UNIONE EUROPEA

MINISTERO DEL LAVORO E DELLE POLITICHE SOCIALI
Ufficio Centrale per l'Orientamento e la Formazione Professionale dei Lavoratori

Regione Puglia

POR Puglia 2000-2006
Misura 6.4: "Risorse umane e società dell'informazione" Azione a) Formazione specifica per la P.A,
Progetto approvato con D.D. n. 172 del 28/12/06 – POR Puglia 2000-2006
Complemento di Programmazione, Avviso pubblico n. 11/2006 per la presentazione di progetti per attività cofinanziate dal FSE, dallo Stato e dalla Regione Puglia

DISPENSA

LA SICUREZZA NELLE RETI INFORMATICHE

Aspetti Organizzativi, Tutela Civile e Penale, Sistemi e Soluzioni Tecniche

Associazione Temporanea di Scopo As. UNISCO Network per lo sviluppo locale e Studiodelta srl

Studiodelta.it formazione e tecnologie informatiche

UNISCO a.p.s. Network per lo sviluppo locale

INDICE GENERALE

Sicurezza Informatica e Crittografia 1

1 Minacce alla sicurezza, attacchi e vulnerabilità 1

1.1 Introduzione 1
1.2 Calamità naturali 2
1.3 Minacce umane 2

2 Metodi, strumenti e tecniche per gli attacchi 7

2.1 Attacchi = motivo + metodo + vulnerabilità 7

3 Vulnerabilità nella sicurezza 9

3.1 Password 9
3.2 Progettazione del protocollo. 9

4 Aggressori esterni o "cracker" 13

4.1 Dipendenti non malintenzionati 14
4.2 Eliminazione e alterazione delle informazioni 15
4.3 Furto di informazioni o frode 15
4.4 Metodi, strumenti e tecniche per gli attacchi 16
4.5 Intrusioni tramite posta elettronica 16
4.6 Social engineering 16
4.7 Attacchi intrusivi 17
4.8 Attacchi di negazione di servizio 18
4.9 Consumo di risorse del server 19
4.10 Saturazione delle risorse della rete 20
4.11 Saturazione con posta 22

5 Attacchi con virus 23

5.1 Breve cronistoria 23
5.2 Funzionamento dei virus 24
5.3 Trojan horse 27
5.4 Worm 28

6 Analisi degli Attacchi 29

6.1 Social Engineering 30
6.2 Acquisizione di informazioni 30
6.3 Sfruttamento di relazioni di fiducia mal gestite 31
6.4 Sfruttamento di servizi non autenticati 32
6.5 Spoofing 34
6.6 Sfruttamento di bugs nel software 35
6.7 Denial of Service 36

7 Aspetti Legali 36

7.1 PRINCIPALI ARTICOLI DI LEGGE SUGLI ATTACCHI INFORMATICI 36
8 Dlgs 196/03 e DPS 40
8.1 QUADRO GENERALE 43
8.2 LE *MISURE IDONEE* DI SICUREZZA 46
8.2.1 La natura dei dati e le caratteristiche del trattamento 47
8.2.2 La classificazione delle misure di sicurezza 47
8.2.3 L'aggiornamento delle misure di sicurezza 49
8.2.4 Il risarcimento per danni 49
8.2.4.1 I danni patrimoniali 50
8.2.4.2 Il danno non patrimoniale 51
8.2.5 Le regole per i fornitori di servizi di comunicazione elettronica 52
8.3 LE MISURE MINIME DI SICUREZZA 54
8.3.1 L'aggiornamento delle misure minime 55
8.3.2 Le sanzioni penali per la omessa adozione delle *misure minime* ... 56
8.3.2.1 L'evoluzione delle sanzioni 57
8.3.2.2 Il ravvedimento operoso 57
8.3.2.3 I soggetti interessati 58
9 Definizione di compiti, ruoli e procedure 60
9.1 IL TITOLARE DEL TRATTAMENTO 61
9.2 IL RESPONSABILE DEL TRATTAMENTO 63
9.2.1 Chi nominare responsabile 65
9.2.2 Il responsabile per la sicurezza 65
9.2.3 L'amministratore di sistema 66
9.3 L'INCARICATO DEL TRATTAMENTO 67
9.3.1 Chi può essere incaricato 69
9.3.2 Le prescrizioni in termini di sicurezza 70
9.3.3 Il preposto alla custodia delle parole chiave 70
9.3.4 Il soggetto incaricato della manutenzione del sistema 71
9.3.5 Il custode dell'archivio ad accesso controllato 71
9.4 LA PREDISPOSIZIONE E L'AGGIORNAMENTO DEL MANSIONARIO PRIVACY 72
10 Le coordinate per definire le misure minime di sicurezza 75
10.1 LA NATURA DEI DATI TRATTATI 75
10.1.1 Le procedure per la classificazione dei dati 76
10.2 GLI STRUMENTI UTILIZZATI PER IL TRATTAMENTO 76
10.2.1 L'evoluzione per i trattamenti effettuati con mezzi elettronici 76
10.3 L'ELENCO DEI TRATTAMENTI DI DATI PERSONALI 78
10.3.1 La banca dati dei sistemi informativi 80
11 L'analisi dei rischi 81
11.1 VALUTAZIONE DELLE MINACCE 82
11.2 L'IMPATTO DEGLI EVENTI NEGATIVI 85
11.3 LA GESTIONE DEI RISCHIO 86
12 I trattamenti senza l'ausilio di strumenti elettronici 88

12.1 L'AFFIDAMENTO AGLI INCARICATI E LA CUSTODIA DI ATTI E DOCUMENTI 90
12.2 L'ARCHIVIAZIONE DI ATTI E DOCUMENTI 91
12.3 I SUPPORTI NON INFORMATICI 92

13 I trattamenti con strumenti elettronici 92

13.1 ADOZIONE DI UN SISTEMA DI AUTENTICAZIONE INFORMATICA 93
13.2 ADOZIONE DI UN SISTEMA DI AUTORIZZAZIONE 101
13.3 MISURE DI PROTEZIONE E PER IL RIPRISTINO DEI DATI 104
13.3.1 La protezione di strumenti e dati 105
13.3.1.1 Virus e programmi analoghi: approfondimenti 107
13.3.1.2 Il controllo sullo stato della sicurezza 110
13.3.2 Le procedure per il ripristino dei dati 112
13.3.2.1 Dal salvataggio dei dati al piano di continuità operativa 112
13.4 CUSTODIA ED USO DEI SUPPORTI RIMOVIBILI 115
13.5 IL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA 117
13.5.1 La protezione di aree e locali 118
13.5.2 Gli interventi formativi degli incaricati 119
13.5.2.1 L'introduzione e diffusione della cultura della sicurezza 119
13.5.3 La sicurezza nella trasmissione dei dati 121
13.6 ULTERIORI PRESCRIZIONI PER GLI ORGANISMI SANITARI 122
13.7 IL CERTIFICATO DI CONFORMITÀ 124

14 I dati personali affidati dal titolare all'esterno 124

14.1 I POSSIBILI CRITERI 125
14.2 LE CLAUSOLE CONTRATTUALI 126

15 Il documento programmatico sulla sicurezza: come redigerlo 128

15.1 LA DUPLICE NATURA DEL DOCUMENTO PROGRAMMATICO 135
15.2 L'APPROVAZIONE DEL DOCUMENTO 135
15.3 DOCUMENTO PROGRAMMATICO SULLA SICUREZZA 136
15.3.1 Elenco dei trattamenti di dati personali 137
15.3.2 Caratteristiche delle aree, dei locali, degli strumenti con cui si effettuano i trattamenti 137
15.3.3 Analisi dei rischi che incombono sui dati 138
15.3.4 Misure da adottare per garantire l'integrità e la disponibilità dei dati 140
15.3.5 Criteri e modalità di ripristino dei dati, in seguito a distruzione o danneggiamento 141
15.3.6 Analisi del mansionario privacy e degli interventi formativi degli incaricati 141
15.3.7 L'affidamento di dati personali all'esterno 142
15.3.8 Controllo generale periodico sullo stato della sicurezza 142

16 La mappa delle misure minime di sicurezza 143

16.1 L'EVOLUZIONE DELLA MAPPA DELLE MISURE MINIME DI SICUREZZA 143
16.2 IL RAPPORTO TRA LE DIVERSE *CLASSI DI SICUREZZA* 147

17 Il periodo transitorio 149

17.1 Il differimento del termine generale 149
17.2 Il particolare differimento a Marzo 2005 150
17.2.1 Entro il 31 dicembre 2004: redazione del documento avente data certa 151
17.2.2 Il rapporto con il Documento programmatico sulla sicurezza 152

18 Pianificazione della sicurezza Proattiva 153

18.1 Introduzione 153
18.2 Sviluppo di controlli e criteri di protezione 154
18.3 Tipi di criteri di protezione 156
18.4 Criteri per le password 156
18.5 Responsabilità amministrative 157
18.6 Responsabilità degli utenti 157
18.7 Criteri per la posta elettronica 158
18.8 Criteri per Internet 159
18.9 Criteri per il backup e il ripristino 159
18.10 Archiviazione dei backup in sede e fuori sede 160

19 Risposta agli incidenti 161

19.1 Case study 164

20 Sistemi Crittografici 168

20.1 Accesso protetto, dati protetti e codice protetto 168
20.2 Infrastrutture a chiave pubblica 170
20.3 Firme digitali 171
20.4 Secure Sockets Layer (SSL) 172
20.5 Protezione della posta elettronica 172
20.6 Crittografia del file system 173
20.7 Autenticazione 174
20.8 Autenticazione Kerberos 175
20.9 Autenticazione NTLM 176
20.10 Smart card 176
20.11 Protezione del codice 177
20.12 Tecnologie per proteggere la connettività della rete 177
20.13 Firewall 178
20.14 Strumenti per rilevare le intrusioni 179
20.15 Antivirus 180
20.16 Controllo 181
20.17 Eventi da controllare 182

Bibliografia 183

Sicurezza Informatica e Crittografia

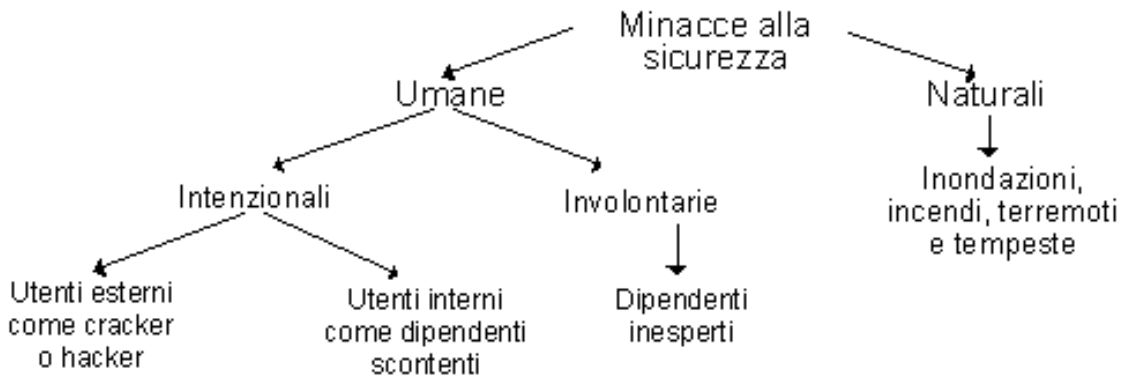
1 Minacce alla sicurezza, attacchi e vulnerabilità

1.1 Introduzione

Le informazioni costituiscono la risorsa più importante nella maggior parte delle organizzazioni. Le società in grado di gestire le informazioni in modo ottimale accrescono la propria competitività. La minaccia proviene da coloro che desiderano acquisire le informazioni o limitare le opportunità di lavoro interferendo nei normali processi aziendali.

Scopo di una corretta strategia di sicurezza è proteggere le informazioni importanti e riservate dell'organizzazione, rendendole contemporaneamente disponibili senza difficoltà. Gli aggressori che tentano di danneggiare un sistema o di ostacolare lo svolgimento delle normali attività aziendali approfittano delle vulnerabilità con tecniche, metodi e strumenti differenti. Per sviluppare misure e criteri che consentano di proteggere le risorse e renderle meno vulnerabili, gli amministratori del sistema devono comprendere i diversi aspetti relativi alla sicurezza.

prova
Gli aggressori hanno generalmente delle ragioni o degli obiettivi, ad esempio ostacolare le normali attività dell'azienda o sottrarre informazioni. Per raggiungere questi scopi, utilizzano tecniche, metodi e strumenti differenti che sfruttano vulnerabilità presenti nel sistema, nei controlli o nei criteri di sicurezza.
Obiettivo + Metodo + Vulnerabilità = Attacco
Questi aspetti verranno descritti in maggiore dettaglio più avanti in questa stessa sezione.



La Figura 1 introduce uno schema utilizzabile per scongiurare minacce alla sicurezza in aree differenti.

1.2 Calamità naturali

Nessuno può impedire il verificarsi di calamità naturali. Terremoti, tempeste, inondazioni, fulmini e incendi possono causare danni gravi ai computer, che possono risultare in perdita di informazioni, tempi di inattività o perdite di produttività. I danni all'hardware possono inoltre danneggiare altri servizi essenziali. Le difese che è possibile predisporre contro le calamità naturali non sono molte. L'approccio migliore consiste nel preparare in anticipo dei piani di ripristino e di emergenza. In questa categoria rientrano anche minacce quali sommosse, guerre e attacchi terroristici. Anche se hanno origine umana, sono classificate come calamità.

