aggiornamenti alle persone coinvolte nel sistema di gestione per la sicurezza delle informazioni.

Deve anche essere stabilito il modello di documento da adottare e la sequenza dei capitoli per evitare difficoltà di interpretazione da parte dei destinatari dei documenti.

Quando si scrivono le procedure, è utile prevedere, per ciascuna di esse, uno schema finale con riportate le registrazioni richieste e le modalità di archiviazione delle stesse.

B.4 Miglioramento

Una delle prime procedure da condividere riguarda quella per il miglioramento continuo, in modo da stabilire:

chi ha l'autorità per decidere quali progetti di miglioramento avviare; come mantenere il registro del miglioramento (paragrafo 15.6.4.2) in modo che tutte le parti interessate ai progetti siano informate del loro avanzamento.

Il registro deve essere presentato nel corso di incontri periodici a evitare

sovraposizioni e conflitti tra i vari progetti.

B.5 Formare il personale

Dopo aver coinvolto i manager è fondamentale formare tutto il personale affinché contribuisca attivamente alla realizzazione del sistema di gestione con le proprie idee e le proprie esperienze, convogliate in uno schema condiviso.

Un primo passo consiste in una veloce presentazione del progetto e qualche elemento teorico di sicurezza delle informazioni. Quasi al termine della realizzazione del sistema di gestione per la sicurezza delle informazioni è necessario prevedere incontri per presentare le procedure e gli strumenti da utilizzare per attuare i controlli di sicurezza.

B.6 Gap analysis

Successivamente alla prima sessione di formazione si può procedere a un'analisi dell'Appendice A della ISO/IEC 27001 per verificare cosa è attuato dall'organizzazione e come. I dati raccolti saranno sicuramente utili per l'analisi del rischio relativo alla sicurezza delle informazioni in quanto possono evidenziare delle vulnerabilità e in seguito saranno consolidati nella Dichiarazione di applicabilità.

Per ciascun controllo di sicurezza occorre individuare dove è applicabile. Per esempio, la politica per la sicurezza delle informazioni è applicabile a tutta l'organizzazione, mentre il controllo degli accessi è applicabile in diversi punti: varchi fisici, rete informatica, applicazioni software, sistemi operativi (a loro

volta diversi), eccetera.

Quando si analizzano i controlli di sicurezza, è sempre opportuno, se applicabile, analizzarne le 4 dimensioni fondamentali (le 4 P):

processi: se il controllo non è un processo, bisogna analizzare il processo con cui è gestito il controllo e se sono previste registrazioni per dimostrare il suo corretto funzionamento (per esempio, nel caso dei backup, bisogna verificare se i processi di programmazione, verifica e test dei backup sono efficaci e se sono conservate delle registrazioni sulla loro pianificazione ed esecuzione);

partner: verificare se il controllo di sicurezza ha impatti su clienti, fornitori e partner e, se il caso, sono attivi accordi o contratti e canali di comunicazione con loro;

prodotti: verificare se la tecnologia adottata per attuare il controllo di sicurezza è adatta;

persone: accertarsi che le persone addette al controllo di sicurezza siano adeguatamente formate, addestrate e consapevoli.

Durante la gap analysis si possono evidenziare modifiche da apportare ai controlli di sicurezza già esistenti o nuove misure da attuare perché, intuitivamente, sono già collegate a rischi molto elevati (molto spesso, già durante la gap analysis, si abbozzano i documenti di descrizione dei processi, si preparano i programmi di manutenzione e di backup, si raccolgono i contratti, eccetera). Queste esigenze potranno avviare dei progetti di miglioramento anche prima della conclusione della valutazione del rischio.

B.7 Realizzare il sistema di gestione

I passi successivi prevedono solitamente di valutare il rischio, predisporre un piano di trattamento del rischio, pianificare le azioni di riduzione del rischio (ricordando di considerare, per ogni controllo di sicurezza, le 4 P), attuare quanto pianificato.

Si ricorda di evitare di realizzare un sistema di gestione come un villaggio Potëmkin, ossia solo con la finalità di mostrare agli auditor dei documenti preparati pochi giorni prima. Questo approccio è inutile e costoso per l'organizzazione e delegittia quanto fatto.

Le ultime attività necessarie alla realizzazione di un sistema di gestione per la sicurezza delle informazioni, oltre all'erogazione della seconda parte della formazione, sono da effettuare qualche tempo dopo la realizzazione dei controlli e dei processi e sono: la conduzione dei primi audit interni e del primo riesame di Direzione straordinario per confermare la buona conclusione del progetto.

Appendice C

La certificazione di un sistema di gestione

Dipinte in queste rive

Son dell'umana gente

“Le magnifice sorti e progressive”

Giacomo Leopardi, La ginestra

L'applicazione degli standard relativi alla sicurezza delle informazioni non è sempre semplice e quindi è spesso parziale. Talvolta ci possono essere errori interpretativi, talvolta non ci si rende conto dei rischi di un'incompleta applicazione. Pertanto i più avveduti richiedono a enti indipendenti una certificazione del completo rispetto dello standard.

In questa appendice si tratta della certificazione dei sistemi di gestione, mentre in appendice D si tratta di quella dei prodotti per la sicurezza delle informazioni.

Si presentano gli attori dello schema di certificazione dei sistemi di gestione e i passi per ottenere un certificato.

C.1 Gli attori

Il termine organizzazione indica l'entità che intende certificarsi o è certificata. La certificazione di un sistema di gestione avviene secondo uno standard di requisiti (ISO 9001, ISO/IEC 14001, eccetera); la ISO/IEC 27001 è lo standard di requisiti per i sistemi di gestione per la sicurezza delle informazioni.

Il certificato è rilasciato da un Organismo di certificazione (OdC) o Certification body (CB). Un organismo di certificazione può essere accreditato da un Ente di accreditamento.

Gli enti di accreditamento sono regolamentati in Europa dal Regolamento della Commissione Europea 765 del 2008 e sono uno per Stato. I diversi enti di accreditamento si riconoscono reciprocamente attraverso dei Multilateral agreement (MLA) o dei Bilateral agreement (BLA) a livello europeo dall'EA¹⁴⁰ o mondiale dall'IAF¹⁴¹. Per esempio, un certificato ISO/IEC 27001 rilasciato da un OdC accreditato in Italia dall'ente ACCREDIA è equivalente ad certificato ISO/IEC 27001 rilasciato da un OdC accreditato in UK dall'ente UKAS, perché ambedue aderenti a degli MLA.

Un Organismo di certificazione può essere accreditato per certificare solo secondo standard e settori specifici. Per certificare secondo la ISO/IEC 27001, un OdC deve essere accreditato secondo i requisiti della ISO/IEC 27006-1.

In questo modo l'OdC aderisce a uno schema e a dei regolamenti che ne garantiscono professionalità, competenza e indipendenza e il riconoscimento dei propri certificati a livello internazionale.

Esistono organismi di certificazione non accreditati e sono numerosi quelli accreditati per alcune norme, per esempio la ISO 9001, che effettuano attività di certificazione su altre norme, per esempio la ISO/IEC 27001, per le quali però non sono accreditati. È sconsigliato rivolgersi a loro. Le organizzazioni che

intendono certificarsi ISO/IEC 27001, dovrebbero quindi rivolgersi a un Organismo di certificazione accreditato e riconosciuto dall'IAF o dall'EA per la certificazione ISO/IEC 27001.

C.2 Il percorso di certificazione

Il percorso di certificazione è esemplificato dalla seguente figura.

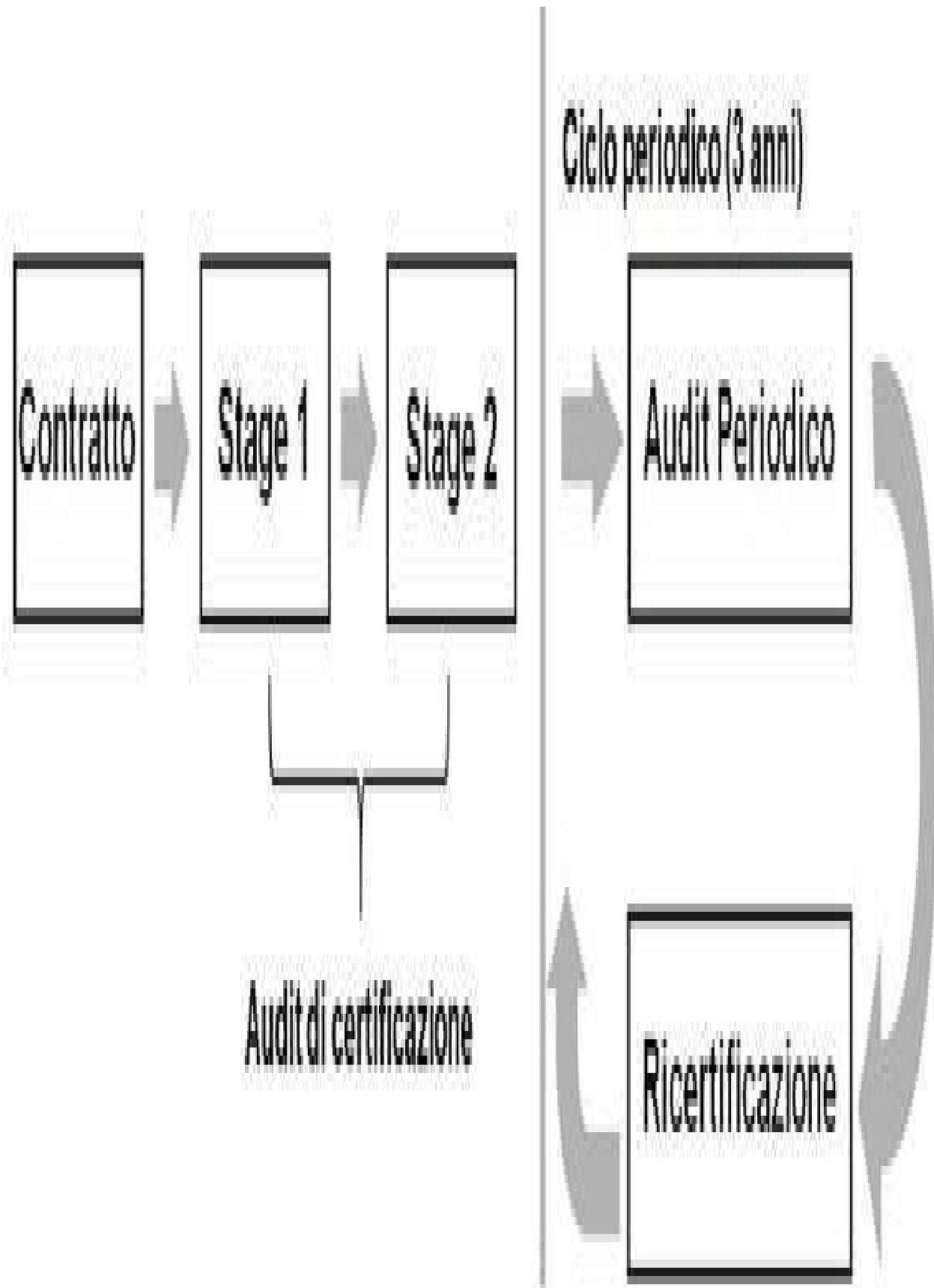


Figura C.2.1:

Il processo di audit

C.2.1 Il contratto

Il processo di audit inizia con un contratto tra l'Organismo di certificazione e l'organizzazione che intende certificarsi. Il contratto, tra le altre clausole, deve riportare il numero di giornate complessive richieste da ciascuna fase di audit.

Per le certificazioni ISO/IEC 27001 il numero di giornate è tratto da tabelle presenti nella ISO/IEC 27006-1 e dipende da alcuni fattori di complessità dell'organizzazione e dal numero di persone e siti compresi nell'ambito del sistema di gestione. Purtroppo alcuni Organismi di certificazione non rispettano le regole stabilite ed effettuano audit in tempi molto inferiori da quelli previsti.

C.2.2 L'audit di certificazione

Dopo aver stipulato il contratto si organizza il primo audit di certificazione. Esso si compone sempre di due fasi, dette stage, a cui si può aggiungere un audit straordinario. Al termine dell'audit di certificazione, se ha esito positivo, l'OdC emette il certificato.

Stage 1

Nello stage 1, l'auditor valuta il livello di preparazione del sistema di gestione per la sicurezza delle informazioni tale da portare, presumibilmente, a concludere lo stage 2 in modo positivo.

L'auditor analizza la documentazione, effettua un primo sopralluogo e, con la conoscenza acquisita, predisponde un piano per lo stage 2.

Se la valutazione dovesse essere negativa, si potrebbe rendere necessaria la ripetizione dello stage.

Stage 2

Durante lo stage 2, condotto secondo le stesse modalità descritte nel paragrafo 15.9.2, sono analizzate tutte le aree fisiche, tecniche e organizzative comprese nel sistema di gestione per la sicurezza delle informazioni al fine di determinare se l'organizzazione è conforme alla ISO/IEC 27001. Nel caso di molti siti si procede a un loro campionamento, secondo quanto stabilito dai regolamenti internazionali applicabili.

Se dovessero essere rilevate non conformità gravi, occorre effettuare un audit straordinario; in caso contrario, si può procedere alla raccomandazione ed emissione del certificato.

C.2.3 Raccomandazione ed emissione del certificato

L'auditor non ha il potere di decidere sull'emissione del certificato, ma può solo raccomandarla all'Organismo di certificazione. L'OdC, dopo aver analizzato e valutato positivamente il rapporto di audit, può procedere all'emissione del certificato; in caso contrario può chiedere chiarimenti all'auditor o anche programmare una visita straordinaria presso l'organizzazione (caso rarissimo).

C.2.4 Audit straordinario

In caso di non conformità grave deve essere effettuato un audit straordinario entro poche settimane dalla conclusione dello stage 2 o dell'audit periodico. L'audit straordinario ha l'obiettivo di verificare la chiusura delle non conformità rilevate. Se la valutazione è positiva, allora si può procedere alla raccomandazione ed emissione del certificato o alla sua conferma.

C.2.5 Audit periodici

Almeno ogni anno, e secondo quanto stabilito dal contratto e dal programma di audit, l'Organismo di certificazione deve effettuare un audit periodico al fine di verificare la continua conformità dell'organizzazione ai requisiti della norma e confermare la validità del certificato.

Gli audit periodici hanno durata inferiore (circa un terzo) rispetto a quella della somma delle giornate previste per lo stage 1 e lo stage 2. Per questo motivo negli audit periodici si verificano solo alcuni processi o controlli di sicurezza o attività. Al termine, se l'audit si conclude positivamente, l'auditor raccomanda il mantenimento del certificato.

In caso di non conformità gravi, si devono effettuare audit straordinari.

C.2.6 Audit di ricertificazione

Il certificato ha solitamente durata triennale e, quindi, ogni tre anni deve essere rinnovato l'accordo ed effettuato un audit di ri-certificazione, di durata non inferiore ai due terzi della somma delle giornate previste per lo stage 1 e lo stage 2.

Nell'audit di ri-certificazione devono essere verificate tutte le aree dell'ambito del sistema di gestione per la sicurezza delle informazioni, come si è fatto nel corso dello stage 2.

C.3 I bandi di gara

Quasi tutti i bandi di gara sono scritti male e riportano molti errori quando si tratta di certificazione di un sistema di gestione. Vi sono bandi che richiedono certificazioni rispetto alla ISO/IEC 17799 (norma obsoleta e per cui non è mai stato possibile certificarsi), alle ISO/IEC 27002, ISO/IEC 27003 e ISO/IEC 27018 (linee guida per le quali non è possibile certificarsi), alla ISO/IEC 27001:2007 (norma inesistente), eccetera.

I bandi, sovente, non richiedono alcunché in merito all'organismo di certificazione e al riconoscimento da IAF o EA.