1.3 Minacce umane

Le minacce intenzionali comprendono attacchi interni effettuati da dipendenti scontenti o malintenzionati e attacchi esterni da parte di utenti non dipendenti allo scopo di creare problemi o danneggiare un'organizzazione.
Gli aggressori più pericolosi sono in genere gli utenti interni o gli ex dipendenti perché conoscono molti dei codici e delle misure di sicurezza utilizzate. Gli utenti interni hanno probabilmente obiettivi specifici e sono autorizzati ad accedere al sistema. I dipendenti sono gli utenti che conoscono meglio i computer e le applicazioni dell'organizzazione e le operazioni da compiere per causare i danni più gravi. Gli utenti interni possono collocare virus, trojan horse o worm e spostarsi all'interno del file system.

L'attacco dall'interno può interessare tutti i componenti di sicurezza del computer. Essendo autorizzati a spostarsi all'interno del sistema, gli utenti interni possono infatti individuare e divulgare informazioni riservate. I trojan horse rappresentano una minaccia sia per l'integrità che per la riservatezza delle informazioni. Gli attacchi dall'interno possono interessare la

disponibilità, sovraccaricando la capacità di archiviazione o di elaborazione del sistema o causando il blocco del sistema.
Questi individui vengono spesso chiamati "cracker" o "hacker". La definizione di "hacker" è cambiata nel corso degli anni. Inizialmente "hacker" era chi si impegnava per ottenere il massimo possibile dal sistema che utilizzava, utilizzando tutte le parti di un sistema e studiandole fino a diventare esperto in tutti i dettagli. Queste persone rappresentavano una fonte di informazioni per gli altri utenti di computer e venivano considerati quasi dei "guru" o "maghi".

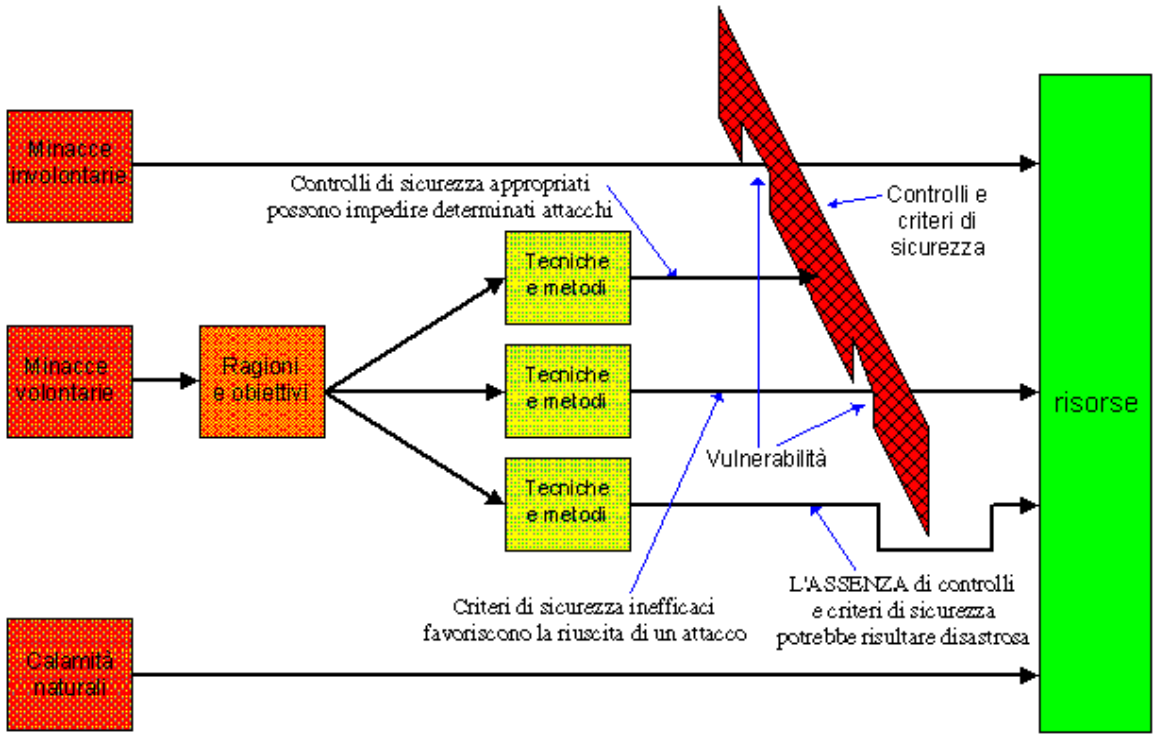
Ora, tuttavia, il termine "hacker" indica persone che penetrano con la forza nei sistemi o oltrepassano intenzionalmente e senza permesso i confini loro assegnati in un sistema.

Il termine corretto da utilizzare per indicare coloro che si introducono nei sistemi senza autorizzazione è "cracker". I metodi più utilizzati per riuscire ad accedere a un sistema comprendono l'identificazione delle password, che sfrutta le vulnerabilità nella sicurezza note, lo "spoofing" della rete e il "social engineering".
Gli aggressori intenzionali hanno in genere un obiettivo o una ragione specifica per attaccare un sistema. Lo scopo potrebbe essere quello di interrompere i servizi e le attività aziendali utilizzando strumenti di attacco volti alla negazione di servizio (DoS, Denial of Service). Potrebbero anche sottrarre informazioni o persino hardware, ad esempio dei portatili. Gli hacker possono quindi vendere informazioni utili ai concorrenti.
Nel 1996 fu rubato da un dipendente di Visa International un portatile contenente 314.000 account di carte di credito. Per annullare i numeri e sostituire le carte, Visa spese una cifra pari a circa 13 miliardi di lire.

Un'organizzazione può essere danneggiata non soltanto tramite attacchi dolosi. La minaccia principale all'integrità dei dati proviene da utenti autorizzati che non si rendono conto delle operazioni che effettuano. Errori e omissioni possono causare la perdita, il danneggiamento o l'alterazione di dati importanti. Le minacce involontarie provengono in genere da dipendenti non esperti di computer e non consapevoli delle vulnerabilità e delle minacce alla sicurezza. Gli utenti che aprono, modificano e salvano i documenti di Microsoft® Word utilizzando Blocco note causano ad esempio danni gravi alle informazioni che vi sono contenute.

Gli utenti, gli addetti all'immissione dei dati, gli operatori di sistema e i programmatori commettono frequentemente errori involontari che contribuiscono ad aggravare, direttamente o indirettamente, i problemi relativi alla sicurezza. Una minaccia può ad esempio essere costituita da un errore di immissione dati o di programmazione, che può causare l'arresto anomalo del sistema. In altri casi, gli errori creano vulnerabilità. Si possono verificare errori durante tutte le fasi del ciclo di vita del sistema.

La Figura descrive un modello teorico su cui è possibile basarsi per determinare le minacce, gli obiettivi, i metodi e le vulnerabilità differenti utilizzate in un attacco.



La tabella seguente fornisce alcuni esempi dei vari aspetti illustrati in precedenza.

Minacce	**Ragioni / Obiettivi**	**Metodi**	**Criteri di sicurezza**
• Dipendenti • Malintenzionati • Inesperti • Non dipendenti • Aggressori esterni • Calamità naturali • Inondazioni • Terremoti • Tempeste • Sommosse e guerre	• Negare i servizi • Sottrarre informazioni • Alterare le informazioni • Danneggiare le informazioni • Eliminare le informazioni • Fare uno scherzo • Mettersi in mostra	• Social engineering • Virus, trojan horse e worm • Riproduzione dei pacchetti • Modifica dei pacchetti • Spoofing degli indirizzi IP • Saturazione con posta • Vari strumenti propri degli hacker • Identificazione delle password	• Vulnerabilità • Risorse • Informazioni e dati • Produttività • Hardware • Personale

Si tenga presente che i dipendenti inesperti non hanno generalmente ragioni o scopi per causare danni. Il danno è accidentale. Inoltre, gli aggressori malintenzionati possono ingannare tali dipendenti utilizzando il "social engineering" per ottenere l'accesso. L'aggressore potrebbe fingersi un amministratore e richiedere nomi utente e password. I dipendenti che non sono stati preparati e che non sono consapevoli dei problemi relativi alla sicurezza possono non riconoscere l'inganno e fornire le informazioni richieste.

La sicurezza fisica e l'integrità e riservatezza dei dati sono strettamente collegate. Infatti, l'obiettivo di alcuni attacchi non è la distruzione fisica del sistema, ma l'intrusione e la rimozione o la copia di informazioni importanti. Gli aggressori agiscono per soddisfazione personale o per avere una ricompensa.
Di seguito sono riportati alcuni dei metodi utilizzati dagli aggressori:

- Eliminazione e alterazione di informazioni. Gli attacchi dolosi sono in genere provocati da utenti che eliminano o alterano le informazioni per dimostrare qualcosa o per vendicarsi di un torto subito. Gli attacchi interni sono causati da utenti generalmente spinti da rancore nei confronti dell'organizzazione perché sono scontenti di qualcosa. Gli aggressori esterni, invece, possono introdursi in un sistema solo per il gusto di farlo o perché desiderano dimostrare la propria abilità.
- Furto di informazioni o frode. Le tecnologie informatiche vengono utilizzate sempre più frequentemente per commettere frodi e furti. I sistemi di computer possono essere violati in molti modi, sia con versioni automatizzate dei metodi tradizionali di frode che con metodi nuovi. I sistemi finanziari non sono i soli a essere oggetto di frodi. Altri obiettivi sono i sistemi che controllano l'accesso a qualsiasi risorsa, ad esempio i sistemi per il controllo delle presenze e degli orari, per la gestione del magazzino, per la valutazione scolastica o per le chiamate interurbane.
- Interruzione delle normali attività aziendali. È possibile che gli attacchi mirino a interrompere le normali attività aziendali. In circostanze come queste, l'aggressore ha un obiettivo specifico da raggiungere. Gli aggressori utilizzano vari metodi per sferrare attacchi di negazione di servizio, descritti nella sezione dedicata ai metodi, agli strumenti e alle tecniche per gli attacchi.

2 Metodi, strumenti e tecniche per gli attacchi

2.1 Attacchi = motivo + metodo + vulnerabilità

Il metodo in questa formula sfrutta la vulnerabilità dell'organizzazione per sferrare un attacco come mostrato nella Figura 2. Gli aggressori intenzionali possono ottenere l'accesso o negare i servizi utilizzando alcune delle strategie elencate di seguito:

- **Virus**. Gli aggressori possono creare codice nocivo denominato virus. Utilizzando tecniche di intrusione, possono penetrare nei sistemi e collocare dei virus. I virus rappresentano generalmente una minaccia per qualsiasi ambiente. Si presentano in forme differenti e anche quando non sono dannosi sono sempre costosi in termini di tempo. Si possono diffondere anche tramite posta elettronica e dischetti.
- **Trojan horse** (cavalli di troia). Si tratta di codice o di un programma dannoso nascosto all'interno di ciò che sembra un programma normale. Quando un utente avvia il programma normale, viene eseguito anche il codice nascosto. Può causare l'eliminazione di file e altri danni. I trojan horse si diffondono in genere tramite gli allegati di posta elettronica. Il virus Melissa, che ha provocato attacchi di negazione di servizio in tutto il mondo nel 1999, è un tipo di trojan horse.
- **Worm**. Sono programmi che vengono eseguiti indipendentemente e che si spostano da un computer all'altro attraverso le connessioni di rete. Alcune parti di worm possono essere in esecuzione su computer differenti. Anche se non modificano altri programmi, possono diffondere codice con questo scopo.
- **Identificazione delle password** (Password cracking). È una tecnica utilizzata dagli aggressori per accedere di nascosto al sistema tramite l'account di un altro utente. Ciò si può verificare perché gli utenti selezionano spesso password facilmente determinabili. Le password non sono efficaci se possono essere indovinate facilmente basandosi sulla conoscenza dell'utente, ad esempio il cognome da nubile della moglie, e se possono essere individuate tramite dizionario (esistono appositi software che utilizzano un dizionario di parole per cercare di indovinare la password di un utente).
- **Attacchi di negazione di servizio** (Denial of service attacks). Questo tipo di attacco sfrutta l'esigenza di rendere sempre disponibile un servizio ed è sempre più diffuso su Internet, perché i siti Web sono in genere porte aperte pronte a essere violate. Gli utenti possono facilmente saturare di comunicazioni il server Web per tenerlo occupato. Le società connesse a Internet devono quindi prepararsi ad

attacchi DoS. Tali attacchi sono difficili da analizzare e permettono di essere assoggettati ad altri tipi di attacchi.