Ancora più interessanti sono i bandi che richiedono una certificazione rispetto alla ISO/IEC 27001 senza specificare per quale ambito. In questo modo, per esempio, può partecipare a una gara per la conduzione operativa di una rete

informatica un'organizzazione certificata solo per l'immagazzinamento e conservazione di documenti cartacei; oppure può partecipare a una gara per la progettazione e sviluppo di servizi informatici un'organizzazione certificata solo per la conduzione sistemistica.

Dall'altra parte i bandi non dovrebbero pretendere una frase esatta da avere sul certificato, in modo da evitare alle organizzazioni partecipanti di chiedere continuamente aggiornamenti al proprio certificato per soddisfare tutte le richieste di tutti i propri potenziali clienti.

Un bando dovrebbe chiedere la certificazione ISO/IEC 27001:

sulla sua versione in vigore secondo i regolamenti EA o IAF;
che copra completamente l'ambito oggetto della gara;
che includa i siti da cui saranno erogati i servizi oggetto della gara (o che verrà estesa quanto prima a quei siti);
che sia rilasciata da un Organismo di Certificazione accreditato da un ente membro degli EA MLA o IAF MLA.

Per maggiori informazioni, l'ente di accreditamento italiano ha pubblicato una guida per le richieste di offerta e i bandi di gara [26], ma non sempre è seguita correttamente.

C.4 Standard e certificazioni per settori specifici

L'ISO pubblica, tra gli altri, documenti di linee guida come l'ISO/IEC 27011 (per le telecomunicazioni) e l'ISO/IEC 27018 (per i fornitori di servizi cloud). Questi standard sono chiamati, in inglese, sector-specific standard. Essi forniscono liste di controlli che possono essere aggiunti a quelli della ISO/IEC 27001. È impossibile richiedere la certificazione rispetto a questi standard (anche se alcuni OdC, scorrettamente, la offrono).

Come detto in 15.6.3, la Dichiarazione di applicabilità può basarsi su una lista di controlli diversa da quella dell'Appendice A della ISO/IEC 27001, purché sia altrettanto completa. È anche possibile usare l'Appendice A della ISO/IEC 27001 e aggiungerci ulteriori controlli.

In questo modo, l'organizzazione che vuole dimostrare l'uso di un sector-specific standard può aggiungere i controlli di questo standard alla propria Dichiarazione di applicabilità e chiedere a un OdC (se l'audit ha risultato positivo) un certificato che identifichi tale standard. Per esempio, un fornitore di servizi cloud che adotta la ISO/IEC 27018 non può ottenere un certificato ISO/IEC 27018, ma un certificato ISO/IEC 27001 che, oltre all'ambito, riporti una frase simile alle seguenti: “La dichiarazione di applicabilità include i controlli delle norme ISO/IEC 27001 e ISO/IEC 27018”.

Ulteriore questione riguarda la ISO/IEC 27701, ossia la norma relativa ai sistemi di gestione per la privacy (PIMS o privacy management system). Essa deve essere applicata a un ambito certificato ISO/IEC 27001, poiché questa norma ne è un'estensione (può anche essere un ambito più piccolo di quello certificato ISO/IEC 27001). Nel caso di questa norma, è prevista l'emissione di certificato a sé stante, seppur collegato a un certificato ISO/IEC 27001. I requisiti per gli organismi di certificazione ISO/IEC 27701 sono riportati nella ISO/IEC 27006-2.

C.5 Accreditamento

I meccanismi di accreditamento degli organismi di certificazione e dei laboratori garantiscono che l'intero processo di certificazione sia controllato da enti indipendenti e che sia assicurata la medesima validità ai certificati rilasciati. Il meccanismo di accreditamento non è però uguale per tutti i tipi di certificazione¹⁴².

C.5.1 Accreditamento per la certificazione dei sistemi di gestione

Le norme come la ISO 9001 e la ISO/IEC 27001 stabiliscono requisiti di sistemi di gestione e il loro rispetto è certificabile da organismi di certificazione.

Gli organismi di certificazione (OdC o, in inglese, conformity assessment body o CAB), a loro volta, devono fornire assicurazioni sulla qualità del processo di certificazione applicando la norma ISO/IEC 17021-1 che riporta i requisiti per soddisfare i principi di imparzialità, competenza, responsabilità, trasparenza e riservatezza.

La ISO/IEC 17021-1 stabilisce anche alcune caratteristiche dei processi di certificazione; per esempio, richiede riesami interni per tutti gli audit di certificazione e ri-certificazione, la suddivisione in due stage degli audit di certificazione e specifica le caratteristiche degli audit di mantenimento e ri-certificazione.

In generale, l'insieme delle regole che deve seguire un OdC per certificare un'organizzazione rispetto a una norma è detto schema di certificazione. Questo prevede anche, per semplificare molto, che un OdC, per essere accreditato rispetto alla ISO/IEC 17021-1, debba sottoporsi a un audit da parte dell'organismo di accreditamento che verifica i processi di certificazione (inclusi

quelli di vendita e anche affiancando gli auditor durante gli audit), i processi di monitoraggio, le competenze degli auditor, le modalità con cui è assicurata l'indipendenza e la trasparenza). In caso di esito positivo, l'OdC si dice accreditato.

Le norme di accreditamento sono, quindi, applicabili da organismi di certificazione e il loro rispetto è verificato da organismi di accreditamento. In questo modo, un certificato emesso da un OdC accreditato deve essere considerato come equivalente a un certificato emesso da un altro OdC accreditato dallo stesso organismo di accreditamento.

Per alcuni schemi, l'OdC deve rispettare altre norme rispetto alla ISO/IEC 17021-1. Per esempio, per la ISO/IEC 27001, l'OdC deve rispettare i requisiti della ISO/IEC 27006-1 (che, in realtà, è la ISO/IEC 17021-1 con l'aggiunta di requisiti specifici) e per la ISO/IEC 27701 quelli della ISO/IEC 27006-2.

Alcuni organismi di accreditamento hanno stretto degli accordi in modo da assicurare l'equivalenza dei certificati emessi sotto il loro accreditamento.

In Europa, il Regolamento europeo 765/2008 ha stabilito che ciascun Stato membro debba designare un unico organismo di accreditamento. In Italia, questo organismo è Accredia che, a sua volta, aderisce ad accordi multilaterali (MLA) e bilaterali (BLA), in particolare quelli promossi dalle associazioni EA (a livello europeo) e IAF (a livello internazionale) di cui è membro.

Questo vuol dire che un certificato ISO 9001 emesso da un OdC accreditato da Accredia va considerato come equivalente a un certificato ISO 9001 emesso da un OdC accreditato da COFRAC (Francia) o DPA (Albania).

Qualche ulteriore appunto è necessario.

Il primo appunto riguarda le norme aggiuntive. Accredia è molto prolifica sotto questo punto di vista, a differenza degli altri organismi. Per alcuni questo è segno di attenzione, per altri è un ulteriore esempio di ansia normativa di antica origine per il nostro Paese (si ricordano qui le “grida manzoniane”).

Il secondo appunto è che non tutti gli schemi di certificazione e accreditamento sono regolamentati da norme ISO o ISO/IEC e dagli organismi regolamentati dal Regolamento 765 o da accordi promossi da EA o IAF. Gli esempi virtuosi più noti sono quelli relativi alle norme OHSAS 18001 (pubblicata al di fuori dei comitati ISO; dal 2018 però sostituita dalla ISO 45001) e SA 8000 sulla responsabilità sociale (sviluppata dal SAI, al di fuori dei comitati ISO, e accreditata dall’organismo SAAS, dedicato a questo tipo di accreditamento e non aderente agli accordi di cui sopra).

Sono molti e numerosi gli esempi non virtuosi, visto che nulla vieta l’uso dei termini “certificazione” e “accreditamento” al di fuori dei canali ufficiali. Sono addirittura presenti organismi di certificazione e organismi di accreditamento al di fuori degli accordi EA o IAF che operano nel mercato delle certificazioni ISO 9001, ISO/IEC 27001, eccetera.

Il terzo appunto riguarda i certificati non accreditati. Alcuni organismi di certificazione emettono certificati al di fuori delle regole di accreditamento. Esempi virtuosi nascono dalla necessità di avviare uno schema di certificazione in assenza di regole di accreditamento. Per esempio, a cavallo del 2000, in Italia furono emessi certificati BS 7799 (la norma che divenne la ISO/IEC 27001) da alcuni OdC senza che fossero ancora disponibili le regole di accreditamento; appena si resero disponibili, questi OdC fecero domanda di accreditamento all’organismo pertinente e convertirono i certificati.

Al contrario, esempi negativi sono relativi a OdC accreditati per alcuni schemi che emettono certificati su altri schemi per cui non sono stati accreditati e senza avvisare chiaramente i clienti.

C.5.2 Certificazione e accreditamento dei laboratori

Il Regolamento europeo 765/2008 tratta anche dei laboratori. I requisiti da soddisfare per essere accreditati sono molto simili a quelli della ISO 9001. Molti laboratori, anzi, richiedono l'accreditamento all'organismo di accreditamento e la certificazione ISO 9001 accreditata a un OdC.

In questo caso, quindi, è improprio parlare di “certificazione dei laboratori” perché si tratta anche e soprattutto di “accreditamento dei laboratori”.

Le norme di riferimento sono:

ISO/IEC 17025 per i laboratori di prova e i laboratori di taratura;

ISO 15189 e ISO 22870 per i laboratori medici;

ISO/IEC 17043 per le organizzatori di prove valutative interlaboratorio;

ISO/IEC 17025 e ISO 15195 per i laboratori di misura di riferimento nell'area della medicina di laboratorio.

Non si vuole qui approfondire questo tipo di accreditamento, ma è opportuno osservare che è applicabile anche ai laboratori che erogano servizi di vulnerability assessment dei sistemi informatici, secondo uno schema promosso da Accredia.

Per quanto riguarda i rapporti internazionali, a livello europeo si fa riferimento a EA, come per gli accreditamenti relativi ai sistemi di gestione; a livello internazionale non si fa riferimento a IAF, ma a ILAC.

C.5.3 Certificazione dei prodotti, servizi e processi

La certificazione dei prodotti, servizi e processi segue un percorso simile a quello per i sistemi di gestione. In particolare, la catena di verifica tra organizzazioni, OdC, organismi di accreditamento e accordi internazionali rimane la stessa.

Diversa è la norma con cui l'organismo di accreditamento verifica gli OdC. Infatti, la norma di riferimento è la ISO/IEC 17065. Essa è molto simile alla ISO/IEC 17021-1, ma richiede la presenza di protocolli di verifica da parte dell'OdC molto più precisi. Questo implica, per esempio, l'uso di liste di riscontro molto precise ed esaustive.

Tra i prodotti più noti e per cui è richiesta una certificazione vi sono i dispositivi medici, secondo quanto previsto dal Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, che promuove l'utilizzo della norma ISO 13485. Queste norme richiedono di effettuare un'analisi del rischio del prodotto, basata su studi e casi clinici, e di stabilire i meccanismi di sicurezza per ridurre al minimo il rischio.

Meccanismi simili si usano per le macchine, i prodotti elettrici ed elettronici, gli ascensori, le caldaie, eccetera. Il risultato positivo della verifica porta all'apposizione della marcatura CE sul prodotto. Per ciascuno di essi sono seguite norme diverse, in alcuni casi pubblicate dall'ISO o ISO/IEC, in altri da

enti di normazione riconosciuti a livello internazionale come ANSI, CENELEC (EN) o UNI e CESI.

Le norme che forniscono presunzione di conformità ai requisiti europei di sicurezza prodotto sono dette norme armonizzate e riportano la sigla EN.

Altri casi riguardano i software utilizzati in ambiente aeronautico (con la DO-178B, utilizzata dalla Federal Aviation Administration o FAA, documento guida per determinare se il software in ambiente aeronautico funziona in modo affidabile e in parte simile ai Common Criteria) e farmaceutico.

L'enorme numero di tipi di prodotti ha portato alla proliferazione di questi schemi. In Italia, sono accreditati organismi per la certificazione, per esempio, della sicurezza degli alimenti e degli imballaggi recuperabili.

Lo stesso meccanismo vale per processi e servizi e infatti la ISO/IEC 17065 ha titolo “Requirements for bodies certifying products, processes and services”. Alcuni processi o servizi oggetto di certificazione accreditata da parte di Accredia sono i procedimenti di saldatura, i servizi di contact centre (norme ISO 18295) e i servizi di erogazione di corsi professionali e di svolgimento delle relative prove di esame per alcune materie.

Di particolare interesse per chi si occupa di informatica sono le certificazioni dei servizi informatici fiduciari, ossia quelli oggetto del Regolamento europeo eIDAS (paragrafo 12.15.1.6), per esempio firma digitale e marcatura temporale, e quelli regolamentati dalle autorità nazionali come, in Italia, lo SPID.

In questo caso, i risultati della certificazione (da parte di OdC accreditati) sono

valutati anche da AgID per includere i fornitori di servizi informatici fiduciari negli appositi registri pubblicati sul sito di AgID.

C.5.4 Certificazione della sicurezza informatica, Common Criteria e Cybersecurity Act

Per la sicurezza dei prodotti informatici, lo schema di certificazione attualmente utilizzato è quello per cui un prodotto è valutato sulla base delle norme della serie ISO/IEC 15408 (i cosiddetti Common criteria). Questi potrebbero anche essere usati per la certificazione dei sistemi informatici, ma al momento non è diffusa.

Lo schema di certificazione per i Common Criteria è un po' diverso da quello sopra descritto.

Gli OdC non effettuano direttamente le prove, ma si avvalgono di laboratori (Licensed laboratories, che non devono essere necessariamente accreditati come sopra descritto), che sottopongono i risultati all'OdC che può provvedere all'emissione del certificato.

Per quanto riguarda i rapporti internazionali, gli Stati aderenti sottoscrivono i Common Criteria Recognition Arrangement (CCRA), che assicurano il mutuo riconoscimento dei certificati. I CCRA prevedono la presenza di un unico OdC per Stato aderente e in Italia questo è l'OCSI.

Con il Regolamento europeo 2019/881 (ossia il Cybersecurity Act) in Europa è stata introdotta la certificazione dei prodotti informatici in modo da estendere gli schemi e da allineare, per quanto possibile, il meccanismo di certificazione della

sicurezza dei prodotti e servizi informatici a quello degli altri prodotti e servizi.

È ancora in corso la discussione su quali requisiti potranno essere usati per valutare i prodotti e i servizi. In questo caso si prevede che saranno approvate più norme tra loro alternative o specifiche per determinate tipologie di prodotti o servizi (sono già in circolazione riflessioni sull'adozione dei Common criteria, della IEC 62443 per gli impianti industriali e i loro componenti, di nuovi schemi per il cloud).

In questo caso, i certificati saranno emessi dalla “autorità nazionale di certificazione della cyber sicurezza” (unica per ciascun Paese; in Italia è l’Agenzia per la cybersicurezza nazionale, istituita nel 2021 con il DL 82), sulla base delle analisi di uno degli “Organismi di valutazione della conformità”, che dovranno essere accreditati dall’organismo di accreditamento nazionale (in Italia, si ricorda, è Accredia) e approvati dalla stessa autorità nazionale di certificazione della cyber sicurezza. Interessante osservare che l’Autorità potrà essere accreditata essa stessa come organismo di valutazione.

Poiché i requisiti di certificazione non sono stati ancora stabiliti, gli schemi di accreditamento non sono stati ancora avviati.

C.5.5 Certificazione e perimetro di sicurezza nazionale

Sulla certificazione della sicurezza informatica è intervenuta anche la normativa sul “perimetro di sicurezza nazionale cibernetica” (DL 105 del 2019 convertito dalla Legge 133 del 2019).

In tale contesto opera il Centro di valutazione e certificazione nazionale

(CVCN), parte dell’Agenzia per la cybersicurezza nazionale, che valuterà, in termini di sicurezza e secondo criteri dettati anche da valutazioni del rischio, le forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti delle pubbliche amministrazioni e altri enti.

Il CVCN potrà accreditare, secondo criteri stabiliti da un DPCM, laboratori di cui avvalersi per condurre verifiche e test. Questo schema di accreditamento, non ancora completato al momento di scrivere questo libro, pertanto, sarà probabilmente distinto da quelli già descritti.

C.5.6 Certificazione di processo e il GDPR

Il GDPR promuove l’istituzione di meccanismi di certificazione della protezione dei dati personali. Questi meccanismi, per quanto stabilito dal GDPR, devono essere accreditati secondo la ISO/IEC 17065 e pertanto i processi di trattamento dei dati personali dovranno essere verificati con protocolli più precisi di quelli che sarebbero usati per la valutazione di un sistema di gestione.

Al momento, risulta approvato da Accredia un solo schema di certificazione della protezione dei dati personali con accreditamento ISO/IEC 17065. I requisiti di accreditamento sono stati sviluppati senza il supporto del Garante per la protezione dei dati personali, cosa richiesta dal GDPR.

La norma ISO/IEC 27701 è relativa ai sistemi di gestione e, quindi, non in linea con quanto richiesto dal GDPR. L’attuazione della norma ISO/IEC 27701 può essere certificata solo con accreditamento basato sulla norma ISO/IEC 27006-2, a sua volta basata sulla ISO/IEC 17021-1, e non sulla ISO/IEC 17065 come richiesto dal GDPR). Al momento di scrivere questo articolo è in fase di elaborazione da parte del CEN uno standard di “requisiti di prodotto” per la privacy.

Il GDPR prevede anche la possibilità di adottare “codici di condotta” e di essere sottoposti al monitoraggio da parte di “organismo di monitoraggio”, che deve essere accreditato da un Garante privacy europeo.

C.6 I falsi miti della certificazione

Sono falsi miti della certificazione:

un’organizzazione certificata ISO/IEC 27001 è sicura;

un fornitore è certificato ISO/IEC 27001, quindi è sicuro anche secondo gli standard dei propri clienti, anche se non glieli hanno mai comunicati;

nella ricerca di un fornitore certificato ISO/IEC 27001 non è necessario comunicare i requisiti di sicurezza da soddisfare; non è necessario neppure verificare l’ambito del certificato e i siti inclusi nel certificato;

un prodotto certificato ISO/IEC 15408 o fornito da un’organizzazione certificata ISO/IEC 27001 è sicuro;

un prodotto certificato ISO/IEC 15408 è sicuro anche se utilizzato in modo non esattamente conforme alla configurazione utilizzata nel corso della certificazione, non nelle medesime ipotesi di utilizzo o per contrastare un potenziale di attacco superiore a quello previsto;

il cliente, fornitore o partner è certificato ISO/IEC 27001, pertanto tutte le sue richieste e affermazioni relative alla sicurezza delle informazioni sono corrette e pertinenti.

Esempio C.6.1. È ben noto il caso della Heartland, società di servizi di pagamento: nel 2009, ha subito un attacco informatico con compromissione dei dati delle carte di credito gestite.

La Heartland era certificata secondo le specifiche PCI (norme di sicurezza promosse dagli emettitori di carte di credito)¹⁴³.

Questa vicenda deve ricordare che “essere certificati” non vuol dire “essere sicuri”, ma che “si è fatto il possibile”.

Note

¹⁴⁰www.european-accreditation.org.

¹⁴¹www.iaf.nu.

¹⁴²Quanto segue è già apparso all’URL
<https://www.cybersecurity360.it/legal/accreditamento-e-certificazioni-regole-metodologie-e-norme-di-riferimento/> e grazie ai consigli di Franco Vincenzo Ferrari, Stefano Ramacciotti e Alice Ravizza.

¹⁴³<http://www.computerworld.com/article/2531653/technology-law-regulation/visa-drops-heartland-rbs-worldpay-from-pci-compliance-list-after-breaches.html>.

Appendice D

Common Criteria (ISO/IEC 15408) e FIPS 140-3

di Stefano Ramacciotti

Ogni scarrafone è bell'a mamma soja!

Pino Daniele, 'O scarrafone

D.1 Common Criteria (ISO/IEC 15408)

D.1.1 Generalità

La valutazione dell'affidabilità di un prodotto informatico, hardware o software o firmware, è uno dei problemi più difficili da risolvere in tutto il campo dell'informatica.

Nel tempo sono stati proposti numerosi criteri di valutazione. I primi criteri noti sono quelli USA denominati "Orange Book" (TCSEC) del 1985. A seguito di quelli sono nati nel 1989: il CTCPSC canadese, il CETIT tedesco, l'UKITSEC inglese e il CCDDCSI francese.

Le procedure di valutazione e certificazione erano complesse e richiedevano tempi lunghi che facevano lievitare i costi e dovevano essere ripetute in ogni Paese dove si voleva impiegare un certo prodotto. Al fine di evitare questi problemi per primi si mossero tedeschi, inglesi, francesi e olandesi creando un sistema comune già agli inizi degli anni Novanta: l'ITSEC, affiancato da un manuale (ITSEM).

Vista la promettente iniziativa si decise un nuovo approccio ancora più ambizioso allargando il gruppo a statunitensi e canadesi. Ciò portò nel 1996 al rilascio della prima versione dei Common Criteria for IT security evaluation¹⁴⁴, spesso abbreviati in Common Criteria o CC [29].

Questo si dimostrò fin da subito il sistema più completo e che, come adesso, fornisce risultati più affidabili tanto che, giunti alla loro maturità operativa con la versione 2.1 del 1999, vennero recepiti come standard internazionale ISO/IEC 15408.

Dagli iniziali sei Paesi, il numero di quelli che hanno adottato i Common Criteria si è ingrandito fino agli attuali 31 Paesi inseriti nel Common Criteria Recognition Agreement o CCRA. Dei 31 paesi, 17 sono Certificate Authorizing, che hanno cioè implementato uno schema di accreditamento per concedere la certificazione ai prodotti o sistemi che hanno superato positivamente la valutazione portata a termine da appositi laboratori che operano sotto la loro giurisdizione. L'accordo CCRA prevede il mutuo riconoscimento dei certificati fino al livello EAL4. I primi 17 Paesi e i rimanenti 14 formano l'insieme dei Paesi Certificate Consuming, che si impegnano a riconoscere le certificazioni emesse dai Certificate Authorizing.

Al fine di dimostrare quanta fiducia si possa riporre nelle misure di sicurezza di un prodotto informatico, si stanno facendo strada anche metodologie più “leggere” e soprattutto meno onerose in termini di tempo e costi. Tra quelle più conosciute vi sono la britannica CAP (Commercial Product Assurance) e la

francese CSPN (Certification de Sécurité de Premier Niveau). In genere si basano su un controllo documentale e un eventuale e successivo penetration test. La metodologia è lungi dall'avere la completezza dei Common Criteria ma è di gran lunga più accettabile in termini di tempi da mettere a calcolo e di costi.

D.1.2 Tecnica della valutazione

I prodotti e sistemi da certificare sono detti Oggetto di valutazione (OdV), anche se più spesso si usa il termine inglese Target of evaluation (TOE). I requisiti di sicurezza per una tipologia di prodotto o sistema sono descritti nel documento denominato Protection Profile o Profilo di protezione (PP). A titolo di esempio sono disponibili Protection Profile per firewall e database management system.

Il documento relativo a uno specifico OdV è detto Security Target (o Target di sicurezza o Traguardo di sicurezza sulle normative italiane) e può fare riferimento a uno o più Protection Profile.

Per comprendere meglio la differenza tra ST e PP si può immaginare che un consorzio di banche voglia dettare i requisiti che un bancomat deve avere per essere proposto al consorzio stesso, come potrebbe avvenire nel caso di un bando di gara. Il documento che delinea i requisiti (il “riferimento”) è il PP. Il ST, invece, sarà quel documento che lo sviluppatore presenterà e nel quale sono descritti i requisiti di sicurezza di un prodotto o di un sistema già realizzato o in corso di realizzazione.

La certificazione è riferibile esclusivamente a una specifica e determinata versione dell'OdV, impiegata solo nella configurazione valutata e nelle condizioni previste. Pertanto, l'utente deve verificare la versione acquistata e al fatto che eventuali cambiamenti, anche correttivi, a seconda della loro entità, potrebbero dover richiedere un'ulteriore verifica.

Il potenziale utilizzatore di un prodotto certificato deve quindi sempre verificare con attenzione la documentazione pertinente prima dell'acquisto per accertarsi se può installarlo con la configurazione appropriata e nelle medesime ipotesi di utilizzo e se è previsto che sia in grado di contrastare un potenziale di attacco adeguato alle proprie esigenze.

Lo schema logico per valutare la sicurezza di un prodotto secondo i Common Criteria è illustrato in figura D.1.1.

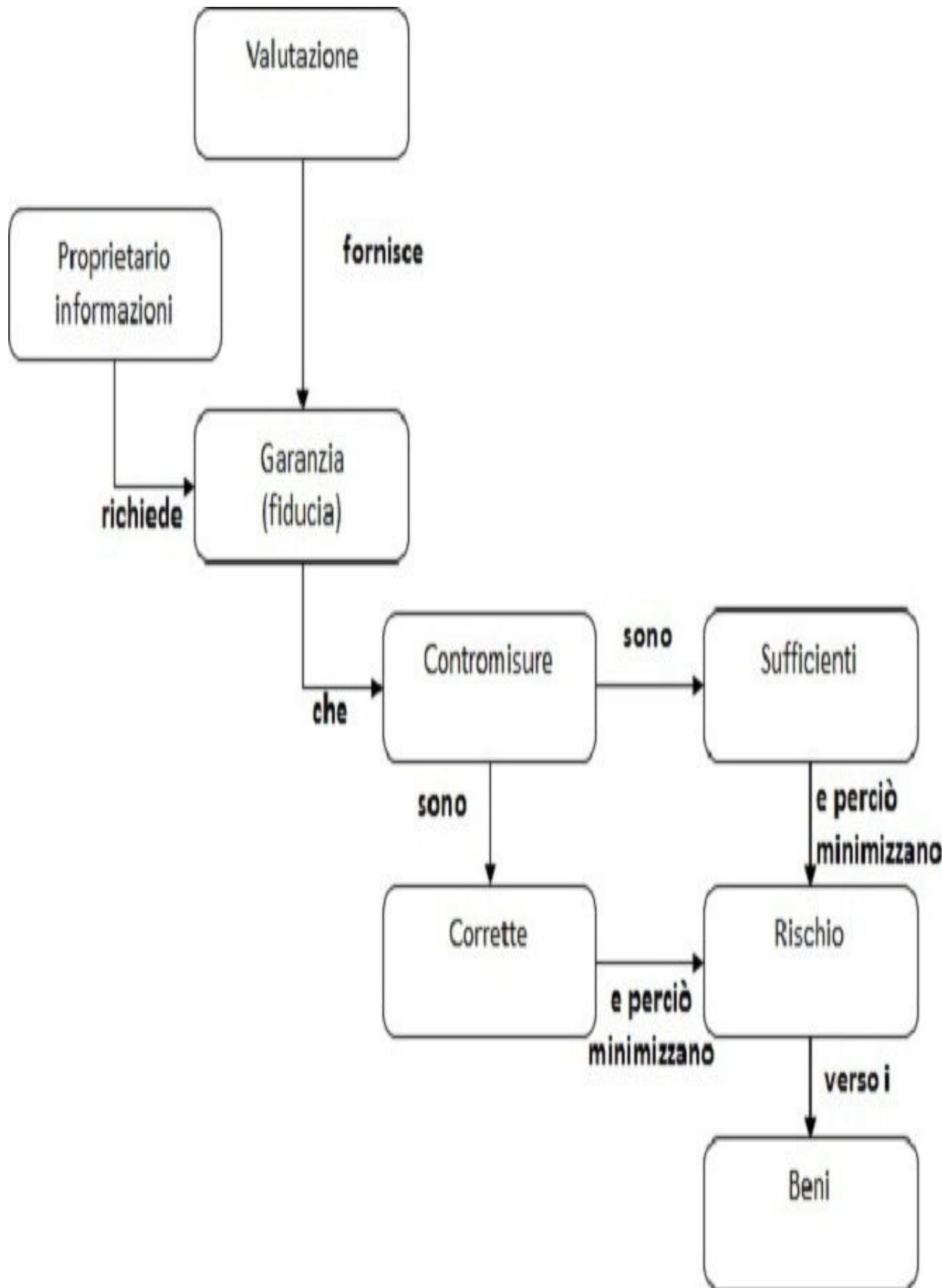


Figura D.1.1:

Concetti relativi alla valutazione ISO/IEC 15408:2009

Lo Schema di valutazione rappresenta il quadro amministrativo e normativo in cui i CC sono applicati da un'autorità di valutazione all'interno di una comunità specifica.

Gli schemi di certificazione italiani sono due: uno relativo ai prodotti e sistemi correlati alla sicurezza nazionale e alle informazioni classificate, regolato dal DPCM dell'11 aprile 2002, e l'altro relativo alla sicurezza “commerciale”, regolato dal DPCM del 30 ottobre 2003¹⁴⁵.

Il primo schema è obbligatorio nel caso che con il prodotto debbano essere trattate informazioni classificate, mentre non sussistono al momento obblighi applicativi per il secondo schema. Sarebbe opportuno che i sistemi connessi a Internet, soprattutto se si tratta di infrastrutture critiche, fossero certificati dato che, non essendo isolati fisicamente come altri, sono più soggetti alle minacce esterne.

Lo standard prevede sette livelli di garanzia crescenti (Evaluation Assurance Level o EAL), da EAL1 a EAL7, dipendenti dall'estensione e formalità della documentazione usata in fase di analisi e sviluppo, nonché dalle modalità seguite nello sviluppo. Ovviamente, più documenti a supporto della valutazione sono analizzati e più analisi tecniche e test sono fatti, maggiori sono le prove che il processo di sviluppo sia stato orientato correttamente agli aspetti di sicurezza. Questo è ancor più valido per i livelli di assurance più elevati, quando iniziano a essere impiegati sistemi formali a dimostrazione della rigorosità del processo stesso.

In definitiva, con la valutazione si avrà contezza che:

i documenti Protection Profile e Security Target, dimostrano che:

tutte le minacce sono contrastate;

sono soddisfatte tutte le politiche di sicurezza dell'organizzazione e le ipotesi;

le probabilità che il ToE contenga vulnerabilità sfruttabili da un attaccante sono molto basse e che, qualora fossero presenti, non potranno essere sfruttate con il potenziale di attacco dell'attaccante ipotizzato e che queste vulnerabilità residue rimangano sotto la soglia del rischio accettabile.

Tutti i livelli superiori al primo richiedono in misura crescente la collaborazione tra lo sviluppatore e i valutatori.

Oltre ai 7 EAL vi sono anche altri 3 livelli utilizzati esclusivamente per prodotti che integrano prodotti diversi (quelli che in precedenti versioni dei CC erano chiamati sistemi) denominati CAP (Composed Assurance Level) dal livello A al C, validi solo ed esclusivamente per prodotti già certificati e non sottoposti a ulteriori sviluppi per la loro integrazione. Per quanto di possibile interesse, soprattutto in Italia, dove la maggior parte delle aziende effettua integrazione di prodotti e più raramente attività di sviluppo, questa classificazione non sembra avere avuto successo e pertanto non sarà ulteriormente analizzata.

La valutazione di un prodotto a livello EAL1 è la valutazione di un qualcosa visto come una scatola nera (black-box), che diventa sempre più trasparente ai livelli EAL2 e EAL3, per divenire una white-box dal livello EAL4 in poi.