- **Intrusioni tramite posta elettronica** (email hacking). La posta elettronica è una delle funzionalità di Internet più diffuse. Accedendo alla posta elettronica Internet è possibile comunicare con milioni di utenti in tutto il mondo. Di seguito sono elencate alcune delle minacce associate alla posta elettronica:
- **Assunzione di identità fittizia**. L'indirizzo del mittente della posta elettronica Internet non può essere considerato attendibile perché è possibile che venga utilizzato un indirizzo mittente falso. L'intestazione potrebbe essere stata modificata durante il percorso o il mittente potrebbe essersi connesso direttamente alla porta SMTP (Simple Mail Transfer Protocol) sul computer di destinazione per immettere la posta.
- **Trafugamento di informazioni** (Eavesdropping). Se non viene utilizzata alcuna crittografia, le intestazioni e il contenuto della posta elettronica vengono trasmesse in chiaro. Il contenuto di un messaggio può quindi essere letto o alterato durante il percorso. L'intestazione può essere modificata per nascondere o cambiare il mittente o per reindirizzare il messaggio.
- **Riproduzione dei pacchetti** (Packet replay). Significa la registrazione e la ritrasmissione dei pacchetti dei messaggi sulla rete. La riproduzione dei pacchetti rappresenta una minaccia significativa per i programmi che richiedono sequenze di autenticazione, perché un intruso potrebbe riprodurre i messaggi di sequenze di autenticazione legittime per ottenere l'accesso a un sistema. La riproduzione dei pacchetti, in genere, non è rilevabile, ma può essere impedita utilizzando indicazioni dell'orario sui pacchetti (timestamp) e numerando la sequenza di pacchetti.
- **Modifica dei pacchetti** (Packet modification. Si riferisce a un sistema che intercetta e modifica un pacchetto destinato a un altro sistema, per modificare o distruggere le informazioni contenute nel pacchetto.
- **Social engineering**. È una forma di intrusione comune. Può essere utilizzata da utenti esterni o interni all'organizzazione. Il termine "social engineering" indica il tentativo degli hacker di indurre gli utenti a rivelare le password o altri tipi di informazioni di sicurezza.
- **Attacchi intrusivi** (intrusion attack). Per ottenere l'accesso ai sistemin, un hacker utilizza vari strumenti di intrusione, quali strumenti per l'identificazione delle password a strumenti per la manipolazione e l'intrusione nei protocolli. Gli strumenti per il rilevamento delle intrusioni consentono spesso di rilevare modifiche e variazioni che si verificano all'interno dei sistemi e delle reti.
- **Spoofing della rete**. Un sistema si presenta alla rete come se fosse un altro (il computer A assume l'identità del computer B inviando l'indirizzo di B invece del proprio). Questo perché i sistemi tendono a funzionare all'interno di gruppi composti da altri sistemi trusted. La relazione di trust viene comunicata in modo biunivoco. Il computer A considera trusted il computer B (questo non implica che il sistema B consideri trusted il sistema A). Tale trust implica anche che

l'amministratore del sistema trusted effettui le operazioni in modo corretto e mantenga un livello di protezione appropriato per il sistema. Lo spoofing della rete si realizza nel modo seguente: se il computer A concede il trust al computer B e il computer C assume l'identità del computer B, il computer C può ottenere l'accesso altrimenti negato al computer A.

3 Vulnerabilità nella sicurezza

3.1 Password

Come descritto in precedenza, un utente malintenzionato utilizza un metodo per approfittare delle vulnerabilità e raggiungere un obiettivo. Le vulnerabilità sono punti deboli o brecce nella sicurezza che un aggressore può sfruttare per avere accesso alla rete e alle relative risorse. Per vulnerabilità non si intende un attacco, ma un punto debole di cui si approfitta. Alcuni punti deboli sono:

La selezione della password costituirà un punto controverso finché gli utenti dovranno sceglierne una. Il problema consiste in genere nel ricordare la password corretta tra le molte che devono essere utilizzate. Gli utenti finiscono per scegliere le password più comuni perché sono facili da ricordare. In genere vengono utilizzate le date di compleanno o i nomi dei propri cari. Questo crea una vulnerabilità perché gli estranei hanno ottime possibilità di indovinare la password corretta.

3.2 Progettazione del protocollo.

I protocolli di comunicazione hanno a volte dei punti deboli, che possono essere utilizzati per ottenere informazioni e possibilmente accedere ai sistemi. Alcuni problemi noti sono:

- TCP/IP. Lo stack del protocollo TCP/IP ha alcuni punti deboli che consentono:
- Spoofing degli indirizzi IP
- Attacchi di richiesta di connessione TCP (SYN)
- **Protocollo Telnet**. Telnet può essere utilizzato per amministrare i sistemi che eseguono Microsoft® Windows® 2000 e Unix. Quando si usa il client telnet per connettersi da un sistema Microsoft a un sistema UNIX e viceversa, i nomi utente e le password vengono trasmesse senza crittografia.
- **FTP** (File Transfer Protocol). Come per Telnet, se il servizio FTP è in esecuzione e gli utenti devono inviare o recuperare le informazioni da

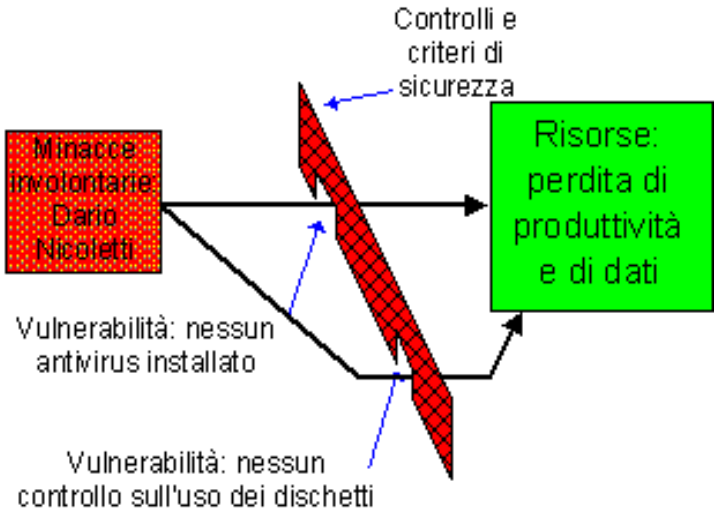
una posizione protetta, i nomi utente e le password vengono trasmesse senza crittografia.

- **Comandi che rivelano informazioni sull'utente**. Non è insolito riscontrare interoperabilità tra prodotti Microsoft e varie versioni di UNIX. I comandi che rivelano informazioni sugli utenti e sul sistema rappresentano una minaccia perché i cracker possono utilizzare tali informazioni per introdursi nel sistema. Eccone alcuni:
- **Finger**. L'utilità client finger su Microsoft Windows NT® e Windows 2000 può essere utilizzata per connettersi a un servizio daemon finger in esecuzione su un computer basato su UNIX per visualizzare informazioni relative agli utenti. Quando il programma finger viene eseguito senza argomenti, vengono visualizzate informazioni su tutti gli utenti correntemente registrati nel sistema.
- **Rexec**. L'utilità rexec è disponibile come client su Microsoft Windows NT e Windows 2000. L'utilità client rexec consente l'esecuzione remota sui sistemi basati su UNIX che eseguono il servizio rexecd. Un client trasmette un messaggio specificando il nome utente, la password e il nome del comando da eseguire. Il programma rexecd è soggetto ad abusi perché può essere utilizzato per sondare un sistema allo scopo di individuare i nomi di account validi. Inoltre, le password vengono trasmesse sulla rete senza crittografia.
- **ATM** (Asynchronous Transfer Mode). La sicurezza può venire compromessa da ciò che viene chiamata "manipolazione delle bocche di accesso", ovvero dall'accesso diretto ai collegamenti e ai cavi della rete presenti nelle aree di parcheggio sotterranee e nei vani di corsa degli ascensori.
- **Frame Relay**. Simile al problema dell'ATM.
- **Amministrazione delle periferiche**. Gli switch e i router sono facilmente gestibili tramite un'interfaccia HTTP o un'interfaccia della riga di comando. Se vengono utilizzate anche password deboli, ad esempio password pubbliche, chiunque sia dotato di conoscenze tecniche di base potrà assumere il controllo delle periferiche.
- **Modem**. I modem sono ormai diventate delle funzionalità standard su molti computer. Qualsiasi modem non autorizzato rappresenta un problema serio per la sicurezza. Gli utenti non li usano infatti solo per accedere a Internet, ma anche per connettersi al proprio ufficio quando lavorano da casa. Il problema è causato dal fatto che utilizzando un modem si aggira il "firewall" che protegge la rete dalle intrusioni esterne. Un hacker che utilizza un "war dialer" per identificare il numero di telefono del modem e un "password cracker" per determinare una password debole, può quindi avere accesso al sistema. A causa della natura delle reti di computer, un hacker che riesce ad accedere a un singolo computer è spesso in grado di connettersi a tutti gli altri computer della rete.

Per illustrare la teoria su cui si basano gli attacchi, sono disponibili i seguenti esempi tratti dalla vita reale.

❶ Esempio : **minaccia involontaria** (dipendenti inesperti).

Un dipendente, qui definito Dario Nicoletti, copia giochi e altri eseguibili da un dischetto da 1,44 MB sul proprio disco rigido locale e li esegue. Sfortunatamente, i giochi contengono vari virus e trojan horse. L'organizzazione non ha ancora distribuito alcun antivirus. Dopo breve tempo, sui computer di Dario Nicoletti e di altri dipendenti iniziano a verificarsi degli eventi strani e imprevisti, che causano interruzioni di servizi e danneggiamento di dati. Nella figura seguente sono illustrate le varie vulnerabilità che erano presenti e la perdita delle risorse coinvolte.



❷ Esempio: **minaccia intenzionale** (attacco doloso)

Una dipendente chiamata qui Alessandra Moretti si vede rifiutare la promozione tre volte. Alessandra, che ha sempre lavorato molto, ritiene di non essere stata promossa in quanto troppo giovane. Alessandra è laureata in informatica e decide di dimettersi dalla società e di vendicarsi provocando l'interruzione dell'esecuzione delle richieste da parte del server Web della società. Per sferrare l'attacco al server Web della società, utilizza uno trumento di attacco di negazione di servizio denominato Trin00.

La maggior parte delle attività commerciali della società sono condotte tramite e-commerce e i client lamentano di non potersi connettere al server Web. Il diagramma seguente descrive i vari strumenti e le diverse vulnerabilità sfruttate da Alessandra Moretti per raggiungere il proprio obiettivo.

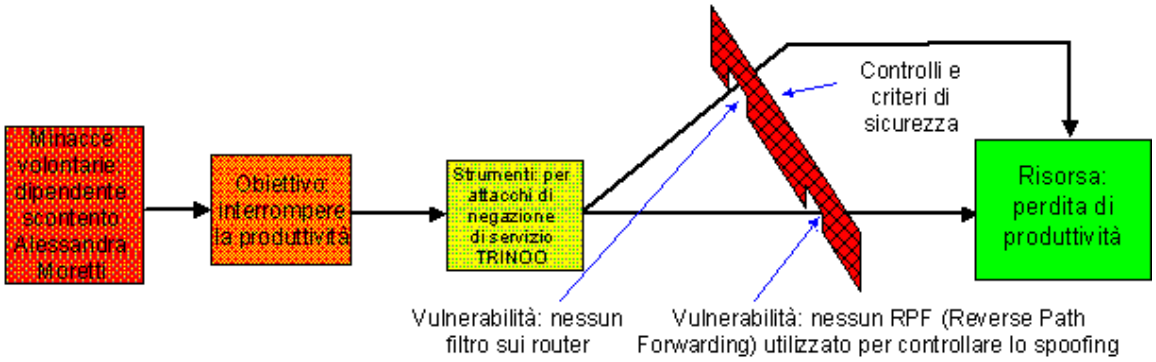


Figura 4

Si tenga presente che si tratta solo di un esempio. Le possibilità, gli strumenti, le vulnerabilità e i modi di contrastare l'attacco possono essere diversi.

➌ Esempio: **calamità naturali**

Un'organizzazione dispone di vari modem e di diversi router ISDN (Integrated Services Digital Network) e non è protetta dai picchi di tensione. Durante un temporale, i lampi colpiscono le linee del telefono e ISDN. Tutti i modem e i router ISDN vengono distrutti, coinvolgendo anche un paio di schede madri. Il diagramma seguente mostra la vulnerabilità e la perdita delle risorse.

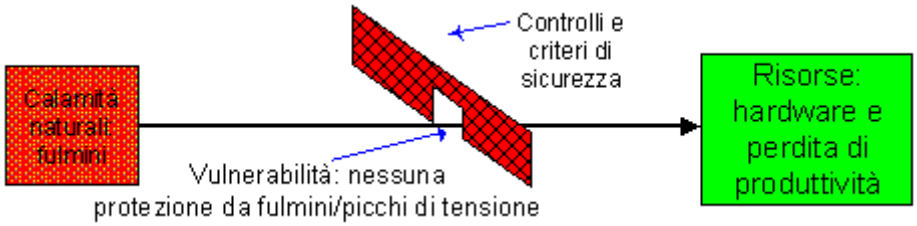


Figura 5

4 Aggressori esterni o "cracker"

I "cracker" vengono spesso definiti "hacker". La definizione di "hacker" è cambiata nel corso degli anni. Inizialmente "hacker" era chi si impegnava per ottenere il massimo possibile dal sistema che utilizzava, utilizzando tutte le parti di un sistema e studiandole fino a diventare esperto in tutti i dettagli. Queste persone rappresentavano una fonte di informazioni per gli altri utenti di computer e venivano considerati quasi dei "guru" o "maghi".

Ora, tuttavia, il termine "hacker" indica persone che penetrano con la forza nei sistemi o oltrepassano intenzionalmente e senza permesso i confini loro assegnati in un sistema.
Il termine corretto da utilizzare per indicare coloro che si introducono nei sistemi senza autorizzazione è "cracker". I metodi più utilizzati per riuscire ad accedere a un sistema comprendono l'identificazione delle password, che sfrutta le vulnerabilità nella sicurezza note, lo "spoofing" della rete e il "social engineering". L'Appendice C contiene una descrizione dettagliata di questi metodi.

4.1 Dipendenti non malintenzionati

Gli aggressori esterni non sono i soli utenti che possono danneggiare un'organizzazione. La minaccia principale all'integrità dei dati proviene da utenti autorizzati che non si rendono conto delle operazioni che effettuano. Errori e omissioni possono causare la perdita, il danneggiamento o l'alterazione di dati importanti.