Una black-box è una “scatola”, intesa sia come mezzo fisico che come insieme di istruzioni, che non può essere osservata al suo interno ma può essere esplorata e compresa solo analizzando ciò che entra (input) e ciò che esce (output) senza avere informazioni sui meccanismi interni. Una white-box è l'esatto opposto di una black-box; ne risultano difatti conosciuti tutti i meccanismi interni fino al codice sorgente. Una grey-box è una via di mezzo delle due precedenti, per la quale si conoscono alcuni dei parametri fondamentali per il suo funzionamento, come la suddivisione in moduli e altre informazioni progettuali, ma non tutte le informazioni in possesso del progettista.

In conclusione, per avere prodotti nei quali nutrire un buon livello di fiducia, questi dovrebbero essere valutati almeno a livello EAL4 (quello a partire dal quale i valutatori iniziano ad analizzare il codice) per scongiurare a esempio la possibilità di attacchi buffer overflow; livelli superiori sarebbero ovviamente migliori ma, data la complessità, i costi crescono notevolmente e sono giustificati solo se opportune analisi del rischio lo suggeriscono e se il livello della minaccia è realmente molto elevato.

D.1.3 Problemi dovuti a una scarsa conoscenza dei Common Criteria

L'ISO/IEC 15408 è considerato il miglior sistema per valutare l'affidabilità di un prodotto e quindi ci si aspetterebbe un loro uso intensivo. Purtroppo alcuni aspetti ne limitano il ricorso. I principali sono gli alti costi della valutazione dovuti alla lunghezza del processo, spesso superiore all'anno (anche se, soprattutto oltreoceano, ove si fa largo uso dei PP, si riescono a ridurre in modo importante le tempistiche), anche per la necessità di adeguare i documenti all'elevato standard richiesto dall'uso dei CC che costringe molti produttori a rivedere parte della documentazione di progetto. Per risolvere questo e altri problemi, gli stessi Common Criteria sono in continua evoluzione per meglio adattarli alle esigenze degli utilizzatori (in ambito WG 3 del SC 27 del JTC 1 di ISO/IEC si sta lavorando alacremente per giungere alla versione 4 dei CC).

I tempi lunghi per la valutazione comportano altri problemi, per cui i prodotti certificati rischiano di diventare presto obsoleti prima della conclusione della loro valutazione.

L'impiego di prodotti certificati è un'attività relativamente semplice, tanto semplice che, se male utilizzata, rischia di essere essa stessa fonte di vulnerabilità. Ciò accade perché non sempre i prodotti certificati sono impiegati al meglio e nella configurazione prevista.

È infatti opinione comune che variare anche di poco la configurazione di un sistema certificato non rappresenti un grave errore, ma non è così. Infatti un piccolo cambiamento della configurazione prevista invalida la certificazione e non potrebbe essere diversamente.

L'onerosità della valutazione può portare un produttore a scegliere di certificare solo una parte delle funzioni di sicurezza del proprio prodotto. Un venditore disonesto, però, potrebbe utilizzare lo stesso sistema per mascherare la presenza di funzioni di sicurezza per qualche motivo “deboli”, facendo valutare le sole funzioni sufficientemente robuste.

Per esempio, se per un qualche motivo la funzione di configurazione da remoto di un apparato di rete non è stata inserita nella configurazione valutata (magari perché vulnerabile a qualche tipo di attacco o perché non aggiornata per ragioni di retro-compatibilità), l’abilitazione di una di tali funzioni farebbe correre un serio rischio all’utilizzatore, aggravato dal senso di fiducia che si ripone nella certificazione del prodotto. Quanto riportato non è un ipotetico esempio, è veramente successo per anni che amministratori di sistema che impiegavano un noto sistema operativo abilitassero la funzione di controllo remoto di questo prodotto che non era nella configurazione portata a certificazione. Questo è un punto importante sul quale i numerosi integratori di sistema italiani dovrebbero riflettere. Infatti, molto spesso, per integrare un prodotto in un sistema sono soliti aprire porte o abilitare servizi non previsti nella configurazione con la quale il

prodotto ha avuto la certificazione, invalidando così tutta la sicurezza del sistema stesso. Il valutatore stesso, che non è in possesso della documentazione dei prodotti già certificati, commetterebbe un grave errore nel continuare la sua attività.

Questo problema, che si riscontra nell'utilizzo di prodotti commerciali (indicati come COTS o commercial off the shelf) già valutati, è che l'integratore non è solitamente in possesso di tutta la documentazione di sviluppo dei prodotti utilizzati (informazioni riservate, solitamente cedute dietro lauto pagamento a partner con elevati volumi di vendite, situazione atipica nel nostro Paese) e quindi non può valutare i prodotti se non a bassi livelli di garanzia fino, al massimo, a EAL3, e talvolta anche meno (in genere non si può andare oltre a EAL1).

Sarebbe auspicabile la possibilità di installare un sistema certificato obbligatoriamente nella sola configurazione valutata, magari premendo un ipotetico "bottone rosso virtuale" [162]. Purtroppo questo bottone non esiste e allora occorre avere personale preparato che adotti le opportune procedure per configurare in modo corretto il prodotto anche a costo di limitarne le funzionalità.

Un ulteriore problema è rappresentato dal fatto che molti utilizzatori non leggono attentamente i Security Target o i Protection Profile. Per esempio, fino a Microsoft Windows Vista e Windows Server 2008 (certificati EAL 4), i vari sistemi operativi di casa Microsoft, così come la distribuzione Red Hat di Linux e Mac OS X, facevano riferimento al Controlled Access Protection Profile (CAPP). Lo stesso CAPP [67] riportava:

Il CAPP prevede un livello di protezione che è appropriato per una comunità di utenti non ostili e ben amministrati, che richiedono una protezione contro le minacce di tentativi involontari o casuali di violare la sicurezza del sistema. Il profilo non è destinato a essere applicabile in circostanze in cui è richiesta la

protezione contro i tentativi determinati da parte di aggressori ostili e ben motivati a violare la sicurezza del sistema. Il CAPP non è del tutto in grado di affrontare tutte le minacce poste dallo sviluppo di sistema contenenti malware o da personale amministratore.

Tradurre quanto sopra in un italiano colloquiale diviene:

Se il computer deve essere connesso a Internet, se bisogna proteggere informazioni preziose come quelle personali o bancarie, se si intendono utilizzare servizi Internet come l'email, se si intende installare software scaricato da Internet da siti sconosciuti, se si può essere attaccati da malintenzionati, non bisogna utilizzare un sistema operativo basato su questo CAPP!

Quanti hanno mai fatto la precedente considerazione?

Inoltre, quando un sistema è certificato vuol dire che i suoi meccanismi sono stati più o meno approfonditamente verificati con test ma non che è completamente esente da difetti (bug). Ogni volta che viene trovato un nuovo bug si dovrebbe apportare la relativa patch ma così facendo si invalida la certificazione. Ciò fa insinuare dubbi sul sistema della certificazione, dubbi che in realtà possono essere fugati tranquillamente perché è sufficiente fare un'analisi di impatto per comprendere quanto e come la modifica influisce sul sistema. Se la modifica è minore, sarà direttamente confermata la certificazione, mentre, se è maggiore, sarà sufficiente rivalutare solo le parti del prodotto che sono state variate e riemettere la certificazione in tempi brevi. Può agevolare il tutto un prodotto dove è implementata la classe di assurance ALC_FLR (Assurance Lyfe Cycle_Flow Remediation) almeno dalla terza componente in su per avere contezza che la procedura di patching è stata eseguita correttamente.

Comunque, una valutazione Common Criteria è solo il primo importante passo

per l'utilizzo in sicurezza di un prodotto. Infatti la valutazione viene effettuata in laboratori dove la realtà è simulata e dove tutte le predisposizioni sono pedissequamente rispettate, contrariamente a quanto purtroppo talvolta avviene nei sistemi effettivamente utilizzati. Inoltre, nella valutazione si fanno delle ipotesi di utilizzo non sempre attuate. Ecco perché, una volta installato il sistema, si devono utilizzare anche altri sistemi per ridurre al minimo le possibilità d'errore, facendo per esempio dei penetration test periodici per le verifiche del rispetto delle predisposizioni.

Per approfondire le tematiche relative ai possibili margini di miglioramento dei CC si veda [162].

D.2 FIPS 140-3

D.2.1 Generalità

Nel lontano 1994 venne rilasciato lo standard FIPS 140-1 (dove FIPS sta per Federal Information Processing Standard Publication) a cura del National Institute of Standards and Technology (NIST) che aveva deciso di rilasciare la serie di pubblicazioni FIPS 140 allo scopo di coordinare i requisiti e gli standard per i moduli crittografici. A questo fece seguito la prima edizione del FIPS 140-2, risalente al 25 maggio 2001, aggiornata, poi, l'ultima volta il 3 dicembre 2002, con la collaborazione del Communication Security Establishment (CSE) del governo canadese. Da subito vennero fatti sforzi per aggiornarla alla versione 3 di cui venne prodotta una bozza nel 2013. Tale bozza non ha mai trovato concordi tutti gli esperti in materia venendo di fatto abbandonata. Nel 2012 l'ISO emanò la ISO/IEC 19790:2012 che presentava notevoli differenze dalla bozza del 2013 e per un anno sembrò rappresentare la possibile evoluzione della seconda versione, ma anche questa volta non venne accettata. Si deve arrivare al 2018 per vedere la riconferma della ISO/IEC 19790:2012, che manteneva però la nomenclatura della FIPS 140-2. Una grande confusione.

Finalmente, dopo sei mesi dalla pubblicazione, entrò in vigore il 22 settembre 2019 la FIPS 140-3 con titolo “Security Requirements for Cryptographic Modules” (“Requisiti di sicurezza per i moduli crittografici”)¹⁴⁶. Un anno esatto dopo iniziano i test con la FIPS 140-3 e dal 22 settembre del 2021 non è più possibile effettuare i test con la versione 2, essendo obbligatoria la sola versione 3. Il 21 settembre 2026 scadranno invece le certificazioni ottenute fino al 22 settembre 2021 con la vecchia FIPS 140-2.

La FIPS 140-3, le cui caratteristiche sono riassunte in figura D.2.1¹⁴⁷, è uno standard di sicurezza impiegato in campo informatico e utilizzato per validare moduli crittografici destinati a trattare informazioni sensibili ma non classificate (SBU, Sensible But Unclassified, per le agenzie e dipartimenti Federali USA, o chi lavora per essi, e Designated Information per il Canada). Anche un modulo approvato per trattare informazioni classificate potrà essere impiegato per trattare informazioni SBU ma non viceversa.

Requirement Area	Security Level 1	Security Level 2	Security Level 3	Security Level 4		
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, approved security functions, and normal and degraded modes of operation. Description of cryptographic module including all hardware, software, and firmware components. All services provide status information to indicate when the service utilizes an approved cryptographic algorithm, security function, or process in an approved manner.					
Cryptographic Module Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths		Trusted channel			
Roles, Services, and Authentication	Logical separation of required and optional roles and services	Role-based or identity-based operator authentication	Identity-based operator authentication	Multi-factor authentication		
Software / Firmware Security	Approved integrity technique, or EDC based integrity test. Defined SFMI, HFMI and HSMI. Executable code	Approved digital signature or keyed message authentication code-based integrity test	Approved digital signature-based integrity test			
Operational Environment	Non-modifiable. Limited or Modifiable Control of SSPs	Modifiable. Role-based or discretionary access control. Audit mechanism				
Physical Security	Production-grade components	Tamper evidence. Opaque covering or enclosure	Tamper detection and response for covers and doors. Strong enclosure or coating. Protection from direct probing EFP or EFT	Tamper detection and response envelope. EFP. Fault injection mitigation		
Non-Invasive Security	Module is designed to mitigate against non-invasive attacks specified in Annex "F".					
	Documentation and effectiveness of mitigation techniques specified in Annex "F"		Mitigation testing	Mitigation testing		
Security Parameter Management	Random bit generators, SSP generation, establishment, entry & output, storage & zeroization					
	Automated SSP transport or SSP agreement using approved methods					
	Manually established SSPs may be entered or output in plaintext form		Manually established SSPs may be entered or output in either encrypted form, via a trusted channel or using split knowledge procedures			
Self-Tests	Pre-operational: software/firmware integrity, bypass, and critical functions test					
	Conditional: cryptographic algorithm, pair-wise consistency, SW/FW loading, manual entry, conditional bypass & critical functions test					
Life-Cycle Assurance	Configuration Management	Configuration management system for cryptographic module, components, and documentation. Each uniquely identified and tracked throughout lifecycle		Automated configuration management system		
	Design	Module designed to allow testing of all provided security related services				
	FSM	Finite State Model				
	Development	Annotated source code, schematics or HDL	Software high-level language. Hardware high-level descriptive language	Documentation annotated with pre-conditions upon entry into module components and postconditions expected to be true when components is completed		
	Testing	Functional testing		Low-level testing		
	Delivery & Operation	Initialization procedures	Delivery procedures	Operator authentication using vendor provided authentication information		
	Guidance	Administrator and non-administrator guidance				
	Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available		Specification of mitigation of attacks with testable requirements		

Figura D.2.1:

Sintesi della FIPS 140-3

Preme qui sottolineare la parola “validato”. Il Cryptographic Module Validation Program (CMVP) valida i moduli crittografici nei confronti della FIPS 140-3 e di altri standard crittografici del National Institute of Standards and Technology e del Canadian Centre for Cyber Security. Nel CMVP, i fornitori di moduli crittografici utilizzano laboratori Cryptographic and Security Testing (CST) indipendenti e accreditati per far testare i propri moduli. Un modulo crittografico validato è quindi un elemento che è stato esaminato da un laboratorio CST accreditato dal NIST, o dal suo equivalente canadese, e a cui è stato assegnato un certificato CVMP.

Purtroppo sono molte le aziende che dichiarano che i loro moduli sono FIPS “compliant” cioè conformi. Questo significa solo che, a detta loro, sono stati progettati secondo i dettami dello standard FIPS, ma che non sono stati sottoposti a valutazione e che non hanno perciò ottenuto la certificazione di una terza parte indipendente che attesti che quanto asserito corrisponde a verità, in modo che l’utente possa nutrire nei loro confronti un livello di fiducia corrispondente alla profondità dei controlli.

Un modulo crittografico è un dispositivo di calcolo che fornisce almeno un servizio di crittografia con algoritmo approvato, come: cifratura e decifratura, secure hashing di un messaggio, generazione e verifica di firma, generazione di chiavi e gestione di chiavi crittografiche. I moduli crittografici possono essere prodotti dal settore privato (anche comunità open source) o pubblico per l’utilizzo da parte di settori particolari (come le istituzioni finanziarie e sanitarie, o più genericamente le infrastrutture critiche) che utilizzano detti moduli per raccogliere, archiviare, trasferire, condividere e diffondere informazioni critiche.

Lo standard FIPS 140-3 non riconosce un prodotto come un modulo crittografico a meno che non contenga almeno un algoritmo di crittografia approvato FIPS. Ciò significa che un prodotto potrebbe essere in grado di fornire funzioni di crittografia, ma se non può essere verificato in base a qualche algoritmo standard NIST, non potrà essere certificato per mezzo dello standard FIPS 140-3.

D.2.2 Tecnica della valutazione

La prima macroscopica differenza tra la FIPS 140-2 e la FISP 140-3 è che la FIPS 140-2 constava in un documento di più di 60 pagine mentre l'attuale è di solo 11. Questa riduzione drastica delle pagine scritte, ma non del contenuto implicito, la si è ottenuta grazie al fatto che fa esplicito riferimento a due standard internazionali e cioè alla ISO/IEC 19790:2012 e alla ISO/IEC 24759:2017.