Gli utenti, gli addetti all'immissione dei dati, gli operatori dei sistemi e i programmatori commettono frequentemente errori involontari che contribuiscono ad aggravare, direttamente o indirettamente, i problemi relativi alla sicurezza. Una minaccia può ad esempio essere costituita da un errore di immissione dati o di programmazione, che può causare l'arresto anomalo del sistema. In altri casi, gli errori creano vulnerabilità. Si possono verificare errori durante tutte le fasi del ciclo di vita del sistema.

Gli errori di progettazione e di programmazione, chiamati spesso "bug", possono essere di gravità diversa e risultare irritanti o catastrofici. I continui miglioramenti nella qualità del software hanno consentito la riduzione ma non l'eliminazione di questa minaccia. Problemi di sicurezza possono inoltre essere causati anche da errori di manutenzione e di installazione.

Gli errori e le omissioni rappresentano importanti minacce all'integrità dei dati. Gli errori vengono commessi non solo dagli addetti all'immissione dei dati che elaborano centinaia di transazioni al giorno, ma anche dagli utenti che creano e modificano i dati. Molti programmi, specialmente quelli sviluppati dagli utenti per i PC, mancano di misure per il controllo della qualità. Tuttavia, nemmeno i programmi più avanzati possono rilevare tutti i tipi di omissioni o di errori di immissione.

Gli utenti considerano spesso le informazioni che ricevono dai computer più accurate di quello che sono in realtà. Molte organizzazioni concentrano l'attenzione su errori e omissioni nella sicurezza dei rispettivi computer, nella qualità del software e nei programmi per il controllo della qualità dei dati.
La sicurezza fisica e l'integrità e riservatezza dei dati sono strettamente collegate. Infatti, l'obiettivo di alcuni attacchi non è la distruzione fisica del sistema, ma l'intrusione e la rimozione o la copia di informazioni importanti. Gli aggressori agiscono per soddisfazione personale o per avere una ricompensa.

4.2 Eliminazione e alterazione delle informazioni

Gli attacchi dolosi sono in genere provocati da utenti che eliminano o alterano le informazioni per dimostrare qualcosa o per vendicarsi di un torto subito. Gli attacchi interni sono causati da utenti generalmente spinti da rancore nei confronti dell'organizzazione perché sono scontenti di qualcosa. Gli aggressori esterni, invece, possono introdursi in un sistema solo per il gusto di farlo o perché desiderano dimostrare la propria abilità.

4.3 Furto di informazioni o frode

Le tecnologie informatiche vengono utilizzate sempre più frequentemente per commettere frodi e furti. I sistemi di computer possono essere violati in molti modi, sia con versioni automatizzate dei metodi tradizionali di frode che con metodi nuovi. I sistemi finanziari non sono i soli a essere oggetto di frodi. Altri obiettivi sono i sistemi che controllano l'accesso a qualsiasi risorsa, ad esempio i sistemi per il controllo delle presenze e degli orari, per la gestione del magazzino, per la valutazione scolastica o per le chiamate interurbane.

Gli utenti interni ed esterni possono commettere delle frodi. Gli utenti interni, che dispongono di autorizzazioni di accesso al sistema, perpetrano la maggioranza delle frodi scoperte sui sistemi. Gli utenti interni conoscono a fondo il sistema, le risorse da esso controllate e le relative pecche e si trovano quindi nella posizione migliore per commettere dei crimini. Anche gli ex dipendenti di un'organizzazione possono rappresentare una minaccia, in particolare se il relativo accesso non viene revocato rapidamente.

Poiché molti computer sono relativamente piccoli e costosi, è semplice rubarli e rivenderli. Un'organizzazione deve quindi cercare di proteggere i propri investimenti in attrezzature con strumenti fisici quali serrature e catenacci. Se il computer viene rubato, le informazioni contenute saranno a disposizione del ladro, che potrebbe cancellarle, leggerle oppure vendere le informazioni riservate, utilizzarle per ricatti o per compromettere altri sistemi.

Anche se è impossibile eliminare totalmente la possibilità di furti, è tuttavia possibile rendere le informazioni rubate virtualmente inutilizzabili, assicurandosi che vengano crittografate e che il ladro non disponga della chiave.

I dati possono essere sottratti da un computer o persino manipolati all'insaputa del proprietario. È ad esempio possibile collegare un'unità Zip alla porta parallela del computer e copiare diversi megabyte di dati.

È possibile che gli aggressori mirino a interrompere le normali attività aziendali. L'attacco potrebbe essere sferrato per dispetto, ad esempio da un dipendente scontento che non desidera lavorare perché non è stato promosso. Gli aggressori esterni potrebbero invece interrompere i servizi per acquisire un vantaggio sulla concorrenza. È inoltre possibile che gli attacchi vengano sferrati solo per il gusto di farlo. In circostanze come queste, l'aggressore ha un obiettivo specifico da raggiungere. Tale azione potrebbe risultare gratificante o remunerativa. Gli aggressori utilizzano vari metodi per sferrare attacchi di negazione di servizio, descritti nella sezione dedicata ai metodi, agli strumenti e alle tecniche per gli attacchi.

4.4 Metodi, strumenti e tecniche per gli attacchi

Gli aggressori intenzionali utilizzano metodi, strumenti e tecniche differenti per immettere, danneggiare e sottrarre informazioni da un sistema.

4.5 Intrusioni tramite posta elettronica

I protocolli per il trasferimento della posta più diffusi, ovvero SMTP, POP3 e IMAP4, non prevedono solitamente misure per l'autenticazione affidabile integrate nel protocollo di base.

Ciò facilita la contraffazione di messaggi di posta elettronica. Tali protocolli non richiedono nemmeno l'uso della crittografia, che potrebbe assicurare la privacy e la riservatezza dei messaggi. L'utilizzo delle estensioni esistenti a questi protocolli di base deve essere stabilito nell'ambito dei criteri che regolano l'amministrazione del server di posta. Alcune estensioni utilizzano strumenti di autenticazione stabiliti in precedenza, mentre altre consentono al client e al server di negoziare un tipo di autenticazione supportato da entrambi.

4.6 Social engineering

È una forma di intrusione comune. Può essere utilizzata da utenti esterni o interni all'organizzazione. Il termine "social engineering" indica il tentativo degli hacker di indurre gli utenti a rivelare le password o altri tipi di informazioni di protezione.

È necessario informare gli utenti in merito ai vari problemi relativi alla sicurezza, anche quelli non comuni. Un esempio comune di social engineering è costituito da un hacker che invia un messaggio di posta elettronica a un dipendente, presentandosi come amministratore e richiedendo la password del dipendente per effettuare delle attività

amministrative. L'utente comune, senza particolari conoscenze relative alla sicurezza, potrebbe non riuscire a distinguere un vero amministratore da un impostore, specialmente in un'organizzazione di grandi dimensioni. Un'altra strategia utilizzata per social engineering prevede che si telefoni a un utente presentandosi come amministratore e chiedendo le credenziali di accesso e la password. L'utente fornisce involontariamente i dati di accesso richiesti e l'impostore dispone di accesso completo.

Tra gli hacker e gli utenti che desiderano conoscere la password di qualcuno è molto diffuso anche lo "shoulder surfing". In questo caso, si indugia nei pressi della scrivania di un utente, parlando e attendendo che l'utente digiti una password. I dipendenti malintenzionati potrebbero agire anche in questo modo. È quindi necessario informare gli utenti in modo che non digitino le password davanti ad altre persone e che modifichino immediatamente la password se sospettano che altri utenti ne siano a conoscenza.
Un'altra forma di social engineering consiste nell'indovinare la password di un utente. Le persone che possono venire a conoscenza di informazioni sulla vita sociale e privata degli utenti, possono sfruttare tali informazioni. È ad esempio possibile che gli utenti scelgano come password il nome o la data di nascita di una sorella o di un figlio o il nome di un amico. Inoltre, gli utenti utilizzano spesso come password frasi che leggono sulle loro scrivanie o su poster presenti nell'area di lavoro. Gli hacker dispongono quindi di un'ulteriore opportunità di indovinare la password.

4.7 Attacchi intrusivi

Gli aggressori possono introdursi in molte reti utilizzando tecniche note. Ciò si verifica spesso quando gli aggressori conoscono le vulnerabilità della rete. Nei sistemi aggiornabili, gli amministratori potrebbero non avere o non allocare il tempo necessario per installare tutte le patch richieste in una quantità elevata di host. Inoltre, in genere non è possibile associare perfettamente i criteri di un'organizzazione sull'uso del computer ai meccanismi di controllo di accesso e questo spesso consente agli utenti autorizzati di effettuare operazioni non legittime.

Inoltre, gli utenti richiedono spesso protocolli e servizi di rete noti per essere difettosi e soggetti ad attacchi. Ad esempio, un utente potrebbe richiedere l'utilizzo di FTP per scaricare dei file. È molto importante che i criteri di sicurezza non prendano in considerazione solo le richieste dell'utente finale, ma anche le minacce e le vulnerabilità insite in tali richieste. In realtà, in pratica, non è mai possibile rimuovere tutte le vulnerabilità.
Il rilevamento delle intrusioni è un processo che consiste nel rilevare l'utilizzo non autorizzato o l'attacco a un computer o una rete. Dal rilevamento delle intrusioni dipendono due funzioni importanti per la protezione delle risorse del sistema contenenti informazioni.

La prima funzione è costituita da un meccanismo di riscontri che informa il team di protezione dell'efficacia degli altri componenti del sistema di sicurezza. La mancanza di intrusioni rilevate indica che non sono presenti intrusioni note, non che il sistema è completamente impenetrabile.

La seconda funzione consiste nel fornire un meccanismo di "trigger" o di "gating" che determini quando attivare le contromisure pianificate in caso di attacco. Un computer o una rete che non dispongono di un sistema di rilevamento delle intrusioni (IDS, Intrusion Detection System) potrebbero consentire agli aggressori di individuarne tranquillamente le debolezze. Se nelle reti sono presenti vulnerabilità, un aggressore determinato le individuerà e le sfrutterà. La stessa rete, ma con un IDS installato, rappresenta un ostacolo molto più arduo per un aggressore. L'aggressore può continuare a sondare la rete per individuarne le debolezze, ma se le vulnerabilità sono note, l'IDS dovrebbe essere in grado di rilevare e bloccare questi tentativi e di avvisare il personale di sicurezza, che potrà quindi adottare le necessarie contromisure.

4.8 Attacchi di negazione di servizio

Gli attacchi DoS sono progettati per impedire il legittimo uso di un servizio. Gli aggressori raggiungono questo obiettivo saturando la rete con una quantità di traffico maggiore di quella che può essere gestita. Ecco alcuni esempi:

- Saturazione delle risorse della rete, impedendo in tal modo agli utenti di utilizzare le risorse della rete.
- Interruzione delle connessioni tra due computer, impedendo le comunicazioni tra i servizi.
- Esclusione di un determinato utente dall'accesso a un servizio.
- Interruzione di servizi per un client o un sistema specifico.

Gli attacchi DoS saturano una rete remota con una quantità enorme di pacchetti di dati. Ciò provoca il sovraccarico dei router e dei server, che tentano di reindirizzare o gestire ciascun pacchetto. Nel giro di alcuni minuti, l'attività della rete aumenta esponenzialmente e la rete cessa di rispondere al traffico normale e alle richieste di servizio provenienti dai clienti. Questo tipo di attacco è noto anche come attacco con saturazione della rete o attacco con elevato consumo di larghezza di banda. Gli aggressori utilizzano vari strumenti, tra cui Trin00 e Tribe Flood Network (TFN e TFN2K).

4.9 Consumo di risorse del server

L'obiettivo di un attacco DoS è quello di impedire agli host o alle reti di comunicare attraverso una rete. Un esempio di questo tipo di attacco è rappresentato dall'attacco con saturazione

SYN:
Quando un client prova a contattare un servizio server, il client e il server si scambiano una serie di messaggi. Il client inizia inviando al server una richiesta di connessione TCP, o messaggio SYN. Il server risponde al messaggio SYN con un messaggio di riconoscimento

ACK-SYN. Il client effettua quindi il riconoscimento del messaggio ACK-SYN del server con un messaggio ACK. Al termine di queste tre operazioni, la connessione tra il client e il server è aperta ed essi possono scambiarsi dati specifici del servizio.

Il problema sorge quando il server ha inviato il messaggio SYN-ACK al client, ma non ha ancora ricevuto una risposta ACK dal client. In questa fase la connessione è aperta a metà. Il server tiene la connessione in sospeso in memoria, attendendo una risposta dal client. Le connessioni presenti in memoria aperte a metà scadono dopo un determinato intervallo di tempo, liberando nuovamente risorse importanti.

Per creare connessioni aperte a metà, viene utilizzato lo spoofing degli indirizzi IP. Il sistema dell'aggressore invia un messaggio SYN al server della vittima. Questi messaggi sembrano essere legittimi, ma di fatto sono riferimenti al sistema di un client che non è in grado di rispondere al messaggio SYN-ACK del server. Questo significa che il server non sarà mai in grado di ricevere un messaggio ACK dal computer client. Il server ha ora connessioni aperte a metà in memoria e alla fine esaurirà le connessioni server. Il server ora non è in grado di accettare nuove connessioni. Il limite di tempo sulle connessioni aperte a metà scadrà., ma il sistema dell'aggressore continua a inviare pacchetti, di cui ha effettuato lo spoofing degli indirizzi IP, con una frequenza elevata rispetto al limite di scadenza impostato sul server della vittima. Nella maggior parte dei casi, la vittima di tale attacco avrà difficoltà ad accettare nuove connessioni in ingresso legittime.

Questo tipo di attacco non riguarda in realtà alcuna delle connessioni correnti o in uscita. Utilizza in genere un'enorme quantità di memoria e di capacità di elaborazione del server, causandone il blocco. Il percorso del sistema di attacco è difficile da determinare, perché l'indirizzo del sistema dell'aggressore si cela sotto un indirizzo IP legittimo. Dal momento che la rete inoltra i pacchetti basandosi sull'indirizzo di destinazione, l'unico modo

per convalidare l'origine di un pacchetto consiste nell'utilizzare filtri delle origini di input.
Questo tipo di attacco non si basa sulla capacità dell'aggressore di utilizzare la larghezza di banda della rete. In questo caso, l'intruso utilizza risorse del server importanti. Di conseguenza, un intruso può effettuare questo attacco tramite una connessione remota contro computer connessi da reti molto veloci.

4.10 Saturazione delle risorse della rete

Un intruso potrebbe anche essere in grado di utilizzare tutta la larghezza di banda disponibile su una rete generando un numero elevato di pacchetti diretti alla rete. Si tratta in genere di pacchetti echo ICMP (Internet Control Message Protocol), ma in realtà potrebbero essere di qualsiasi altro tipo. Inoltre, l'intruso non deve necessariamente utilizzare un singolo computer, ma potrebbe coordinare o cooptare più computer su reti differenti per raggiungere lo stesso risultato. Questa strategia è nota come attacco di negazione di servizio distribuito (DDoS, Distributed Denial of Service Attack).

L'ICMP viene utilizzato per trasmettere informazioni sullo stato e sugli errori, tra cui notifiche di congestione e di altri problemi relativi alla rete. L'ICMP può essere utilizzato per determinare se un computer su Internet risponde, tramite l'invio di un pacchetto di richiesta echo ICMP a un computer sulla rete. Se il computer funziona, risponderà alla richiesta inviando un pacchetto di risposta echo ICMP. Un esempio comune è costituito dal comando Ping.
Sulle reti TCP/IP, un pacchetto può essere inviato a un singolo computer o trasmesso a tutti i computer sulla rete. Quando un pacchetto IP viene inviato da un computer sulla stessa rete locale a un indirizzo broadcast IP, tutti i computer su quella rete ricevono il pacchetto IP. Quando un computer esterno alla rete locale invia un pacchetto broadcast IP, tutti i computer sulla rete di destinazione ricevono il pacchetto broadcast, purché i router siano stati configurati per inoltrare i pacchetti broadcast.

In questi attacchi sono coinvolte tre parti: l'aggressore, l'intermediario e la vittima. È possibile che anche l'intermediario sia una vittima. L'intermediario riceve un pacchetto di richiesta echo ICMP diretto all'indirizzo di rete broadcast IP. Se le richieste echo ICMP non vengono filtrate, tutti i computer della rete riceveranno il pacchetto di richiesta echo ICMP e risponderanno con un pacchetto di risposta echo ICMP. Quando tutti i computer rispondono a questi pacchetti, si possono verificare gravi congestioni o interruzioni della rete.

Per creare questi pacchetti, gli aggressori non usano il proprio indirizzo di origine IP, ma l'indirizzo di origine della vittima predestinata. Tale azione è chiamata spoofing degli indirizzi IP. Quando i computer intermedi rispondono al pacchetto di richiesta echo ICMP, inviano quindi il pacchetto di risposta all'indirizzo IP della vittima. La rete del computer della vittima risulta quindi congestionata e potrebbe cessare di rispondere.

Gli aggressori hanno sviluppato un'ampia gamma di strumenti per questo scopo. Tali strumenti consentono agli hacker di inviare pacchetti di richiesta echo ICMP a più computer intermedi, facendo in modo che rispondano tutti all'indirizzo IP di origine della stessa vittima. Questi strumenti potrebbero anche essere utilizzati per individuare i router di rete che non filtrano il traffico broadcast.

Gli attacchi DDoS prevedono la violazione di centinaia o migliaia di computer su Internet. L'aggressore installa quindi su di essi il software DDoS per controllarli e avviare attacchi coordinati contro i siti vittima. Questi attacchi saturano in genere la larghezza di banda, la capacità di elaborazione dei router e le risorse di stack della rete, interrompendo la connettività di rete delle vittime.

L'aggressore inizia penetrando nei computer protetti in modo insufficiente sfruttando noti difetti dei programmi dei servizi di rete standard e la debolezza delle comuni configurazioni dei sistemi operativi. Esegue quindi altri passaggi su ciascun sistema. Innanzitutto, installa del software che consente di nascondere la violazione e le tracce della propria attività successiva. Ad esempio, sostituisce i comandi standard che consentono di visualizzare tutti processi in esecuzione con versioni che non mostrano i processi degli aggressori.
Installa quindi un processo speciale che consente di controllare in modo remoto il computer violato. Questo processo accetta comandi dalla rete, consentendo all'intruso di sferrare attacchi su Internet contro i siti vittima designati. Infine, prende nota dell'indirizzo IP del computer di cui ha preso il controllo.

Tutti questi passaggi sono estremamente automatizzati. Per evitare di essere scoperti, gli intrusi cominciano violando pochi siti, quindi utilizzano tali siti per introdursi in altri e ripetono questo ciclo molte volte. Quando hanno preso il controllo di migliaia di computer, riuniti in una rete DDoS, sono pronti per lanciare altri attacchi. Una volta installato il software DDoS, l'aggressore esegue un singolo comando che invia pacchetti di comandi a tutti i computer controllati, in modo da fornire istruzioni su come sferrare l'attacco, scegliendo tra un'ampia gamma di attacchi con saturazione, contro una specifica vittima. Quando l'aggressore decide di interrompere l'attacco, invia un altro comando singolo.
I computer controllati utilizzati per lanciare gli attacchi inviano un flusso di pacchetti. Nella maggior parte degli attacchi, questi pacchetti sono diretti al computer vittima. In una variante, chiamata "smurf" dal primo programma in circolazione che ha effettuato questo attacco, i pacchetti sono indirizzati ad altre reti, su cui provocano echo multipli tutti diretti alla vittima, come descritto in precedenza.

I pacchetti utilizzati negli attacchi DDoS contengono indirizzi di origine contraffatti o indirizzi IP di cui è stato effettuato lo spoofing. Se un pacchetto arriva al primo router e l'indirizzo IP di origine non corrisponde alla rete IP di provenienza, tale pacchetto verrà scartato dal router. Questo modo di controllare i pacchetti è chiamato filtraggio "ingress" o "egress", a seconda del punto di vista: "egress"" se rivolto alla rete del cliente, "ingress" se rivolto a Internet.
I primi segnali di un attacco si hanno quando migliaia di sistemi compromessi in tutto il mondo iniziano contemporaneamente a saturare la rete della vittima. Il primo sintomo è probabilmente il blocco di un router o qualcosa di simile, che provoca l'interruzione del traffico tra la vittima e Internet.

4.11 Saturazione con posta

Si tratta di un attacco basato sulla posta elettronica. La posta elettronica satura il sistema attaccato finché questo non si blocca. Possono verificarsi problemi differenti, a seconda del tipo di server e di come è configurato. Alcuni provider di servizi Internet forniscono account temporanei a chiunque effettui una sottoscrizione di prova. Questi account possono essere utilizzati per sferrare attacchi con la posta elettronica.
Di seguito sono riportati alcuni dei problemi tipici che potrebbero verificarsi:

- Il server della posta elettronica accetta i messaggi finché il disco contenente la posta non si riempie. La posta successiva non viene accettata. Se il disco della posta elettronica è anche quello principale del sistema, il sistema potrebbe bloccarsi.
- La coda in ingresso viene riempita di messaggi da inoltrare finché non viene raggiunto il relativo limite. I messaggi successivi non possono essere accodati.
- La quota disco del server di un determinato utente può essere superata. Questo potrebbe impedire la ricezione della posta successiva e il completamento delle operazioni dell'utente. Il ripristino potrebbe presentare delle difficoltà perché è possibile che l'utente debba utilizzare più spazio su disco proprio per eliminare la posta elettronica.

5 Attacchi con virus

5.1 Breve cronistoria

Tutti gli amministratori hanno sentito parlare dei virus e dei loro effetti. I virus possono essere molto distruttivi e causare la perdita di informazioni. Fred Cohen ha definito formalmente il termine "virus di computer" nel 1983, quando effettuò esperimenti accademici su un sistema VAX di Digital Equipment Corporation.
I virus sono stati suddivisi in due categorie: virus di ricerca e virus "in the wild". I virus di ricerca sono stati creati a scopo di studio o di ricerca e non sono stati distribuiti pubblicamente. I virus che invece si presentano periodicamente sono denominati "in the wild".
I primi virus di computer sono stati sviluppati all'inizio degli anni ottanta. I primi virus "in the wild" sono stati rilevati su Apple II. Nel 1981 è stato ad esempio segnalato il virus Elk Cloner. Attualmente, sono stati rilevati virus nelle piattaforme seguenti: Apple II, IBM PC, Macintosh, Atari e Amiga.

All'uscita sul mercato dei PC, i sistemi operativi come Microsoft MS-DOS® erano destinati ai singoli utenti, che avevano il controllo totale del computer. Non erano disponibili meccanismi di sicurezza per distinguere gli utenti, separare l'utente dal sistema o impedire la modifica intenzionale dei file dell'utente e del sistema.
Dato il modo con cui i computer venivano utilizzati, questi meccanismi non erano necessari. Tuttavia, la diffusione dei computer contribuì a creare una nuova industria che si sviluppò attorno ad essi, con l’introduzione di:

- Prodotti software commerciali quali fogli di calcolo ed elaboratori di testo.
- Giochi per computer.
- Utilizzo condiviso dei computer, sia da parte di più dipendenti che utilizzano lo stesso computer che da parte di organizzazioni di grandi dimensioni che collegano i computer tramite LAN.

Si noti che tutti i virus "in the wild" trovati hanno come bersaglio i PC. Attualmente, il maggior numero di tipi di virus rilevati riguardano di gran lunga i PC IBM.

I virus si sono evoluti negli anni grazie all'impegno dei loro autori per rendere il codice più difficile da rilevare, disassemblare ed estirpare. Questa evoluzione è stata particolarmente evidente per i virus dei PC IBM. Un'analisi della famiglia di virus dei PC IBM indica che la maggior parte dei virus scoperti variano a seconda del continente, ma che "Stoned", "Brain", "Cascade" e i membri della famiglia "Jerusalem" si sono ampiamente diffusi e continuano ad apparire. Questo significa che la maggior parte dei virus che vivono a lungo tendono a essere benigni, a replicarsi molte volte prima dell'attivazione o a essere piuttosto innovativi, in quanto adottano tecniche mai utilizzate prima per i virus.

I virus dei PC sfruttano la mancanza di controlli di accesso efficaci. I virus modificano i file e persino lo stesso sistema operativo. Si tratta di azioni legittime nel contesto del sistema operativo. Mentre sui sistemi operativi multiutente e multitasking vengono predisposti controlli più efficaci, gli errori di configurazione e le brecce nella sicurezza (bug di sicurezza) rendono più probabile la presenza dei virus sui PC.

Con l'avvento dei PC, gli utenti iniziarono a scambiarsi il software con i dischi floppy, sullo stesso computer venne eseguito software sia per uso professionale che per uso privato e le società trasferirono le informazioni su computer non più controllati da reparti IT centrali ma da singoli utenti. La mancanza di consapevolezza per i problemi relativi alla sicurezza e di meccanismi di sicurezza su questi sistemi iniziarono quindi a farsi sentire.
I ricercatori di virus si sono impegnati molto nello sviluppo di schemi per descrivere, denominare e classificare i virus dei computer e per definire le caratteristiche peculiari che consentono di distinguere i virus da altro software dannoso.

5.2 Funzionamento dei virus

Un virus è un segmento di codice in grado di replicarsi automaticamente collegato ad altro codice. Può trattarsi di codice innocuo e causare ad esempio la visualizzazione di un messaggio o la riproduzione di un motivo oppure essere dannoso e provocare l'eliminazione e la modifica dei file.
Il codice del virus cerca tra i file dell'utente un eseguibile ancora integro per il quale l'utente disponga di privilegi di scrittura. Il virus si introduce collocando un segmento di codice nel file del programma scelto. Quando viene eseguito un programma contenente un virus, il virus assume immediatamente il controllo, individuando e attaccando altri programmi e file.

Alcuni virus sono "residenti in memoria". Quando un utente esegue un programma contenente questo tipo di virus, il virus si trasferisce nella memoria e vi rimane anche se il programma originale viene arrestato. I programmi eseguiti successivamente vengono attaccati dal virus finché il computer non viene arrestato o spento. Alcuni virus hanno una fase di "inattività" e appariranno solo in determinati momenti o quando vengono effettuate determinate operazioni.

Una variante è un virus che viene generato modificando un virus noto, ad esempio aggiungendo nuove caratteristiche o tecniche per eludere il rilevamento. Il termine "variante" si utilizza in genere solo quando le modifiche sono minori, ad esempio il cambiamento della data di attivazione da venerdì 13 a martedì 12.