L'entrata in vigore della FIPS 140-3 rappresenta infatti l'adozione formale di due standard internazionali descritti di seguito, anche se con alcune modifiche ai suoi allegati (Annexes):

ISO/IEC 19790:2012(E) - Security Requirements for Cryptographic Modules (Requisiti di sicurezza per i moduli crittografici). Specifica i requisiti dettagliati per la valutazione della sicurezza del modulo crittografico per la protezione delle informazioni sensibili. Lo standard ISO/IEC 19790:2012 definisce quattro livelli di sicurezza (Security Level), da SL1, il più semplice da ottenere a SL4, per ciascuna delle undici aree dei requisiti. Tutti i Security Level sono destinati a coprire un'ampia gamma di potenziali applicazioni e ambienti. Ogni livello di sicurezza è cumulativo. Ciò significa che a livello 2 è necessario soddisfare tutti i requisiti di livello 1. A livello 3 si devono soddisfare tutti quelli di livello 2 e livello 1, eccetera.

ISO 24759:2017 - Test Requirements for Cryptographic Modules (Requisiti di prova per moduli crittografici) è il corrispettivo del documento del NIST Derived Test Requirements for FIPS 140-2). Questo specifica il meccanismo e le procedure che devono essere impieghi dai laboratori di prova per garantire che il modulo crittografico segua i requisiti specificati di ISO/IEC 19790:2012. L'obiettivo principale dello sviluppo di questo standard è fornire autenticità e conformità al processo di test affinché sia lo stesso in tutti i laboratori. Evidenzia anche il formato delle informazioni (prove sussidiarie per la dimostrazione della conformità a ISO/IEC 19790:2012) fornito dai fornitori/sviluppatori ai laboratori di prova.

I test per i requisiti di cui alla ISO/IEC 19790:2012 devono essere conformi alla norma ISO/IEC 24759:2017, con le modifiche, aggiunte o eliminazioni delle prove del fornitore e dei test consentiti dall'autorità di convalida. Il principale cambiamento in FIPS 140-3 è limitato all'introduzione di requisiti fisici non invasivi.

È interessante notare la fiducia che il governo americano nutre nei confronti di ISO tanto da dichiarare, al paragrafo 3.1 della FIPS 140-3, che si applica sempre l'ultima edizione dei due standard internazionali citati.

Le FIPS 140-3 Special Publications (SP) del NIST cui si fa riferimento sono:

SP 800-140: FIPS 140-3 Derived Test Requirements (DTR);

SP 800-140 Annex A: CMVP Documentation Requirements;

SP 800-140 Annex B: CMVP Security Policy Requirements;

SP 800-140 Annex C: CMVP Approved Security Functions;

SP 800-140 Annex D: CMVP Approved Sensitive Security Parameter

Generation and Establishment Methods;

SP 800-140 Annex E: CMVP Approved Authentication Mechanisms;

SP 800-140 Annex F: CMVP Approved Non-Invasive Attack Mitigation Test Metrics.

Vi sono cinque fasi principali per la validazione ai sensi della FIPS 140-3:

il vendor sottomette il modulo crittografico e la documentazione al laboratorio CST;

il laboratorio CST, sulla base del (CAVP), utilizza una serie di test per verificare la corretta funzionalità crittografica nei confronti degli algoritmi di crittografia approvati (Approved Cryptographic algorithms). Una volta superato il CAVP, il laboratorio invia il rapporto dei test CAVP al NIST/CSE che verifica che il test sia stato superato con successo e che la documentazione e la progettazione del modulo siano conformi allo standard;

il passo successivo è ottenere che il modulo sia inserito nella “Cryptographic Module Validation Program FIPS 140-3 Implementation Under Test List” che dimostra che l’IUT viene testato da un laboratorio CST;

una volta terminato il processo di test da parte del CST, il modulo viene elencato nel “Cryptographic Module Validation Program FIPS 140-3 Modules in Process List” in attesa che la documentazione venga esaminata dal NIST/CSEC;

infine, l’IUT sarà elencato negli “FIPS 140-3 Cryptographic Module Validation Lists” non appena la convalida termina con successo.

Per capire le verifiche richieste dallo standard FIPS 140-3, è necessario comprendere innanzitutto l’oggetto della convalida. Questo può essere una qualsiasi combinazione di hardware, firmware e software che fornisca almeno una funzione di sicurezza approvata. I moduli di crittografia più comuni oggi

eseguono cifratura e decifrazione con AES. Tuttavia sarebbe possibile convalidare un modulo crittografico che utilizza solo un algoritmo di hash per l'autenticazione, come lo SHA-256.

Le applicazioni informatiche o di telecomunicazioni in cui vengono impiegati moduli crittografici sono molteplici e vanno da quelle di identificazione e autenticazione a quelle di accesso, a quelle relative ai vari stati in cui si può trovare un dato e cioè: a riposo (at rest), come in un database, in movimento (in transit), come quando vengono trasmesse su un canale o tramite un protocollo protetto, e in uso (in use).

Gli ambienti in cui si utilizzano sono quelli a maggior rischio e pertanto il livello di sicurezza dovrà essere appropriato ai requisiti di sicurezza dell'applicazione e dell'ambiente in cui verrà utilizzato il modulo e ai servizi di sicurezza che il modulo fornirà.

I requisiti di sicurezza coprono aree relative alla progettazione e implementazione sicura di un modulo crittografico. Queste aree includono:

le specifiche del modulo crittografico;

le interfacce per moduli crittografici;

ruoli, servizi e autenticazione;

sicurezza del software e firmware;

l'ambiente operativo;

la sicurezza fisica;

la sicurezza non invasiva;

la gestione dei parametri sensibili di sicurezza;

l'autotest;

la garanzia del ciclo di vita;

la mitigazione da altri attacchi.

Quanto sopra non significa che la conformità a questo standard sia sufficiente per garantire che un particolare modulo sia sicuro. Anche l'applicazione in cui il modulo è inserito deve essere valutata al fine di individuare qualsiasi rischio residuo in modo che sia riconosciuto e accettato.

I requisiti di sicurezza specificati in questo standard sono il risultato di un processo che ha visto la cooperazione del settore privato con il governo federale per determinare quali fossero adatti a contrastare le varie minacce implementando un sistema tale da rendere un qualsiasi attacco più costoso del possibile profitto. Dato che la tecnologia in questo campo evolve rapidamente, occorre che lo standard sia sufficientemente flessibile e, come minimo, lo standard dovrà essere rivisto ogni 5 anni.

Occorre sfatare due grandi miti sulla FIPS 140-3:

un modulo crittografico valutato positivamente rispetto a questo standard (ad esempio un modulo che implementa l'AES) non è affatto un modulo che impiega crittografia militare, termine molto usato dai commerciali per definire la bontà di un prodotto che usa la crittografia;

la verifica non usa simulazioni di attacchi crittoanalitici, ma solo test di comparazione tra algoritmi di riferimento e l'algoritmo del modulo crittografico attraverso il programma CAVP.

D.2.3 Problemi dovuti all’impiego della FIPS 140-3

Il primo aspetto veramente negativo è che i due standard ISO/IEC ricordati sopra sono a pagamento mentre la FIPS 140-2 si poteva scaricare gratuitamente a tutto beneficio della diffusione della cultura della sicurezza informatica.

Purtroppo l’uso di FIPS 140-2, anche quando combinato ai CC, non garantisce la completa sicurezza. Soprattutto quando sono le istituzioni che introducono delle backdoor nell’algoritmo crittografico; come pare sia successo nel caso del Dual_EC_DRBG (Dual Elliptic Curve Deterministic Random Bit Generator, NIST 800-90A) con la NSA. In detto algoritmo sembra che i parametri P e Q delle curve ellittiche fossero stati scelti appositamente in correlazione tra loro per inficiare i risultati del protocollo SSL quando li utilizza. Probabilmente questo ha avuto impatti su molti sistemi, dato che il Dual_EC_DRBG è inserito come default nella libreria crittografica RSA BSAFE. Con tutta probabilità, poi, è stato per questo sospetto che, nel 2018, ISO si è rifiutò di adottare i due algoritmi di cifratura a blocchi “leggieri” Simon e Speck, proposti dal NIST, dopo una diatriba durata 4 anni.

Un altro disastro eclatante, con vasta eco nel 2008, è quello relativo all’implementazione di OpenSSL su Debian dove, per un errore dello sviluppatore, fu ridotto il campo del seme del random bit generator per la generazione delle chiavi.

Altro difetto, poi risolto, fu identificato su alcune versioni certificate di chiavi USB di marca SanDisk, Verbatim e Kingston. Questo permetteva di avere accesso ai dati cifrati da parte di persone non autorizzate. La vulnerabilità non si trovava nell’algoritmo crittografico AES con chiave a 256-bit, bensì nell’applicazione di interfacciamento installata sul computer ospite, atta a validare la password utilizzata per autorizzare la decifrazione dei dati. Alcuni

ricercatori tedeschi scoprirono che quando l’utente utilizzava la password corretta il programma inviava sempre la stessa stringa al drive per autorizzare la decifrazione dei dati. Realizzarono allora una routine nel programma di validazione in modo che, qualsiasi password venisse digitata, il sistema inviava la stringa di autorizzazione prevista e i dati venivano decifrati senza impiegare la password corretta. Impressionante vero?

Questi esempi negativi non devono però scoraggiare i ricorso a sistemi di certificazione, che garantiranno sempre e comunque che persone competenti abbiano fatto delle verifiche e non ci si debba fidare ciecamente del vendor che potrebbe avere interessi ben comprensibili a mettere in vendita prodotti di qualità discutibile, come in passato hanno fatto anche aziende dai nomi altisonanti.

Note

¹⁴⁴<https://www.commoncriteriaportal.org/cc/>

¹⁴⁵<https://atc.mise.gov.it/index.php/sicurezza/ocsi>.

¹⁴⁶La FIPS 140-2 e le sue appendici sono reperibili presso il sito del NIST:
<https://csrc.nist.gov/publications/fips>.

¹⁴⁷<https://lightshipsec.com/fips-140-3-is-here/>

Appendice E

Requisiti per i cambiamenti

Lui: Io sono come sono.

Lei: Cerca di cambiare.

Lui: Sono cambiato.

Lei: Non sei più quello di una volta.

Elio e le Storie tese, Cara ti amo

In questa appendice sono riportati i requisiti da considerare quando si apportano cambiamenti ai sistemi informatici.

Questo elenco potrebbe essere considerato anche per verificare, in fase di analisi dei controlli di sicurezza e delle vulnerabilità, la sufficienza e correttezza delle misure di sicurezza previste e attuate per i sistemi informatici (server, apparati di rete, applicazioni, PC, dispositivi portatili come cellulari, smartphone e tablet). Ovviamente, non tutte le misure sono pertinenti a ciascun tipo di sistema.

E.1 Requisiti funzionali di controllo accessi

Meccanismi per la gestione degli utenti (inserimento, modifica dei diritti di accesso, sospensione, cancellazione) o garanzia di interfacciamento con

strumenti già in uso presso l'organizzazione (per esempio LDAP).

Livello di dettaglio con cui si possono impostare i diritti di accesso ai sistemi (singola funzionalità, singola transazione, eccetera).

Verifica delle autorizzazioni per accedere o visualizzare le elaborazioni.

Disponibilità di documentazione sui ruoli predefiniti e di tecniche per disattivarli.

Opzione “cambia la password al primo utilizzo” quando si inserisce un nuovo utente o quando la password è modificata dagli amministratori di sistema (per esempio se l'utente l'ha dimenticata);

Password nascosta nel campo dove inserire la password.

Possibilità di bloccare l'utenza dopo un certo numero di tentativi errati di inserimento della password (da non applicare a tutti gli amministratori di sistema perché, in caso di attacco, nessuno potrebbe più accedere al sistema).

Modalità di recupero delle password di amministrazione.

Possibilità di assegnazione a più utenti dei poteri di amministrazione, anche su singole parti del sistema.

Personalizzazione delle credenziali per gli amministratori di sistema.

Controllo automatico delle caratteristiche delle password in modo che gli utenti non le scelgano banali: complessità (devono essere presenti lettere e numeri; oppure lettere minuscole, lettere maiuscole e numeri e caratteri speciali), lunghezza (minimo 8 caratteri), scadenza (affinché siano cambiate almeno ogni 3 mesi), blocco in caso di inattività dell'utente (dopo non più di 6 mesi), non ripetibilità delle ultime 5 o 10 password.

Controllo automatico della non banalità delle password; p.e. password non nel dizionario, non una variazione della user-id come Cesare1970, non una variazione del nome dell'applicazione come Oracle70, non una password popolare come 12345678 (queste regole sono considerate alternative e più sicure di quelle relative alla complessità descritta sopra [57]);

Configurazione affinché gli utenti siano sconnessi dopo 5 o 10 o più minuti di inattività.

Configurazione affinché gli utenti non possano connettersi in specifici orari o da alcuni Paesi.

E.2 Requisiti sulla connettività

Possibilità di rendere obbligatorio l'uso di connessioni cifrate per accedere al sistema.

Modalità di interfacciamento con altri programmi o con l'utente che preveda connessioni cifrate, scambio di certificati digitali, autenticazione reciproca senza utenze di amministrazione o generiche.

E.3 Requisiti funzionali relativi alla crittografia

Memorizzazione dei dati con cifratura.

Meccanismi di firma o logging se devono essere garantiti certi livelli di non ripudiabilità delle attività.

Protocolli crittografici sicuri e adeguati agli standard applicabili (AES per la crittografia a chiave privata, RSA per la crittografia a chiave pubblica, DSS del NIST FIPS 186-3 per le firme, FIPS 140-2 Annex C per la generazione di numeri casuali, eccetera).

Accesso alla chiavi crittografiche limitato ai soli amministratori di sistema o solo a processi interni del software.

Chiavi crittografiche generate secondo metodi sicuri, partendo da seed generati

casualmente.

E.4 Requisiti di monitoraggio

Disponibilità di log applicativi e log delle attività degli amministratori di sistema.

Meccanismi per garantire la sicurezza dei log.

Meccanismi per stabilire la durata della conservazione dei log.

Modalità di collegamento del sistema ai sistemi di monitoraggio già in uso.

Clock sincronizzabile con un NTP server.

E.5 Requisiti di capacità

Definizione di “prestazioni accettabili”

Numero totale di utenti per cui il sistema garantisce prestazioni accettabili.

Numero di utenti connessi contemporaneamente per cui il sistema garantisce prestazioni accettabili.

E.6 Requisiti architetturali

Modularità del sistema, in modo che sue diverse componenti possano essere

installate in ambienti diversi.

Separazione del sistema da altri sistemi, per evitare accessi non autorizzati.

Possibilità di utilizzo del sistema anche nell’ambiente di disaster recovery (verificare anche se è necessario acquistare licenze ulteriori).

Per i dispositivi IoT, possibilità di utilizzo anche in assenza di alimentazione elettrica.

Per i dispositivi IoT e OT, riavvio tale da non compromettere altri processi e la sicurezza fisica delle persone.

Per i dispositivi di sicurezza fisica, completa separazione dagli altri sistemi informatici.

Per i dispositivi OT, possibilità di accesso agli operatori in caso di emergenza.

Se i dispositivi sono soggetti a polvere, calore, eccetera, adeguati livelli di protezione.

E.7 Requisiti applicativi

Verifica e sanamento (dall’inglese sanitization) dei dati in ingresso a livello server, soprattutto quando ricevuti da fonti non sicure come il web (per esempio, se è prevista una data, il sistema verifica che si tratti di una data e non di altri caratteri; se sono previsti input di un certo numero di caratteri, il sistema verifica che la loro lunghezza non sia eccedente).

Verifica degli input anche nei campi di testo libero come quelli usati per le note e i commenti.

Filtri quando si modificano i dati, per esempio con messaggi “sei sicuro di voler modificare” o con richiesta di validazione da altri utenti.

Limitazione delle possibilità di ricerca, in modo che un utente non possa

visualizzare dati a cui non è autorizzato.

Dati a video e stampati senza informazioni riservate o per le quali l'utente non ha le autorizzazioni ad accedere.

Tipo di messaggi e di avvisi lanciati dal sistema che forniscano sufficienti informazioni al personale autorizzato, ma non forniscano informazioni a malintenzionati (per esempio, fornendo troppi dettagli sul tipo di errore quando si inseriscono credenziali sbagliate).

Sistemi di cancellazione automatica dei dati, o di avviso, quando hanno superato il tempo di conservazione previsto (retention time).

Quadratura delle elaborazioni.

Richiesta di approvazione da parte di più ruoli per le azioni più critiche.

E.8 Requisiti di servizio

Disponibilità di attività di formazione.

Manuali aggiornati per gli utenti e gli operatori.

Processo per cambiare le procedure, le istruzioni e i manuali.

Garanzia della gestione delle vulnerabilità riscontrate e del patching (il produttore deve garantire un servizio di avviso e di invio delle correzioni).

Appendice F

Requisiti per contratti e accordi con i fornitori

“Così fanno 60.000 tonde

mi scusi non ho il resto

le do anche 400 caramelle”

“in cartone?!?”

“no!....sciolte...”

Vasco Rossi, Alibi

Nel seguito sono elencati i requisiti da prevedere nei contratti o accordi con i fornitori. Sono riportati tre casi di requisiti per:

fornitori di prodotti e della relativa assistenza;

fornitori di servizi non informatici;

fornitori di servizi informatici.

Nel seguito i requisiti previsti dalla normativa in materia di trattamento dei dati personali sono accennati. Si raccomanda lo studio di altri testi per approfondire.

In tutti i casi, il contratto deve riportare i prodotti e servizi oggetto del contratto, la durata e, nel caso di trattamento di dati personali, il tipo di dati personali trattati e le categorie di interessati.

F.1 Requisiti per i fornitori di prodotti

Questi requisiti possono essere applicati a fornitori di prodotti e della relativa assistenza, esclusa quella che prevede l'accesso diretto ai sistemi informatici e alle informazioni del cliente.

Accordo di riservatezza reciproco.

Misure di sicurezza applicabili al prodotto (vedere appendice E).

Canali di comunicazione da utilizzare.

Modalità per inoltrare e gestire i reclami dal cliente al fornitore.

Modalità per ricevere segnalazioni di potenziali criticità sulla qualità del prodotto dal fornitore al cliente.

Applicabilità dei requisiti normativi al prodotto.

Processo da seguire per modificare o aggiornare il contratto e i requisiti tecnici.

Modalità da seguire al momento della chiusura del contratto di assistenza (passaggio di consegne).

Certificati o attestati di test relativi alla sicurezza informatica dei prodotti forniti.

F.2 Requisiti per i fornitori di servizi non informatici

Accordo di riservatezza reciproco.

Misure di sicurezza tecniche del servizio.

Diritto di audit presso il fornitore.

Modalità di monitoraggio o verifica delle attività del fornitore.

Canali di comunicazione da utilizzare.

Modalità per inoltrare i reclami dal cliente al fornitore.

Modalità per ricevere segnalazioni di potenziali criticità sulla qualità del servizio dal fornitore al cliente.

Reciproci obblighi per il rispetto della normativa vigente e i criteri da seguire in caso di modifiche alla stessa.

Ruoli privacy.

Modalità di gestione dei sub-fornitori.

Gestione dei trasferimenti in altri Paesi.

Piano di continuità operativa del fornitore.

Prestazioni previste (per esempio, in termini di velocità di risposta) in base al carico di lavoro concordato.

Tempi massimi di indisponibilità del servizio e casi per cui il loro mancato rispetto non dà origine a penali per il fornitore.

Procedura da seguire in caso di necessità di raccolta di prove legali presso il fornitore.

Processo da seguire per modificare o aggiornare il contratto e i requisiti tecnici.

I casi e le modalità con cui è possibile chiudere il contratto prima della sua naturale scadenza.

Modalità da seguire al momento della chiusura del contratto (passaggio di consegne) e tempi di conservazione dei dati.

Tempi e modalità di comunicazione e di presa in carico e di risoluzione degli incidenti.

Modalità di gestione delle richieste e dei diritti degli interessati al trattamento dei dati personali.

Certificati relativi al sistema di gestione per la sicurezza delle informazioni del fornitore.

Certificati relativi alle competenze in materia di sicurezza delle informazioni delle persone addette al servizio.

F.3 Requisiti per i fornitori di servizi informatici

Questi requisiti sono applicabili, tra gli altri, ai fornitori di assistenza che prevede l'accesso diretto ai sistemi informatici e alle informazioni del cliente.

Accordo di riservatezza reciproco.

Misure di sicurezza applicabili al servizio (vedere anche appendice E).

Diritto di audit presso il fornitore.

Modalità di monitoraggio o verifica delle attività del fornitore.

Canali di comunicazione da utilizzare.

Caratteristiche del sistema di ticketing da utilizzare per le segnalazioni dal cliente al fornitore e viceversa.

Modalità per inoltrare e gestire i reclami dal cliente al fornitore.

Modalità per inoltrare segnalazioni di potenziali criticità sulla qualità del servizio dal fornitore al cliente.

Reciproci obblighi per il rispetto della normativa vigente e i criteri da seguire in caso di modifiche alla stessa.

Ruoli privacy.

Modalità di gestione dei sub-fornitori.

Gestione dei trasferimenti in altri Paesi e luoghi dove sono collocati i server utilizzati per il servizio, anche per evitare Paesi dove è in vigore una legislazione in contrasto con quella a cui è soggetta l'organizzazione.

Piano di continuità operativa del fornitore.

Prestazioni previste (per esempio, in termini di velocità di risposta) in base al carico di lavoro concordato.

Tempi massimi di indisponibilità del servizio e casi per cui il loro mancato rispetto non dà origine a penali per il fornitore.

Processo da seguire per modificare o aggiornare il contratto e i requisiti tecnici.

I casi e le modalità con cui è possibile chiudere il contratto prima della sua naturale scadenza.

Modalità da seguire al momento della chiusura del contratto (passaggio di consegne) e tempi di conservazione dei dati.

Caratteristiche di sicurezza fisica delle sale dove sono collocati i server.

Caratteristiche di continuità dell'alimentazione dei server (UPS e generatori regolarmente verificati).

Caratteristiche dei canali di connessione alla rete pubblica (utilizzo di canali alternativi nel caso in cui uno di essi si guasti).

Procedura da seguire quando il cliente vuole chiedere cambiamenti al servizio informatico.

Procedura da seguire quando il fornitore vuole apportare cambiamenti al servizio informatico (per esempio, il cliente deve essere preavvisato di ogni modifica con congruo anticipo, in modo da prepararsi in caso di interruzioni o da recidere il contratto se le modifiche risultassero inaccettabili).

Messa a disposizione di manuali per gli operatori e per gli utenti del servizio informatico.

Responsabilità per l'esecuzione e verifica dei backup dei dati e del software.

Caratteristiche di sicurezza della rete informatica del fornitore e della sua segmentazione.

Caratteristiche di sicurezza dell'accesso ai dati e ai programmi (per esempio, canali sicuri mediante connessioni cifrate).

Modalità da seguire in caso di dismissione o riutilizzo dei supporti di memorizzazione.

Procedure per la gestione degli utenti del cliente e delle loro credenziali.

Caratteristiche di sicurezza dei server e degli apparati di rete, incluse le modalità di configurazione.

Tempi e modalità di comunicazione e di presa in carico e di risoluzione degli incidenti.

Modalità di gestione delle richieste e dei diritti degli interessati al trattamento dei dati personali.

Procedura da seguire in caso di necessità di raccolta di prove legali presso il fornitore.

Dichiarazione per stabilire chi è il proprietario del software e dei sistemi informatici.

Certificati o attestati di test relativi alla sicurezza informatica dei prodotti utilizzati per erogare i servizi.

Processo per la conduzione di vulnerability assessment sui sistemi informatici da

parte del cliente (o un suo rappresentante) o del fornitore.

Certificati relativi al sistema di gestione per la sicurezza delle informazioni del fornitore.

Certificati relativi alle competenze in materia di sicurezza delle informazioni delle persone addette al servizio.

Appendice G

I controlli della ISO/IEC 27002:2022

La tabella riporta i controlli della ISO/IEC 27002:2022 e i paragrafi di questo libro che li trattano. La traduzione dei controlli della ISO/IEC 27002 non è quella ufficiale, in quanto non è ancora disponibile.

Controllo ISO/IEC 27002:2022 (Italiano)	Paragrafo di questo libro
5.1 Politiche per la sicurezza delle informazioni	12.2 Politiche di sicurezza delle informazioni
5.2 Ruoli e responsabilità per la sicurezza delle informazioni	12.3.1 Organizzazione
5.3 Separazione dei compiti	12.3.2 Separazione dei ruoli
5.4 Responsabilità della direzione	12.3.1.1 La Direzione
5.5 Contatti con le autorità	12.3.4 Rapporti con le autorità
5.6 Contatti con gruppi di interesse	12.4.3.2 Gruppi di interesse
5.7 Monitoraggio delle minacce	12.3.5 Monitoraggio delle minacce
5.8 Sicurezza delle informazioni nella gestione dei progetti	12.3.3 Gestione dei progetti
5.9 Inventario delle informazioni e degli altri asset associati	12.5.1.1 Identificazione e censimento delle informazioni 12.5.1.2 Responsabile delle informazioni
	12.5.2.1

	Identificazione e censimento degli asset
5.10 Uso accettabile delle informazioni e degli altri asset associati	12.5.2.2 Proprietà degli asset
5.11 Restituzione degli asset	12.2 Politiche di sicurezza delle informazioni 12.5.1.5 Trattamento
5.12 Classificazione delle informazioni	12.6.3.1 Assegnazione e ritiro delle autorizzazioni
5.13 Etichettatura delle informazioni	12.5.1.3 Classificazione delle informazioni
5.14 Trasferimento delle informazioni	12.5.1.4 Etichettatura
5.15 Controllo degli accessi	12.10.4 Scambi di informazioni
5.16 Gestione delle identità	12.6 Controllo degli accessi 12.10.1 Servizi autorizzati 12.6.3 Autorizzazioni
5.17 Informazioni di autenticazione	12.6.1 Credenziali e identificazione 12.6.3.1 Assegnazione e ritiro delle autorizzazioni”
5.18 Diritti di accesso	12.6.1 Credenziali e identificazione 12.6.3.1 Assegnazione e ritiro delle autorizzazioni”
5.19 Sicurezza delle informazioni nelle relazioni con i fornitori	12.6.3.1 Assegnazione e ritiro delle autorizzazioni 12.6.3.2 Riesame delle utenze
5.20 Sicurezza delle informazioni negli accordi con i fornitori	12.12.2 Selezione dei fornitori
	12.12.1 Gli accordi e i contratti con i fornitori

- 5.21 Sicurezza delle informazioni nella filiera di fornitura ICT
 - 12.12.1.2 Clausole specifiche per i servizi informatici
 - 12.12.3 Monitoraggio dei fornitori
 - 12.12.4 Cloud computing e fornitori
- 5.22 Monitoraggio, riesame e gestione dei cambiamenti dei servizi dei fornitori
 - 12.13.1 Ruoli e procedure
 - 12.13.2.7 Notifica
 - 12.13.2.3 Categorizzazione
 - 12.13.2.6 Escalation
 - 12.13.2.8 Risoluzione e ripristino
 - 12.13.4 Gestione dei problemi
 - 12.13.6 Digital forensics
- 5.23 Sicurezza delle informazioni per l'uso dei servizi cloud
 - 12.14.1 La business impact analysis (BIA)
 - 12.14.3 Obiettivi e strategie di ripristino
 - 12.14.4 I piani di continuità
 - 12.14.5 Test e manutenzione
 - 12.14.1 La business impact analysis (BIA)
 - 12.14.3 Obiettivi e strategie di ripristino
 - 12.14.4 I piani di continuità
- 5.24 Pianificazione e preparazione per la gestione degli incidenti relativi alla sicurezza delle informazioni
 - 12.7.6 Normativa applicabile alla crittografia
 - 12.15.1 Normativa vigente
 - 12.15.2 Contratti
- 5.25 Valutazione e decisione sugli eventi relativi alla sicurezza delle informazioni
 - 12.15.1.3 Normativa sul
- 5.26 Risposta agli incidenti relativi alla sicurezza delle informazioni
 - 12.14.1 La business impact analysis (BIA)
 - 12.14.3 Obiettivi e strategie di ripristino
 - 12.14.4 I piani di continuità
- 5.27 Apprendimento dagli incidenti relativi alla sicurezza delle informazioni
 - 12.14.1 La business impact analysis (BIA)
 - 12.14.3 Obiettivi e strategie di ripristino
 - 12.14.4 I piani di continuità
- 5.28 Raccolta di prove
 - 12.14.1 La business impact analysis (BIA)
 - 12.14.3 Obiettivi e strategie di ripristino
 - 12.14.4 I piani di continuità
- 5.29 Sicurezza delle informazioni durante le interruzioni
 - 12.14.1 La business impact analysis (BIA)
 - 12.14.3 Obiettivi e strategie di ripristino
 - 12.14.4 I piani di continuità
- 5.30 Preparazione dell'ICT per la continuità operativa
 - 12.14.1 La business impact analysis (BIA)
 - 12.14.3 Obiettivi e strategie di ripristino
 - 12.14.4 I piani di continuità
- 5.31 Requisiti legali, statutari, regolamentari e contrattuali
 - 12.7.6 Normativa applicabile alla crittografia
 - 12.15.1 Normativa vigente
 - 12.15.2 Contratti
- 5.32 Diritti di proprietà intellettuale
 - 12.15.1.3 Normativa sul

	diritto d'autore e sulla proprietà industriale
5.33 Protezione delle registrazioni	12.1.4 Archiviazione delle registrazioni 12.1.5 Tempo di conservazione 12.5.1.8 Tempi di conservazione
5.34 Privacy e protezione dei dati personali	12.15.1.9 Normativa sui dati personali (Privacy) 12.15.3 Audit 12.15.4 Vulnerability assessment
5.35 Riesame indipendente della sicurezza delle informazioni	12.15.5 Il riesame del sistema di gestione
5.36 Conformità con le politiche, le regole e le norme di sicurezza delle informazioni	12.1 Documenti
5.37 Procedure operative documentate	12.4.1.1 Selezione del personale
6.1 Screening	12.4.1.2 Contratto con il personale
6.2 Termini e condizioni di impiego	12.4.3 Competenze e sensibilizzazione
6.3 Consapevolezza, istruzione, formazione e addestramento sulla sicurezza delle informazioni	12.4.1.4 Sanzioni disciplinari
6.4 Processo disciplinare	12.4.2 Uscita del personale e cambiamenti di posizione
6.5 Responsabilità dopo la cessazione o variazione del rapporto di lavoro	12.4.1.3 Accordo di riservatezza con il personale 12.12.1 Gli accordi e i contratti con i fornitori 12.15.2 Contratti
6.6 Accordi di riservatezza o di non divulgazione	12.4.4 Lavoro fuori sede
6.7 Lavoro remoto	12.13.2.1 Rilevazione e comunicazione
6.8 Segnalazione degli eventi di sicurezza delle informazioni	