Un virus di tipo overwriting distruggerà il codice o i dati del programma host sostituendoli con il proprio codice. Si tenga presente che la maggior parte dei virus tentano di conservare le funzionalità e il codice originale del programma host dopo l'attacco perché è più probabile che il virus venga rilevato ed eliminato se il programma cessa di funzionare. Un virus non-overwriting è progettato per aggiungere il codice del virus alla fine fisica del programma o per spostare il codice originale in un'altra posizione.
Una procedura di auto-riconoscimento è una tecnica per mezzo della quale un virus determina se un eseguibile è già stato "infettato". La procedura consiste in genere nella ricerca di un determinato valore in una posizione nota dell'eseguibile. L'auto-riconoscimento risulta necessario se il virus deve impedire che si verifichino più intrusioni in un singolo eseguibile. Più intrusioni causano infatti un aumento eccessivo della dimensione degli eseguibili e del corrispondente spazio di memorizzazione, fattori che facilitano il rilevamento del virus.

Un virus residente si installa come parte del sistema operativo all'esecuzione di un programma host che lo contiene. Il virus rimarrà residente fino all'arresto del sistema. Una volta installato in memoria, un virus residente è in grado di introdursi in tutti gli host adatti cui viene effettuato l'accesso.

Un virus stealth è un virus residente che tenta di eludere il rilevamento nascondendo la propria presenza nei file. Per raggiungere questo obiettivo, il virus intercetta le chiamate di sistema che esaminano il contenuto o gli attributi dei file interessati. Il risultato di queste chiamate deve essere modificato in modo che corrisponda allo stato originale del file. Ad esempio, un virus stealth potrebbe rimuovere il proprio codice da un eseguibile quando questo viene letto, piuttosto che eseguito, in modo tale che un package software antivirus esamini il programma che lo include integro.

Un virus crittografato è composto da due parti: un piccolo strumento di decrittazione e il corpo del virus crittografato. Quando il virus viene eseguito, viene innanzitutto impiegato lo strumento di decrittazione per decrittarne il corpo. Il corpo del virus può quindi essere eseguito, replicato o può diventare residente. Il corpo del virus comprenderà uno strumento di crittografia che verrà impiegato durante la replica. Un virus a crittografia variabile utilizzerà chiavi crittografiche o algoritmi di crittografia differenti. I virus crittografati sono più difficili da disassemblare e studiare poiché è innanzitutto necessario decrittarne il codice.

Un virus polimorfo crea durante la replica copie funzionalmente equivalenti, ma con flussi di byte nettamente differenti. A tale scopo, il virus potrebbe inserire istruzioni superflue in modo casuale, scambiare l'ordine delle istruzioni indipendenti o utilizzare schemi crittografici differenti. Questa mutevolezza rende il virus difficile da rilevare, identificare o rimuovere.
Un virus di ricerca è un virus che è stato creato, ma mai diffuso pubblicamente. Appartengono a questa categoria i virus inviati ai ricercatori dai creatori di virus. I virus che sono stati rilevati all'esterno delle comunità di ricerca sono chiamati "in the wild".
Come si diffondono i virus dei computer?
Di seguito sono elencate le caratteristiche peculiari di un virus:

- È in grado di replicarsi.
- Richiede un programma ospite come vettore.
- Viene attivato da un'azione esterna.
- La capacità di replica è limitata al sistema (virtuale).

I virus si spostano da un computer all'altro introducendosi nei file o nei record di avvio dei dischi e dei dischetti. Attualmente non è raro trovarli negli allegati della posta elettronica e in altri programmi scaricabili da Internet.
Un virus è un agente relativamente passivo, la cui attivazione e propagazione dipende dagli utenti comuni. Se il file che lo contiene viene eseguito, può spostarsi da un file all'altro sullo stesso computer, dalla memoria del computer a un file su disco, tramite un disco che viene trasportato da un computer all'altro (alcune società vietano l'uso di dischi floppy, per impedire che gli utenti copino informazioni sui rispettivi computer), tramite file eseguibili allegati alla posta elettronica e per mezzo di un modem o una connessione di rete.
Danni causati dai virus
I virus possono distruggere le tabelle di allocazione file (FAT, File Allocation Table) e causare la corruzione dell'intero file system, rendendo necessari il ricaricamento e la reinstallazione completa del sistema. Possono anche danneggiare settori del disco, distruggendo parti di file e programmi. Inoltre, possono ridurre lo spazio disponibile sui dischi rigidi duplicando i file e formattare determinate tracce di un disco o l'intero disco.

I virus possono distruggere specifici file eseguibili e alterare le informazioni contenute nei file di dati, provocando la perdita dell'integrità dei dati. Inoltre, possono causare interruzioni del sistema, che non risponderà più alla tastiera e agli spostamenti del mouse.

5.3 Trojan horse

Il termine "trojan horse" deriva da un mito secondo cui i greci consegnarono un cavallo di legno gigante ai loro nemici, i troiani, apparentemente come dono di pace. Dopo che i troiani portarono il cavallo all'interno delle mura della città di Troia, i soldati greci uscirono furtivamente dal ventre cavo del cavallo e aprirono le porte della città, consentendo ai loro compatrioti di entrare e prendere il controllo di Troia.

Che cosa sono i trojan horse?

Un trojan horse è un codice nascosto in un programma come un gioco o un foglio di lavoro la cui esecuzione appare sicura ma presenta degli effetti collaterali nascosti. Quando il programma viene eseguito, esso sembra funzionare come previsto, ma in realtà sta distruggendo, danneggiando o alterando informazioni in background. È un vero e proprio programma e non richiede un programma ospite in cui annidarsi. Un esempio di trojan horse è rappresentato dall'eseguibile Christmas che, quando eseguito, visualizza una figura animata di Babbo Natale e un messaggio che augura Buon Natale. In background, il codice aggiuntivo elimina i file ed effettua altre operazioni dannose.

Come si sono diffusi i trojan horse?

I trojan horse si sono diffusi principalmente attraverso la posta elettronica e lo scambio di dischi e di informazioni tra i computer. Anche i worm possono diffondere trojan horse.
Danni causati dai trojan horse
Il danno causato dai trojan horse è simile a quello causato dai virus. Per la maggior parte del tempo gli utenti non sono consapevoli dei danni provocati dai trojan horse in quanto la relativa azione viene nascosta.

5.4 Worm

All'inizio, i worm furono utilizzati come meccanismo legittimo per effettuare operazioni in un ambiente distribuito. In base a una serie di esperimenti presso il centro di ricerche Xerox di Palo Alto nel 1982, le prestazioni dei worm di rete in operazioni di gestione della rete furono infatti giudicate promettenti. La gestione dei worm, ovvero il controllo del numero di copie in esecuzione in un determinato istante, risultava tuttavia difficile.

I worm furono considerati una minaccia potenziale alla sicurezza dei computer per la prima volta nel corso del dicembre 1987, quando il Christmas Tree Exec attaccò i mainframe IBM, colpendo sia la rete IBM mondiale che BITNET. Il Christmas Tree Exec non era un vero worm: si trattava di un trojan horse con un meccanismo di replica. Gli utenti ricevevano un biglietto d'auguri natalizio tramite posta elettronica contenente codice (REXX) eseguibile. Una volta eseguito, il programma apparentemente disegnava semplicemente un albero di Natale sullo schermo. L'albero di natale veniva effettivamente visualizzato, ma il programma inviava contemporaneamente anche una copia a tutti gli utenti della Rubrica.

Internet Worm era invece un vero worm. Fu rilasciato il 2 novembre 1988. Attaccò i sistemi UNIX DEC e Sun collegati a Internet. Comprendeva due insiemi di codici binari, uno per ciascun sistema. Per propagarsi, sfruttò i protocolli TCP/IP, le vulnerabilità nell'invio della posta, i comuni protocolli a livello di applicazione, i bug dei sistemi operativi e vari errori nell'amministrazione dei sistemi. I vari problemi di gestione dei worm si tradussero in prestazioni dei sistemi estremamente ridotte e nella negazione del servizio di rete. Sfruttò i difetti dei sistemi operativi e i comuni problemi di gestione del sistema.
Che cosa sono i worm?
Di seguito sono elencate le caratteristiche peculiari di un worm:

- È in grado di replicarsi.
- Contiene e controlla il proprio codice. Non richiede un host.
- Viene attivato tramite creazione di processi. Richiede un sistema multitasking.
- Se si tratta di un worm di rete, è in grado di replicarsi attraverso i collegamenti di comunicazione.

Un worm è un programma progettato per replicarsi, ma potrebbe effettuare anche qualsiasi altro tipo di attività. Il primo worm di rete fu creato per eseguire funzioni utili per la gestione della rete. Per eseguire tali funzioni, utilizzava le proprietà del sistema. Tuttavia, un worm dannoso può trarre beneficio dalle stesse proprietà. Gli strumenti che consentono a tali programmi di replicarsi non sempre distinguono, infatti, tra codice innocuo e codice dannoso.

Per replicarsi, i worm sfruttano i difetti, ovvero i bug del sistema operativo, o una gestione inadeguata del sistema. In genere, la diffusione di uno worm provoca brusche interruzioni che arrestano intere reti.

I worm sono programmi che vengono eseguiti indipendentemente e che si spostano da un computer all'altro attraverso le connessioni di rete. Alcune parti dei worm possono essere in esecuzione su molti computer differenti. I worm non cambiano gli altri programmi, anche se possono diffondere altro codice che effettua tale attività.
Influenza dei worm sui sistemi di rete
Per sviluppare un worm, occorrono un ambiente di rete e un autore che non conosca solo le funzionalità e i servizi di rete, ma anche gli strumenti operativi necessari per supportarli una volta raggiunto il computer. Proteggersi contro i programmi worm equivale a proteggersi contro le violazioni. Se un intruso può penetrare in un computer, lo può fare anche un worm.
Proteggendo un computer dall'accesso non autorizzato, lo si protegge quindi anche dai worm.

6 Analisi degli Attacchi

Le svariate tipologie di attacco possono essere raggruppate in queste quattro categorie:

- **Acquisizione di informazioni**: non è una tipologia di attacco vera e propria ma un insieme di azioni che anticipano un attacco. Esempi potrebbero essere: scanning e sniffing.
- **Accesso non autorizzato**: un intruso ottiene l'accesso ad una rete o ad un computer non avendone l'autorizzazione dopo di ciò potrebbe ottenere l'accesso ad ulteriori informazioni o bloccare determinati servizi.
- **Accesso alle informazioni** (ed eventuale modifica): l'operazione di accesso alle informazioni e l'eventuale modifica potrebbe derivare da un accesso non autorizzato al sistema mediante interrogazione a servizi esistenti o mediante spoofed mail.
- **Denial of Service** (interruzione del servizio): l'intruso rende un sistema, un servizio o una rete non disponibile esaurendone le risorse, siano queste risorse di rete (banda), connessioni TCP (Syn Floods) o spazio disco (effettuando un upload di dati o causando delle registrazioni nei logs). Potrebbe avvenire anche mediante impersonazione del sistema avversario. Non richiede nessun accesso al sistema.

6.1 Social Engineering

Il meno tecnico dei metodi di attacco. Consiste nell'acquisizione di informazioni parlando dei metodi di sicurezza con la gente sfruttando il fatto che di solito si è portati ad aver fiducia e ad aiutare gli altri. L'attaccante finge di essere una persona degna di fiducia. La migliore difesa consiste nell'autenticazione (chiamata di conferma e richiesta di autenticazione).

6.2 Acquisizione di informazioni

Ci sono diverse tecniche per acquisire informazioni utili all'attaccante:

- **Dumpster diving**: analisi dei rifiuti alla ricerca di organigrammi (per trovare nomi di persone da impersonare in un attacco di social engineering), archivi cartacei, appunti o altre informazioni.
- **Shoulder surfing**: consiste nello spiare stando alle spalle le operazioni di inserimento di informazioni sensibili (password, codici di accesso, numeri telefonici).
- **Scanning**: il tentativo di connettersi ad un intervallo di numeri di porta o indirizzi IP per vedere quali servizi o sistemi sono presenti ed attivi.
- **Servizi di base (Basic services)**: i servizi di base (finger, netstat, primitive SMTP VRFY e EXPN) possono essere utilizzati da un attaccante per ottenere informazioni sugli utenti o per verificare l'esistenza di un utente.
- **Sniffing**: Il processo di acquisire il traffico di rete utilizzando un analizzatore di protocollo. E' necessario un accesso alla rete.
- **Version information**: è utilizzata per fornire informazioni all'attaccante circa le problematiche di sicurezza note (known security holes) all'interno della rete.

6.3 Sfruttamento di relazioni di fiducia mal gestite

Le relazioni di fiducia sono degli strumenti potenti e potenzialmente pericolosi che possono sia aumentare la produttività degli utenti che, se mal gestite o peggio, lasciate nella loro configurazione "di vendita", creare delle vaste brecce nella sicurezza.

- **User Accounts e Passwords**: la più semplice delle relazioni di fiducia soffre di queste problematiche:
  - Gli utenti tendono a scegliere delle passwords semplici da ricordare.
  - Se gli utenti sono portati a scegliere passwords difficili da ricordare tendono a scriverle da qualche parte. La soluzione prevede l'uso di software in grado di generare passwords difficili ma allo stesso tempo semplici da ricordare.
  - Le passwords sono suscettibili ad un attacco di sniffing.
  - I files che contengono le passwords sono a volte accessibili e quindi decrittabili utilizzando strumenti sviluppati ad hoc (NTCrack, LC).
  - La soluzione potrebbe essere quella di utilizzare uno schema di password resistente, a singolo uso, memorizzato su token card.
- **Windows Disk Sharing**: L'accesso alle risorse avviene o attraverso quelli che sono i diritti dell'utente una volta autenticato all'interno della rete (Dominio NT) o sulla base della singola condivisione, o senza autenticazione (MS Windows 95/3.11). L'accesso da parte di un attaccante potrebbe essere causato da un'erronea assegnazione dei permessi. Quindi, per un utilizzo di questa risorsa bisognerebbe prevedere un'amministrazione tesa a ridurre i privilegi ed a filtrare o bloccarne l'uso dall'esterno della rete. Venendo a mancare tutto questo, questa funzionalità non dovrebbe essere utilizzata.