7.1 Perimetri di sicurezza fisica	12.8.1.1 Perimetro di sicurezza fisica
7.2 Accessi fisici	12.8.1.3 Controllo degli accessi alla sede e ai locali
	12.8.1.4 Visitatori
	12.8.1.5 Aree di consegna e ritiro di materiali
	12.8.1.9 Aree speciali
	12.8.3.1 Controllo accesso agli archivi fisici
7.3 Sicurezza degli uffici, stanze e strutture	12.8.1.8 Uffici, stanze e aree di servizio
7.4 Monitoraggio della sicurezza fisica	12.8.1.7 Antintrusione e videosorveglianza
7.5 Protezione dalle minacce fisiche e ambientali	12.8.1.2 Sicurezza ambientale
7.6 Lavorare in aree sicure	12.8.1.9 Aree speciali
7.7 Scrivania e schermo puliti	12.8.3.3 Scrivania pulita
7.8 Disposizione delle apparecchiature e loro protezione	12.9.8.3 Clear screen
7.9 Sicurezza delle apparecchiature e degli asset all'esterno delle sedi	12.8.2.1 Disposizione delle apparecchiature
7.10 Supporti di memorizzazione	12.8.2.5 Apparecchiature e impianti fuori sede
7.11 Infrastrutture di supporto	12.8.1.6 Controllo del materiale in uscita
7.12 Sicurezza dei cablaggi	12.8.2.6 Sicurezza dei supporti
7.13 Manutenzione delle apparecchiature	12.8.3.1 Controllo accesso agli archivi fisici
	12.10.4 Scambi di informazioni
	12.8.2.2 Infrastrutture e CED
	12.8.2.4 Cablaggio
	12.8.2.3 Manutenzione

		degli impianti
7.14 Dismissione sicura o riutilizzo delle apparecchiature		12.8.2.7 Dismissione, riuso e cancellazione delle apparecchiature e dei supporti
8.1 Dispostivi finali degli utenti		12.9.8.2 Regole per i dispositivi 12.9.8.5 COIT e BYOD
8.2 Diritti di accesso privilegiato		12.6.3.4 Gli amministratori di sistema
8.3 Restrizione degli accessi alle informazioni		12.6.3 Autorizzazioni
8.4 Controllo degli accessi al codice sorgente dei programmi		12.9.3.10 Sicurezza degli ambienti
8.5 Autenticazione sicura		12.6.2.2 Sicurezza dell'autenticazione
8.6 Gestione della capacità		12.9.7 Gestione della capacità
8.7 Protezione contro il malware		12.9.4 Malware
8.8 Gestione delle vulnerabilità tecniche		12.13.3 Controllo delle vulnerabilità 12.15.4 Vulnerability assessment
8.9 Gestione delle configurazioni sicure e dell'hardening		12.9.2 Configurazione dei dispositivi e dei sistemi informatici
8.10 Cancellazione delle informazioni		12.9.9 Cancellazione dei dati
8.11 Mascheramento e anonimizzazione dei dati		12.5.1.7 Mascheramento e anonimizzazione
8.12 Prevenzione dalla perdita di dati		12.5.1.6 Data loss prevention
8.13 Backup delle informazioni		12.9.5 Backup
8.14 Ridondanza delle strutture di elaborazione delle informazioni		12.14.3 Obiettivi e strategie di ripristino
8.15 Logging		12.9.6.1 Logging

	12.9.6.2 Protezione dei log
	12.9.6.3 Monitoraggio
8.16 Attività di monitoraggio	12.9.6.3 Monitoraggio
8.17 Sincronizzazione degli orologi	12.9.6.4 Clock
8.18 Uso di programmi di utilità privilegiati	12.6.3.4 Gli amministratori di sistema
8.19 Installazione del software sui sistemi di produzione	12.9.3.8 Installazione in ambiente di produzione
8.20 Sicurezza delle reti	12.11.1 Acquisizione dei sistemi IT
8.21 Sicurezza dei servizi di rete	12.10.3 Sicurezza della rete
8.22 Segregazione delle reti	12.12.1.2 Clausole specifiche per i servizi informatici
8.23 Filtro del web	12.10.2 Segmentazione della rete
8.24 Uso della crittografia	12.10.2.1 Separazione da Internet
8.25 Ciclo di vita dello sviluppo sicuro	12.7 Crittografia
8.26 Requisiti di sicurezza delle applicazioni	12.9.3 Gestione dei cambiamenti
8.27 Principi di architettura e ingegnerizzazione dei sistemi sicuri	12.9.3.1 Richiesta e requisiti
8.28 Codifica sicura	12.9.3.4 Sviluppo e ingegnerizzazione (sicuri)
8.29 Test di sicurezza durante lo sviluppo e per l'accettazione	12.9.3.5 Codifica sicura
8.30 Sviluppo affidato all'esterno	12.9.3.7 Verifiche e test
	12.15.4 Vulnerability assessment
	12.12.5 L'acquisizione di prodotti informatici e lo sviluppo affidato

	all'esterno
8.31 Separazione degli ambienti di sviluppo, test e produzione	12.9.3.10 Sicurezza degli ambienti
8.32 Gestione dei cambiamenti	12.9.3 Gestione dei cambiamenti
8.33 Dati di test	12.9.3.11 Dati di test
8.34 Protezione dei sistemi informativi durante i test di audit	12.15.3.2 La sicurezza durante gli audit

Si conclude dalla pagina precedente

Bibliografia

- [1] ABILab. Linee guida sulla digital forensics nel settore bancario italiano. Roma: ABILab, 2011.
- [2] Agenzia per l’Italia Digitale. Linee guida per la valutazione comparativa prevista dall’art. 68 del D.Lgs. 7 marzo 2005, n. 82 “Codice dell’Amministrazione digitale”. Circolare 6 dicembre 2013 n.63. Allegato alla determinazione commissariale n. 193/2013DIG.
- [3] Agenzia per l’Italia Digitale. Misure minime di sicurezza ICT per le pubbliche amministrazioni. Italia: Agenzia per l’Italia Digitale, 2016.
<http://www.agid.gov.it/>.
- [4] Albers Christopher J., Dorofee Audrey J. OCTAVESM Method Implementation Guide. Version 2.0. USA: Carnegie Mellon University, 2001.
- [5] Anderson Ross J., Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Edition. USA: Wiley, 2008.
- [6] Baldoni Roberto, Montanari Luca. 2015 Italian Cyber Security Report: Un Framework Nazionale per la Cyber Security. Versione 1.0. Italia: Research Center of Cyber Intelligence and Information Security (Sapienza Università di Roma) e Laboratorio Nazionale CINI di Cyber Security (Consorzio Interuniversitario Nazionale per l’Informatica), 2016.
<http://www.cybersecurityframework.it/>.

[7] Banca d'Italia, Eurosistema, Nuove disposizioni di vigilanza prudenziale per le banche. Circolare della Banca d'Italia n. 263 del 27 dicembre 2006. 150 aggiornamento del 2 luglio 2013.

[8] Beatino Francesco, Parata Antonio. Sicurezza Applicativa: Un'introduzione. Presentazione all'Università Sapienza di Roma, 2011.

[9] Bellazzi Giuseppe. La gestione legale delle prove digitali. 2010 <www.slideshare.net/gbellazzi/la-gestione-legale-delle-prove-digitali>.

[10] Biasotti Adalberto. Il nuovo regolamento europeo sulla protezione dei dati. Italia: EPC Editore, 2016.

[11] Bishop Matt. Introduction to Computer Security. USA: Addison-Wesley, 2004.

[12] Block Peter. Flawless Consulting: A Guide to Getting Your Expertise Used. 2nd ed. USA: Pfeiffer, 2000.

[13] Boatti Giorgio, Tavaroli Giuliano. Spie. Milano: Mondadori, 2008.

[14] Briski Kari Ann, Chitale Poonam, Hamilton Valerie, Pratt Allan, Starr Brian, Veroulis Jim, Villard Bruce. Minimizing code defects to improve software quality and lower development costs. USA: IBM Corporation, 2008.

[15] the Business Continuity Institute. Good Practice Guidelines 2018. UK: the Business Continuity Institute, 2018.

[16] Cebula James J., Young Lisa R. A Taxonomy of Operational Cyber Security Risks. USA: Carnegie Mellon University - Software Engineering Institute, 2014. <www.sei.cmu.edu>.

[17] Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI. Information assurance: Situation in Switzerland and internationally. Semi-annual report 2017/II (July – December). Svizzera: MELANI, 2017. <www.melani.admin.ch>.

[18] Cloud Security Alliance. Cloud Controls Matrix and CAIQ v4. S.l.: Cloud Security Alliance, 2021. <cloudsecurityalliance.org>.

[19] Cloud Security Alliance. CSA IoT Security Controls Framework. Version 2. S.l.: Cloud Security Alliance, 2019. <cloudsecurityalliance.org>.

[20] Cloud Security Alliance. CSA Security Guidance for Critical Areas of Focus in Cloud Computing. v4.0. S.l.: Cloud Security Alliance, 2018. <cloudsecurityalliance.org>.

[21] Clusit Community for Security. Intelligenza artificiale e sicurezza: opportunità, rischi e raccomandazioni. S.l.: Clusit, 2021. <<https://iasecurity.clusit.it/>>.

[22] Clusit Community for Security. IoT Security e Compliance: gestire la complessità e i rischi. S.l.: Clusit, 2020. <<https://iotsecurity.clusit.it/>>.

[23] Comando Generale della Guardia di Finanza. Manuale operativo in materia di contrasto all'evasione e alle frodi fiscali. Circolare n. 1 2018 Voll. I - IV. Roma: Comando Generale della Guardia di Finanza - III Reparto Operazioni – Ufficio Tutela Entrate, 2018. <<http://www.gdf.gov.it/documenti-e-pubblicazioni/circolari/circolare-1-2018-manuale-operativo-in-materia-di-contrastoe-allevasione-e-alle-frodi-fisca>>.

[24] Common Methodology for Information Technology Security Evaluation: Evaluation methodology. September 2012, Version 3.1, Revision 4. S.l.: s.n., 2012. <www.commoncriteriaportal.org>.

[25] CyberCrime@IPA. Electronic Evidence Guide. Version 1.0. March 2014. S.l.: Council of Europe. 2014.

[26] De Giovanni Roberto, Riva Emanuele, Linee Guida ACCREDIA: I riferimenti all'accreditamento e alla certificazione nelle richieste di offerta e nei bandi di gara. Roma: Accredia. 2014.

[27] Description of automated risk management packages that NIST/NCSC risk management research laboratory have examined. USA: National Institute of Standards and Technology, 1991.

[28] Dewdney A. K. "Computer Recreations: Of Worms, Viruses and Core

War”. Scientific American 252, marzo 1985: 14-23.

[29] Di Cecco Vittorio Emanuele, Ramacciotti Stefano. “I Common Criteria ed il Centro di Valutazione della Difesa. Lo standard ISO 15408 e le attività di valutazione del Ce.Va. Difesa 1, 2008.

[30] Diffie Whitfield, Hellman Martin E. “New Directions in Cryptography”. IEEE Transactions on Information Theory IT-22, n.6, novembre 1976: 644-654.

[31] “The digital arms trade”. The Economist, 30 marzo 2013.

[32] DoD 5200.28-STD. Department of Defence Standard: Trusted computer system evaluation criteria (TCSEC). USA: s.n., 1985.

[33] DTR - T001-01 Final DFRWS technical report. A Road Map for Digital Forensic Research: Report From the First Digital Forensic Research Workshop (DFRWS), a cura di Gary Palmer. USA: s.n., 2001.

[34] Easttom Chuck. Network Defense and Countermeasures: Principles and Practices. USA: O’ Reilly, 2018.

[35] Emegian Fulvia, Perego Monica. Privacy & Audit. S.l.: Wolters Kluwer, 2019.

[36] European Committee for Electrotechnical Standardization. EN 50600.

Information technology - Data centre facilities and infrastructures. Multi-part standard. Bruxelles: CENELEC.

[37] European Network and Information Security Agency (ENISA). Artificial Intelligence Cybersecurity Challenges. S.l.: ENISA, 2020.
<<https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges>>.

[38] European Network and Information Security Agency (ENISA). Baseline Security Recommendations for IoT. S.l.: ENISA, 2017.
<<https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot>>.

[39] European Network and Information Security Agency (ENISA). Good Practices for Security of IoT - Secure Software Development Lifecycle. S.l.: ENISA, 2019. <<https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1>>.

[40] European Network and Information Security Agency (ENISA). Guidelines for Securing the Internet of Things. S.l.: ENISA, 2020.
<<https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things>>.

[41] European Network and Information Security Agency (ENISA). Handbook on Security of Personal Data Processing. S.l.: ENISA, 2017.

[42] European Network and Information Security Agency (ENISA). Handbook on Security of Personal Data Processing. S.l.: ENISA, 2017.

[43] European Network and Information Security Agency (ENISA). Incentives and barriers of the cyber insurance market in Europe. S.l.: ENISA, 2012. <<https://www.enisa.europa.eu/publications/incentives-and-barriers-of-the-cyber-insurance-market-in-europe>>.

[44] European Network and Information Security Agency (ENISA). Measurement Frameworks and Metrics for Resilient Networks and Services: Technical report. Discussion Draft. S.l.: ENISA, 2010.

[45] Epifani Mattia, Stirparo Pasquale. Learning Ios Forensics. UK: Packt Publishing Ltd, 2015.

[46] ETSI. ETSI TS 103 645 V2.1.2. Cyber Security for Consumer Internet of Things: Baseline Requirements. Francia: ETSI, 2020.

[47] Dinei Florêncio, Cormac Herley. Sex, Lies and Cybercrime Surveys. USA: Microsoft Research, 2011. <<https://www.microsoft.com/en-us/research/publication/sex-lies-and-cyber-crime-surveys/>>.

[48] Gaio Giulio Cesare. De bello gallico. <<https://www.apoftegma.it/de-bello-gallico.asp>>.

[49] Galgano Alberto. Toyota. Milano: Guerini e associati, 2005.

[50] Galgano Alberto. Qualità totale. Milano: Guerini e associati, 2008.

- [51] Gallotti Cesare. Sicurezza delle informazioni: Analisi e gestione del rischio. Milano: Franco Angeli, 2003.
- [52] Gallotti Cesare. Un metodo di Risk Assessment semplice. Presentazione all'ICT Security di Roma, settembre 2009.
- [53] Gallotti Cesare. VERA: Very easy risk assessment. Versione 6. Milano: s.n., 2021. <www.cesaregallotti.it>.
- [54] Gallotti Cesare, Guasconi Fabio. Quaderni Clusit 009: Certificazioni Professionali in Sicurezza Informatica. Versione 2. Milano: Clusit, 2013.
- [55] Ghirardini Andrea, Faggioli Gabriele. Computer forensics. Milano: Apogeo, 2007.
- [56] Giustozzi Corrado. La sindrome di Fort Apache: La sicurezza delle informazioni nella società postindustriale. S.l.: Monti & Ambrosini, 2007.
- [57] Grassi Paul, Newton Elaine, Perlner Ray, Regenscheid Andrew, Fenton James, Burr William, Richer Justin, Lefkovitz Naomi, Danker Jamie, Choong Yee-Yin, Greene Kristen, Theofanos Mary. NIST Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management. USA: National Institute of Standards and Technology, 2017.
- [58] Gruppo di Lavoro UNINFO sulla serie di norme ISO/IEC 27000.

Quaderno Uninfo: La gestione della sicurezza delle informazioni e della privacy nelle PMI. Torino: UNINFO, 2012.

[59] Guasconi Fabio. ISO/IEC 27701, la norma internazionale per certificare la protezione dei dati personali. 2019.

<<https://www.ictsecuritymagazine.com/articoli/iso-iec-27701-la-norma-internazionale-per-certificare-la-protezione-dei-dati-personali/>>.

[60] A guide to the Project Management Body of Knowledge (PMBOK® Guide). Sixth Edition. USA: Project Management Institute, 2017.

[61] Gutmann Peter. “Secure Deletion of Data from Magnetic and Solid-State Memory”. Sixth USENIX Security Symposium Proceedings, San Jose, California, July 22-25, 1996.

[62] Herzog Pete. OSSTMM 3: The Open Source Security Testing Methodology Manual. USA: Institute for Security and Open Methodologies, 2010.

[63] High-Level Expert Group on AI. Ethics Guidelines for Trustworthy Artificial Intelligence. Brussels: European Commission, 2019. <<https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>>.

[64] Holguera Carlos, Müller Bernhard, Schleier Sven, Willemsen Jeroen. OWASP Mobile Security Testing Guide. 1.1.3 Release. S.l.: The OWASP Foundation, 2021 <www.owasp.org>.

[65] Idraulici della privacy. Un piccolo libro sulla privacy, il GDPR e come attuarlo. S.l.: Youcanprint (cartaceo) e StreetLib (ebook), 2020.

[66] IEC/TR 80002-1:2009. Medical device software. Part 1: Guidance on the application of ISO 14971 to medical device software. Svizzera: IEC, 2009.

[67] Information Systems Security Organization. Controlled Access Protection Profile. Versione 1.d. USA: National Security Agency, 1999
<www.commoncriteriaportal.org/files/ppfiles/capp.pdf>.

[68] ISACA. COBIT 5. A Business Framework for the Governance and Management of Enterprise IT. USA: ISACA, 2012.

[69] ISACA Venice Chapter. Vulnerability Assessment e Penetration Test: Linee guida per l'utente di verifiche di terze parti sulla sicurezza ICT. Venezia: ISACA Venice Chapter, 2013.

[70] ISO 9000:2015. Quality management systems: Fundamentals and vocabulary. Svizzera: ISO, 2015.

[71] ISO 14971:2007. Application of risk management to medical devices. Svizzera: ISO, 2007.

[72] UNI EN ISO 19011:2018. Linee guida per audit di sistemi di gestione. Milano: UNI, 2018. Edizione originale con il titolo ISO 19011:2018. Guidelines for auditing management systems (Svizzera: ISO, 2018).

[73] ISO 22300:2018. Societal security - Terminology. Svizzera: ISO, 2018.

[74] ISO 22301:2019. Security and resilience. Business continuity management systems. Requirements. Svizzera: ISO, 2019.

[75] ISO 22313:2020. Security and resilience. Business continuity management systems. Guidance on the use of ISO 22301. Svizzera: ISO, 2020.

[76] ISO 31000:2018. Risk management: Principles and guidelines. Svizzera: ISO, 2018.

[77] ISO 45001:2018. Occupational health and safety management systems - Requirements with guidance for use. Svizzera: ISO, 2018.

[78] ISO/IEC 15408-1:2009. Information technology. Security techniques. Evaluation criteria for IT security. Part 1: Introduction and general model. Switzerland: ISO; Switzerland: IEC, 2009.

[79] ISO/IEC 15408-2:2008. Information technology. Security techniques. Evaluation criteria for IT security. Part 2: Security functional components. Switzerland: ISO; Switzerland: IEC, 2008.

[80] ISO/IEC 15408-3:2008. Information technology. Security techniques. Evaluation criteria for IT security. Part 3: Security assurance components. Switzerland: ISO; Switzerland: IEC, 2008.

- [81] ISO/IEC 20889:2018. Privacy enhancing data de-identification terminology and classification of techniques. Svizzera: ISO; Svizzera: IEC, 2018.
- [82] ISO/IEC 22337. Information technology — Data centre facilities and infrastructures (multi-part standard). Svizzera: ISO.
- [83] ISO/IEC 27000:2018. Information technology. Security techniques. Information security management systems: Overview and vocabulary. Svizzera: ISO; Svizzera: IEC, 2018. <[standards.iso.org/ittf/PubliclyAvailableStandards](https://www.iso.org/ittf/PubliclyAvailableStandards)>.
- [84] ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems: Requirements. Svizzera: ISO; Svizzera: IEC, 2022.
- [85] ISO/IEC 27002:2013. Information technology. Security techniques. Code of practice for information security controls. Svizzera: ISO; Svizzera: IEC, 2013.
- [86] ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection. Information security controls. Switzerland: ISO; Switzerland: IEC, 2022.
- [87] ISO/IEC 27003:2017. Information technology. Security techniques. Information security management systems. Guidance. Svizzera: ISO; Svizzera: IEC, 2017.

- [88] ISO/IEC 27004:2016. Information technology. Security techniques. Monitoring, measurement, analysis and evaluation. Svizzera: ISO; Svizzera: IEC, 2016.
- [89] ISO/IEC 27006:2015. Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems. Svizzera: ISO; Svizzera: IEC, 2015.
- [90] ISO/IEC 27031:2011. Information technology. Security techniques. Guidelines for information and communication technology readiness for business continuity. Svizzera: ISO; Svizzera: IEC, 2011.
- [91] ISO/IEC 27035:2016. Information technology. Security techniques. Information security incident management. Parti 1 e 2. Svizzera: ISO; Svizzera: IEC, 2016.
- [92] ISO/IEC 31000:2018. Risk management. Guidelines. Svizzera: ISO; Svizzera: IEC, 2018.
- [93] ISO/IEC 31010:2019. Risk management: Risk assessment techniques. Svizzera: ISO; Svizzera: IEC, 2019.
- [94] ITIL® Foundation: ITIL 4 Edition. UK: TSO (The Stationery Office), 2019.

[95] ITIL® 4 Create, Deliver and Support. UK: TSO (The Stationery Office), 2020.

[96] Jansen Wayne, Grance Timothy. NIST Special Publication 800-144. Guidelines on Security and Privacy in Public Cloud Computing. USA: National Institute of Standards and Technology, 2011 <csrc.nist.gov>.

[97] Joint Task Force Transformation Initiative. NIST Special Publication 800-53A. Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans. Revision 4. USA: National Institute of Standards and Technology, 2014.

[98] Jørgensen Magne. “Identification of More Risks Can Lead to Increased Over-Optimism of and Over-Confidence in Software Development Effort Estimates”. *Information and Software Technology* 52(5), 2010:506-516.

[99] JTC1/SC 27 Communications Officer. ISO/IEC JTC 1/SC 27 IT Security Techniques: Corporate Presentation. ver 19/June 2016. S.l. ISO/IEC JTC 1/SC 27, 2016.

[100] Bianchi Fabrizio. Kaizen. Milano: Guerini e associati, 2010.

[101] Kaplan Robert S., Norton David P. Balanced scorecard: Tradurre la strategia in azione. Torino: ISEDI, 2000.

[102] Richard Kissel, Andrew Regenscheid, Matthew Scholl, Kevin Stine.

NIST Special Publication 800-88 revision 1. Guidelines for Media Sanitization. USA: National Institute of Standards and Technology, 2014.

[103] Lacey David. Managing Security in Outsourced and Offshored Environments. UK: BSI, 2010.

[104] Libro bianco: Le Prove, i Controlli, le Valutazioni e le Certificazioni per i prodotti, i servizi, le aziende ed i professionisti, a cura del Comitato d'Area PCVC di Confindustria Servizi Innovativi e Tecnologici. Roma: Confindustria Servizi Innovativi e Tecnologici, 2010.

[105] Managing Successful Projects with PRINCE2®. 6th ed., 2017 edition. UK: Stationery Office, 2017.

[106] Manganelli Raymond L., Klein Mark M. The reengineering handbook. USA: Amacom, 1994.

[107] McVittie Fred. The Data Information Knowledge Wisdom Hierarchy. In The Poetics of Thought, 2009 <poeticsofthought.wordpress.com/2009/12/15/the-data-information-knowledge-wisdom-hierarchy>.

[108] Mehari 2010. Francia: Club de la sécurité de l'information français, 2010 <<https://clusif.fr/mehari/>>.

[109] Mell Peter, Grance Timothy. NIST Special Publication 800-145. The NIST Definition of Cloud Computing. USA: National Institute of Standards and

Technology, 2011.

[110] Mitnick Kevin D. L'arte dell'inganno: I consigli dell'hacker più famoso del mondo. Milano: Feltrinelli, 2005.

[111] Naidu Krishni. Web Application Checklist. Versione 1.0. USA: SANS Institute, s.d.

[112] Naone Erica. "Cybercrime Surveys Aren't Telling Us What We Need to Know". MIT Technology Review, 28 giugno 2011
<www.technologyreview.com/s/424492/cybercrime-surveys-arent-telling-us-what-we-need-to-know/>.

[113] National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. USA: NIST, 2018.
<<https://www.nist.gov/cyberframework>>.

[114] Nepi Alberto. Introduzione al project management. Milano: Guerini e associati, 1997.

[115] OWASP Proactive controls for developers. 2016. v 2.0.. S.l.: The OWASP Foundation, 2016. <www.owasp.org>.

[116] OWASP Secure Coding Practices: Quick Reference Guide. Version 2.0. S.l.: The OWASP Foundation, 2010 <www.owasp.org>.

[117] OWASP Top 10:2021. S.l.: The OWASP Foundation, 2021
<<https://owasp.org/Top10/>>.

[118] Oxford Dictionaries. UK: Oxford University Press, s.d.
<www.oxforddictionaries.com>.

[119] PAS 99:2012. Specification of common management system requirements as a framework for integration. UK: The British Standards Institution, 2012.

[120] Paul Mano, Official (ISC)2 Guide to the CSSLP. USA: CRC Press, 2011

[121] Pelino Enrico, Bolognini Luca, Bistolfi Camilla. Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali. Italia: Giuffrè, 2016.

[122] Perego Monica, Ponti Chiara. “Conservazione dei dati: criteri e criticità (nell’incertezza normativa)”. Agenda Digitale, 19 settembre 2019
<<https://www.agendadigitale.eu/sicurezza/privacy/conservazione-dei-dati-criteri-e-criticita-nellincertezza-normativa/>>.

[123] Perri Pierluigi, Ziccardi Giovanni. Tecnologia e Diritto. Italia: Giuffrè, 2019.

[124] Peteanu Razvan. Best Practices for Secure Development. v4.03. S.l.: s.n., 2001.

[125] Progetto di semplificazione del linguaggio: Manuale di stile. Materiale didattico per il corso Tecniche di redazione di atti e testi amministrativi: laboratorio di scrittura, Provincia di Lecce, 2008.

[126] Il progetto per la semplificazione del linguaggio amministrativo, a cura di Fioritto Alfredo. Roma: Istituto poligrafico e Zecca dello Stato, 2002.

[127] Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008. Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema. Modificato in base al provvedimento del 25 giugno 2009.

[128] Qassim Awatif Amin “Why information systems projects fail: Guidelines for Successful Projects”. IntoIT Issue 26, May 2008: 12-17.
<http://www.intosaiitaudit.org/publication_and_resources/1>.

[129] Quinn Stephen, Ivy Nahla, Barrett Matthew, Feldman Larry, Witte Greg, Gardner R. K. NISTIR 8286A: Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management. USA: National Institute of Standards and Technology (NIST), 2021
<<https://csrc.nist.gov/publications/detail/nistir/8286a/final>>.

[130] Ramacciotti Stefano. I requisiti di sicurezza per i moduli crittografici e la validazione degli algoritmi crittografici secondo lo standard FIPS 140-2. Milano: Clusit, 2011.

[131] Rapporto Clusit 2016 sulla sicurezza ICT in Italia. Milano: CLUSIT; Milano: Astrea, 2016 <www.clusit.it>.

[132] Regole e suggerimenti per la redazione dei testi normativi. 2007 <<http://www.consiglio.regione.toscana.it:8085/leggi-e-banche-dati/Oli/Manuale/man-ed-3.asp>>.

[133] Rodriguez Victor A. SPSMM, Secure Programming Standards Methodology Manual. v0.5.1. USA: Institute for Security and Open Methodologies, 2002.

[134] ROSI Return on Security Investments: un approccio pratico. Come ottenere Commitment sulla Security. Versione 2.0. S.l.: s.n., 2011. <rosi.clusit.it>.

[135] Sandhu Ravi S., Coynek Edward J., Feinstein Hal L., Youmank Charles E. “Role-Based Access Control Models”. IEEE Computer 29, n. 2, February 1996: 38-47.

[136] Schneier Bruce. Applied cryptography. 2nd Edition. USA: Wiley, 1996.

[137] Schwaber Ken, Sutherland Jeff. The Scrum Guide™. The Definitive Guide to Scrum: The Rules of the Game. November 2017. <www.scrumguides.org/>.

[138] Singh Simon. Codici & segreti. Milano: Rizzoli, 1999.

[139] Souppaya Murugiah, Scarfone Karen. NIST Special Publication 800-46 revision 2. Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. USA: National Institute of Standards and Technology, 2016.

[140] Spanos Nicholas. 100 IT Performance Metrics. S.l.: Computer Aid Inc., s.d.

[141] Stallings William. Cryptography and network security. USA: Prentice Hall, 1999.

[142] Stoneburner Gary, Hayden Clark, Feringa Alexis. NIST Special Publication 800-27. Engineering Principles for Information Technology Security (A Baseline for Achieving Security). Rev A. USA: National Institute of Standards and Technology, 2004.

[143] Stouffer Keith, Pillitteri Victoria, Lightman Suzanne, Abrams Marshall, Hahn Adam. NIST Special Publication 800-82. Guide to Industrial Control Systems (ICS) Security. Revision 2. USA: National Institute of Standards and Technology, 2015.

[144] Swanson Marianne, Bowen Pauline, Phillips Amy Wohl, Gallup Dean, Lynes David. NIST Special Publication 800-34. Contingency Planning Guide for Federal Information Systems. Rev. 1. USA: National Institute of Standards and Technology, 2010.

[145] Tavaglini Marco, Ravarini Aurelio, Sciuto Donatella. Sistemi per la gestione dell'informazione. Milano: Apogeo, 2003.

[146] Tech & Law Center. Security of the digital natives. S.l.: Tech And Law Center, 2014 <www.techandlaw.net>.

[147] Tieghi Enzo M. Quaderni Clusit 007: Introduzione alla protezione di reti e sistemi di controllo e automazione (DCS, SCADA, PLC, ecc.). Maggio 2007. Milano: Clusit, 2007.

[148] Timberg Craig. Net of insecurity: A flaw in the design. The Internet's founders saw its promise but didn't foresee users attacking one another. USA, 2015. <www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/>.

[149] UNI - Ente Nazionale Italiano di Unificazione. UNI 11697:2017: Attività professionali non regolamentate - Profili professionali relativi al trattamento e alla protezione dei dati personali - Requisiti di conoscenza, abilità e competenza. Milano: UNI, 2017.

[150] UNI - Ente Nazionale Italiano di Unificazione. Le regole del gioco. Milano: UNI, 2012.

[151] Uptime Institute. Tier Standard: Topology. USA: Uptime Institute LLC, 2012.

[152] U.S. Department of Commerce, National Bureau of Standards. FIPS PUB 73. Guidelines for security of computer applications. USA: U.S. Department of Commerce, 1980.

[153] Ustaran Eduardo. European Data Protection. USA: the International Association of Privacy Professionals (IAPP), 2018. <<https://iapp.org/>>.

[154] Valle Antonio. The Fractal Nature of PDCA cycle. 2011 <www.gobiernotic.es/2011/05/fractal-nature-of-pdca-cycle.html>.

[155] Van Eck Wim. “Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?”. North-Holland Computers & Security, numero 4, 1985: 269-286.

[156] Varanini Francesco. Contro il management. Milano: Guerini e Associati, 2010.

[157] Verizon RISK Team. 2016 Data Breach Investigations Report. USA: Verizon, 2016.

[158] Womack James P., Jones Daniel T. Lean thinking. Milano: Guerini e associati, 1997.

[159] Woods Daniel W., Moore Tyler. “Does insurance have a future in governing cybersecurity?”. IEEE Security & Privacy, vol. 18, no. 1, pp. 21-27, Jan.-Feb. 2020. doi: 10.1109/MSEC.2019.2935702.

[160] Wright Peter. Cacciatore di spie. Milano: Rizzoli, 1988.

[161] Bayse Gail Zemanek. A Security Checklist for Web Application Design. USA: SANS Institute, 2004.

[162] Zhou Changying, Ramacciotti Stefano. “Common Criteria: Its Limitations and Advice on Improvement”. ISSA Journal, aprile 2011.

[163] Ziccardi Giovanni. Crittografia e diritto. Torino: G. Giappichelli Editore, 2003.

[164] Ziccardi Giovanni. Informatica giuridica. Milano: Giuffrè Editore, 2008.

[165] Zwicky Elizabeth D., Cooper Simon, Chapman D. Brent. Building Internet firewalls. USA: O’ Reilly, 2000.

You talk too much.

Dal film Westworld