6.4 Sfruttamento di servizi non autenticati

Un certo numero di servizi di rete non utilizzano l'autenticazione, e per questo possono facilmente subire un attacco di spoofing o l'accesso e la successiva modifica delle informazioni:

- **TFTP**: si basa solo sui permessi del filesystem e potrebbe essere utilizzato per acquisire files sensibili del sistema.
- **SMTP**: la maggior parte dei sistemi non effettuano dei controlli sulla vera identità degli utenti e quindi possono essere utilizzati per un attacco di spoofing.
- **DNS**: il sistema potrebbe essere sensibile ad un attacco di spoofing, portando l'utente a connetersi al sistema sbagliato.
- **RIP**: visto che il protocollo non utilizza l'autenticazione, qualsiasi sistema o router in ascolto di pacchetti di RIP potrebbero essere indirizzati verso la rete errata dove l'attaccante potrebbe (per esempio) intercettare o almeno monitorare il traffico.
- **Redirezione ICMP**: soffre degli stessi problemi del protocollo RIP.

La migliore soluzione consiste nel disabilitare i servizi che non vengono utilizzati o limitarne l'uso/accesso agli elementi della rete degni di fiducia. La migliore soluzione in assoluto per l'SMTP è la crittografia o l'autenticazione.

Sfruttamento dei servizi centralizzati

I servizi centralizzati vengono utilizzati per la gestione dei sistemi connessi alla rete:

- **SNMP**: SNMP utilizza un community name come password che viene trasmesso in chiaro e che di solito è uguale a 'public'.

L'utilizzo di questi servizi dovrebbe essere ridotto alle reti sicure.

Malicious Data

Le nuove caratteristiche dei software permettono azioni non pianificate durante la fase di sviluppo degli stessi:

- **Vulnerabilità intenzionali**, per esempio:
- Macros (per esempio in MS Office);
- Primitive di I/O nei files PostScript;
- Java & ActiveX;
- Funzionalità di Autoplay attiva (MS Windows).

  La soluzione ovvia sarebbe quella di disabilitare queste funzionalità, in attesa dello sviluppo delle stesse con caratteristiche più sicure; ma questo potrebbe limitare l'utilità dei programmi verso gli utenti.

- **Vulnerabilità non intenzionali**:
- Dati inseriti in un programma non validi;
- Buffer overflow: viene utilizzato per interrompere il funzionamento di un sistema o per ottenerne l'accesso. E' richiesta una rilevante conoscenza tecnica nell'analisi delle variabili di una applicazione alla ricerca di valori non testati o al di fuori dei limiti consentiti. In pratica, il codice dell'attaccante invia una stringa in ingresso che è superiore al buffer allocato dal programma e sovrascrive il byte successivo in memoria che potrebbe contenere i valori puntati dallo stack. Visto che questi valori indicano al programma dove andare per eseguire le prossime istruzioni, inserendo all'interno dei dati ben calcolati, l'attaccante potrebbe reindirizzare il tutto per far si che vengano eseguite delle operazioni presenti nella stringa di input. L'operazione è mirata ad una specifica variabile di uno specifico programma su uno specifico hardware o piattaforma software.

  L'unica soluzione è quella di analizzare in fase di sviluppo la lunghezza delle variabili in input.

6.5 Spoofing

E' la capacità di sostituirsi a qualcuno/qualcosa.

- **User account spoofing**: usare nome utente e password di un altro utente senza averne il diritto. Può avvenire utilizzando strumenti come sniffing e password crackers.
- **DNS spoofing**: invio di una risposta DNS ad un Name Server nella rete della vittima. E' difficile da contrastare ma è anche difficile da attuare.
- **IP Address spoofing**: è l'attacco più diffuso. Si basa sul fatto che la maggior parte dei routers all'interno di una rete controllino solo l'indirizzo IP di destinazione e non quello sorgente. Questo fa si che un attaccante possa inviare dei pacchetti ad un sistema bersaglio e le risposte di quest'ultimo saranno invece inviate al falso IP utilizzato dall'attaccante. L'IP spoofing potrebbe essere limitato inserendo dei filtri sull'indirizzo IP sorgente a livello routers.
- **IP Address spoofing e TCP Sequence Number Prediction**: utilizzato da Kevin Mitnick contro Tsutomu Shimamura. E' suddiviso in diversi passaggi :
  1. L'attaccante (X) apre diverse connessioni TCP successive per determinare il modo con cui viene generato il numero di sequenza TCP sull'host della vittima. Quindi effettua un TCP Syn Flood di A, l'host a cui si deve sostituire.
  2. 2. L'attaccante invia un pacchetto a B pretendendo di essere A ed imposta il flag SYN nel pacchetto.
  3. B invia un pacchetto ACK, SYN ad A che non può riceverlo perchè è sottoposto al flooding. L'attaccante deve indovinare quale sarà il valore utilizzato nella parte di SYN del pacchetto basandosi sulle analisi fatte nel punto 1.
  4. L'attaccante invia l'ultimo pacchetto dell'handshake a 3 passaggi del TCP a B (ACK al posto di A più il numero di sequenza indovinato) ed invia dei comandi a B impersonando una eventuale relazione di fiducia esistente con A.

  Questo tipo di attacco può essere evitato filtrando l'indirizzo IP sorgente ed utilizzando software che non utilizzino degli algoritmi che consentano di indovinare i numeri di sequenza TCP.

6.6 Sfruttamento di bugs nel software

Molti problemi di sicurezza nascono come bugs nel software e possono essere raggruppati in:

- Software complesso: più il software è complesso maggiore è la probabilità di sbagliare;
- Opzioni per il debug o trapdoors inserite dal programmatore: inserendo una certa parola il programma esegue una determinata operazione a volte non documentata;
- Scarsa pratica di programmazione: il programmatore per mancanza di esperienza non sviluppa il programma valutando tutti gli accorgimenti necessari dal punto di vista della sicurezza:
- non verifica la lunghezza delle variabili di input;
- non verifica la corretta implementazione dei protocolli (ping of death);
- condizioni transitorie non valutate: il programma effettua delle operazioni passando da un livello ad uno con diritti superiori. Riuscendo a bloccare il programma si potrebbe ottenere una shell con i diritti associati al programma in quel momento.
- Scarsa protezione dei segreti: molte applicazioni inviano o memorizzano informazioni sensibili in chiaro oppure utilizzano algoritmi crittografici facilmente decrittabili. Lo stesso dicasi per i protocolli (FTP/Telnet/SMTP/POP3).
- Anomalie nel protocollo: difficili da prevenire, sfruttano caratteristiche del protocollo non analizzate:
- Frammentazione IP: l'attaccante invia un secondo frame IP con una parte che si sovrappone al primo già ricevuto.
- **TCP SYN Flood:**

  E' un attacco di tipo Denial of Service (DOS) che può interrompere un servizio su un host inviando solo da 4 a 6 pacchetti ogni due minuti. Funziona utilizzando l'handshake a 3 passaggi del TCP.

  Nell'attacco X invia il primo SYN fingendo di essere un indirizzo IP che non esiste (NOBODY). B invia un SYN, ACK al sistema che non esiste ed attende da questo l'invio dell'ACK. Questa attesa a volte può durare fino a 76 secondi.

  Nel frattempo comunque il sistema occupa risorse per attendere l'eventuale risposta all'interno del Backlog Queue, un'apposita area, riservata a questo, ma limitata comunque in quantità (dipende dall'implementazione del fornitore e può variare da 6 a 10 slots o più). Se l'attaccante invia un numero di pacchetti tale da riempire il Backlog Queue, il sistema attaccato non sarà più in grado di accettare connessioni e l'amministratore potrebbe anche non accorgersi di nulla. La soluzione potrebbe essere quella di adottare dei software in grado di rilevare l'anomalia e di inviare dei pacchetti RST al sistema attaccato per ripure il Backlog Queue.

6.7 Denial of Service

Causano la perdita dell'utilizzo di una risorsa sovraccaricandola, ma non ne permettono l'accesso all'attacante. I principali attacchi sono:

- **Ping floods**: invio di ICMP echo request in numero maggiore a quelli gestibili dalla rete o dal sistema attaccato (FPING);
- **Out of Band Data Crash**: l'attaccante invia un pacchetto con l'Urgent Pointer impostato e visto che la macchina bersaglio non lo gestisce ne causa il crash oppure il riavvio.
- **TCP SYN Floods, Ping of Death, UDP Bombs ...**

Le soluzioni al problema non sono semplici. Nel caso dell'ICMP si può risolvere inserendo dei filtri. Alcuni servizi possono essere interrotti, ma non lo si può fare con tutti visto che questo non farebbe altro che far raggiungere lo scopo prefissato dall'attaccante.

7 Aspetti Legali

Prima di procedere ad analizzare praticamente le tecniche di attacco è basilare avere una cognizione di ciò che si intende compiere e di quali implicazioni questo potrebbe avere dal punto di vista legale.

7.1 Principali Articoli di Legge sugli attacchi informatici

Il legislatore, con la legge del 23 Dicembre 1993 n. 547, pubblicata sulla Gazzetta Ufficiale N.305 del 30.12.1993, ha offerto uno strumento decisivo per contrastare tutti quei reati che si configurano all'interno del vasto panorama del crimine informatico. Ed in particolare:

- **Violenza sulle cose (art. 1.1 - aggiunge il seguente comma dopo il secondo comma art. 392 C.P.)**: Si ha, altresì, violenza sulle cose allorchè un programma informatico viene alterato, modificato o cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento di un sistema informatico o telematico.

- **Attentato a impianti di pubblica utilità (art. 2.1 - sostituisce art. 420 C.P.)**: Chi commette un fatto diretto a danneggiare o distruggere sistemi informatici o telematici di pubblica utilità, ovvero dati, informazioni o programmi in essi contenuti o ad essi pertinenti è punito, salvo che il fatto costituisca più grave reato, con la reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione o il danneggiamento dell'impianto o del sistema, dei dati, delle informazioni o dei programmi ovvero l'interruzione anche parziale del funzionamento dell'impianto o del sistema la pena è della reclusione da tre a otto anni.

- **Accesso abusivo ad un sistema informatico o telematico (art. 4.1 - aggiunge articoli dopo art. 615-bis C.P.)**:
  [art. 615-ter] Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

  La pena è della reclusione da uno a cinque anni:

  1. Se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema. Qualora i fatti riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Si procede a querela della persona offesa.

  2. Se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato. Qualora i fatti riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Si procede d'ufficio.

  3. Se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Si procede d'ufficio.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici:
[art. 615 quater] Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto

scopo, è punito con la reclusione sino ad un anno e con la multa sino a lire dieci milioni.

La pena è della reclusione da uno a due anni e della multa da lire dieci milioni a venti milioni se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.

- **Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico**:
  [art. 615-quinquies] Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a lire venti milioni.

Da notare che il DPR 318 del 28 Luglio 1999 prevede:

"**Art. 4 - Codici identificativi e protezione degli elaboratori**
...
c) gli elaboratori devono essere protetti contro il rischio di intrusione ad opera di programmi di cui all'articolo 615 *quinquies* del codice penale, mediante idonei programmi, la cui efficacia ed aggiornamento sono verificati con cadenza almeno semestrale."

- **Corrispondenza (art. 5.1 - sostituisce quarto comma art. 616 C.P.)**: per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza.

- **Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 6.1 - inserisce dopo l'articolo 617-ter C.P.)**:
  [art. 617-quater] Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.

Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

1. in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
2. da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
3. da chi esercita anche abusivamente la professione di investigatore privato.

- **Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche [art. 617-quinquies]** Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.

  La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.
- **Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche**
  [art. 617-sexies] Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad

  un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni.
  La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.

- **Danneggiamento di sistemi informatici e telematici (art. 9.1 - aggiunge articolo dopo l'art. 635 C.P.)**:
  [art. 635 bis] Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, é punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.

  Se ricorre una o più delle circostanze di cui al secondo comma dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.

- **Frode informatica (art. 10.1 - aggiunge articolo dopo l'art. 640-bis del C.P.):**
  [art. 640-ter] Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da lire centomila a due milioni.

  La pena è della reclusione da uno a cinque anni e della multa da lire seicentomila a tre milioni se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

  Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante .

- **Intercettazioni di comunicazioni informatiche o telematiche (art. 11.1 - aggiunge articolo dopo l'art. 266 C.P.):**
  [art. 266-bis] 1. Nei procedimenti relativi ai reati indicati nell'articolo 266, nonchè a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche, è consentita l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi .

8 Dlgs 196/03 e DPS

Con l'entrata in vigore del nuovo codice privacy, **a partire dal 1° gennaio 2004**, il quadro delle misure di sicurezza, che devono essere adottate nel trattamento dei dati personali, cambia profondamente.
Ferma restando la distinzione tra *misure idonee*, la cui inosservanza espone alla responsabilità per danni, e *misure minime*, dalla mancata adozione delle quali conseguono addirittura responsabilità di ordine penale, per quanto riguarda la individuazione di queste ultime viene mandato in soffitta il Dpr 318/1999, per essere sostituito dal *disciplinare tecnico in materia di misure minime di sicurezza*, che entra a fare parte integrante del nuovo codice privacy, di cui costituisce l'Allegato B.

Una scadenza così ravvicinata, entro cui adottare le ***nuove misure minime*** previste, avrebbe potuto creare problemi di ordine tecnico ed organizzativo, ai soggetti che trattano dati personali. Il legislatore ha quindi differito, con le disposizioni transitorie, il termine ultimo entro il quale è possibile adeguarsi, a quanto previsto dal disciplinare tecnico, nei seguenti termini:

a) per **tutti i soggetti**, il comma 1 dell'articolo 180 stabilisce il termine ultimo del **30 giugno 2004 (prorogato oggi al 31 dicembre)**, per adottare le ***nuove*** misure minime. Per i fini in esame, il termine ***nuove*** misure minime va inteso nella duplice accezione di:

- **novità oggettiva**, conseguente cioè al fatto che il nuovo codice introduce, per la generalità dei soggetti, una misura che non era prevista dal Dpr 318/1999
- **novità soggettiva**, che deriva cioè dal fatto che, alla luce delle nuove regole, possa aumentare la portata degli adempimenti cui è tenuto un determinato soggetto, rispetto a quanto avveniva in base alla previgente normativa. Tipico esempio è quello di chi tratta dati sensibili o giudiziari, con l'uso di strumenti elettronici che non sono in rete pubblica, che ai sensi delle nuove regole deve procedere alla redazione del documento programmatico sulla sicurezza, adempimento al quale non era in precedenza tenuto. Anche in questa ipotesi, che non è nuova dal punto di vista *oggettivo*, ma solo da quello *soggettivo* del titolare in esame, si può beneficiare del maggiore termine, previsto dalle disposizioni transitorie, per procedere alla adozione delle ulteriori misure, previste da tale documento, ed alla redazione dello stesso

b) nel solo caso in cui si possiedano **strumenti elettronici tecnicamente inadeguati**, i commi 2 e 3 dell'articolo 180 differiscono ulteriormente al **31 dicembre 2004** il termine ultimo, entro cui si devono adottare le ***nuove*** misure minime.

La norma detta le condizioni che, al verificarsi dell'ipotesi **b)**, autorizzano ad avvalersi del maggiore termine:

- la circostanza di disporre di strumenti elettronici che, per obiettive ragioni tecniche, non consentono in tutto o in parte l'immediata applicazione delle misure minime, deve essere verificata in data 1° gennaio 2004. Chi si trovasse in questa situazione può quindi beneficiare del maggiore termine del 31 dicembre 2004, anche nell'ipotesi in cui gli strumenti elettronici venissero sostituiti, con strumenti adeguati, prima della scadenza generale del 30 giugno 2004 (oggi prorogato al 31 dicembre)
- **entro il 30 giugno 2004**(oggi prorogato al 31 dicembre), il titolare deve redigere un *documento avente data certa*, da custodire presso la propria struttura (non va quindi inviato al Garante), nel quale espone le ragioni per cui gli strumenti elettronici sono, in tutto o in parte, inadeguati: per ottenere il requisito della data certa, non è necessario recarsi da un notaio o all'Ufficio del registro, ma è ad esempio sufficiente inviare a sé stessi il documento, mediante piego raccomandato con ricevuta di ritorno (***la data del 30 giugno 2004 è stata ufficializzata dal Garante*** con provvedimento del 22 marzo, fugando quindi i dubbi di coloro, dei quali fa parte chi scrive, che ritenevano che, in assenza di una presa di posizione ufficiale, il termine ultimo per redigere il documento dovesse necessariamente essere il 31 dicembre 2003)

- durante il processo di adeguamento, il titolare deve comunque adottare ogni possibile misura di sicurezza, in relazione agli strumenti elettronici detenuti, in modo da evitare un incremento dei rischi per la sicurezza.

Dal punto di vista operativo, i primi sei mesi del 2004 sono cruciali, per l'analisi e l'adozione delle nuove misure di sicurezza, in quanto **entro il 30 giugno 2004**(oggi prorogato al 31 dicembre):

- in generale, tutti i soggetti che trattano dati personali devono completare il processo di adozione delle misure introdotte dal Dlgs 196/2003
- nel caso particolare, in cui al 31 dicembre 2003 si fossero posseduti strumenti elettronici tecnicamente inadeguati, si deve provvedere ad attestare tale fatto, per beneficiare del più lungo termine del 31 dicembre 2004 per completare il processo di adeguamento
- in ogni caso, tutti i soggetti che trattano dati sensibili o giudiziari con strumenti elettronici devono redigere per la prima volta, o aggiornare, il Documento programmatico sulla sicurezza.

Il presente manuale approfondisce tutti gli aspetti, legati al nuovo quadro normativo, per illustrare in modo semplice ed immediato:

- ***tutte le misure***, previste dal nuovo disciplinare tecnico in materia di misure minime di sicurezza
- quali misure sono ***nuove***, rispetto a quanto era previsto dall'abrogando Dpr 318/1999: i soggetti che trattano dati personali possono in tale modo capire ***cosa cambia***, e prendere di conseguenza le opportune decisioni, in materia di tutela della sicurezza nella tutela dei dati personali
- ***quali documenti redigere entro il 30 giugno 2004***(oggi prorogato al 31 dicembre)
- ***come redigere tali documenti***, fornendo tra l'altro una bozza su file elettronico, copiabile, personalizzabile e stampabile:
  - del **documento avente data certa**, che può essere redatto dai soggetti che, possedendo al 31 dicembre 2003 strumenti elettronici tecnicamente inadeguati, intendono avvalersi del più lungo termine del 31 dicembre 2004, entro cui adottare le nuove misure di sicurezza introdotte dal Dlgs 196/2003
  - del **Documento programmatico sulla sicurezza**, redatto secondo i nuovi criteri previsti dal Dlgs 196/2003.

8.1 Quadro generale

Non c'è privacy senza sicurezza.
Raramente si riesce ad esprimere con tanta sintesi ed efficacia un concetto estremamente importante: a nulla serve essere estremamente scrupolosi nel trattamento dei dati, inviando informative, acquisendo consensi ed autorizzazioni, aggiornandoli con maniacale puntualità, se si lasciano poi i supporti contenenti i dati incustoditi sulla scrivania, alla mercé di chiunque possa entrare nell'ufficio.

Non a caso si è introdotto un esempio che prescinde dal trattamento informatico: la questione sicurezza non riguarda infatti i soli dati trattati elettronicamente. Tale aspetto è oggi certo di primaria importanza, in virtù dell'invasione del mondo virtuale, ma non è l'unico.
La sicurezza si ottiene anche con l'uso dei vecchi lucchetti e delle pesantissime casseforti, e con la vigilanza sulle strutture esterne.

Ma non ci si può fermare neppure qui, perché si è finora parlato delle ***misure di sicurezza fisiche***, accennato a quelle ***logiche legate all'informatica***, ma si è dimenticato l'aspetto più importante: le ***misure organizzative***, il cui fine è di fare in modo che l'intera struttura adotti comportamenti conformi ai principi della sicurezza e, più in generale, della privacy.

Molti ricorderanno l'infortunio in cui è incorso il Ministero delle Finanze, allorché predispose una busta per contenere la dichiarazione *Unico 98* che recava un'ampia finestra, non protetta da pellicola trasparente, tale da permettere a chiunque maneggiasse la busta di prendere facilmente visione dell'intero frontespizio della dichiarazione e dei dati personali ivi riportati, compresi quelli idonei a rivelare dati sensibili concernenti la destinazione dell'otto e del quattro per mille dell'IRPEF.
Da cosa è derivata questa palese violazione della sicurezza ? non certo da una carenza nelle misure di sicurezza fisiche, né tantomeno logiche. Semplicemente dal fatto che chi al Ministero sapeva di privacy, e saranno stati verosimilmente in molti, non è entrato in contatto con chi ha concepito e realizzato le buste per conto del Ministero stesso: quindi da una **carenza organizzativa.**

Sotto un altro aspetto, non si deve pensare che l'obbligo di adottare le misure di sicurezza, in relazione al trattamento dei dati personali, riguardi solo le imprese e, più in generale, le organizzazioni di rilevanti dimensioni: lungi dall'essere limitato a pochi soggetti, tale obbligo è invece ***generalizzato***, sino al punto da estendersi anche a coloro che trattano tali dati per *fini esclusivamente personali*. A tale proposito, l'articolo 5 del nuovo codice privacy ribadisce infatti che, anche in questi casi, trovano

applicazione le disposizioni in tema di responsabilità per danni (articolo 15) e di sicurezza dei dati (articolo 31).

Cosa deve garantire la sicurezza

NUOVO CODICE	L 675/1996
31[1] Ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati personali oggetto di trattamento, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.	**15[1]** Ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati personali oggetto di trattamento, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

L'articolo 31 del nuovo codice conferma che la sicurezza dei dati è considerata un aspetto fondamentale del sistema-privacy, ribadendo la prescrizione per cui è obbligatorio *adottare in via preventiva* misure che *riducano al minimo* i rischi di:

- **distruzione o perdita, anche accidentale, dei dati**: nel mondo fisico è facile pensare ad un incendio, piuttosto che ad una agendina persa in metropolitana. Nel mondo informatico si ricorre la concetto di ***disponibilità del dato***: si deve impedire che dati, informazioni e risorse siano resi irreperibili da persone, mediante processi non autorizzati, o da eventi accidentali. In tale ambito assume inoltre una particolare valenza il requisito della ***integrità del dato***, che deve essere quello originario o legittimamente modificato, in relazione alla relativa facilità di procedere fraudolentemente a modifiche senza lasciare indizi
- **accesso non autorizzato ai dati**: nel mondo fisico è immediato pensare ad estranei, che nella notte si introducono in un'azienda per rubare dei dati o farne delle copie, piuttosto che a personale dell'azienda stessa che viola determinati archivi durante l'orario di lavoro. Nel mondo informatico si parla di ***confidenzialità*** o ***riservatezza,*** con ciò intendendosi che un determinato dato deve essere accessibile solo a chi è autorizzato: si dovrà quindi fare in modo che il personale non possa consultare files che non lo riguardano; che estranei non possano accedere abusivamente al sistema informativo, con un'azione analoga a quella dello spione notturno che apre le porte con il passpartout e disattiva il sistema d'allarme; che durante la trasmissione di dati da un computer ad un altro, dislocato magari all'altro capo del mondo, novelli briganti armati di computer invece che di spadone non intercettino i messaggi per violare le informazioni in essi contenuti. Correlato a tali aspetti vi è il requisito della ***autenticità*** dei dati, che concerne la garanzia e certificazione della loro provenienza

- **trattamento non consentito o non conforme alle finalità della raccolta**.

Si noti che la legge parla realisticamente di **riduzione al minimo**, non di eliminazione dei rischi, nella consapevolezza che il raggiungimento di tale assoluto obiettivo è di fatto impossibile.
Questa considerazione induce a formulare una importante riflessione: la sicurezza non deve essere intesa solo come *protezione* da eventi negativi, accidentali o intenzionali, ma anche come *limitazione degli effetti causati dall'eventuale verificarsi di tali eventi.*
Nel realizzare i sistemi di sicurezza non ci si dovrà quindi preoccupare solo della porta blindata, che ha il fine di impedire ai ladri di entrare nell'appartamento, ma anche di nascondere bene all'interno dello stesso gli ori di famiglia, per minimizzare gli effetti negativi che potrebbero conseguire da una eventuale violazione.
In un'azienda ciò potrebbe assumere il significato di impedire che, anche nell'ipotesi in cui un attacco informatico abbia successo, e quindi la porta blindata venga sfondata, gli invasori possano reperire i codici delle carte di credito dei clienti, cioè gli ori dell'azienda che ha subito l'attacco.

Il nuovo codice ripropone la tradizionale distinzione tra:

- le cosiddette ***misure idonee*** (*Capo I del Titolo V della parte I*), che consistono in generale nell'insieme degli accorgimenti che il soggetto che tratta i dati deve adottare, in relazione alla sua specifica situazione, in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. Dalla mancata adozione, di tali misure, consegue l'obbligo di risarcimento dei danni eventualmente causati
- all'interno di quelle che, in generale, possono essere le misure idonee, vengono individuate le ***misure minime*** (*Capo II del Titolo V della parte I*), che il comma 3, lettera a) dell'articolo 4 definisce come *il complesso delle misure tecniche, informatiche, organizzative, logistiche* (leggasi *logiche,* NdR) *e procedurali di sicurezza che configurano il livello minimo di protezione*, richiesto in relazione ai rischi previsti nell'articolo 31. La loro adozione è imposta dalla norma, che provvede a descriverle analiticamente, con la conseguenza che sono previste sanzioni di natura penale, in caso di mancata adozione.

8.2 Le *misure idonee* di sicurezza

NUOVO CODICE	L 675/1996
31[1] I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.	**15[1]** I dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

L'obbligo di adottare le misure di sicurezza è ribadito dall'articolo 31 del nuovo codice, che disciplina quelle che sono comunemente definite le ***misure idonee di sicurezza***, in merito alle quali la relazione al precedente Dpr 318/1999 sottolinea che "la norma impone al titolare e al responsabile, se designato, l'obbligo di custodire e controllare i dati personali oggetto di trattamento mediante l'adozione di idonee e preventive misure di sicurezza, individuabili alla luce delle conoscenza acquisite in base al progresso tecnico in relazione alla natura dei dati ed alle specifiche caratteristiche del trattamento, in grado di ridurre al minimo i rischi. Si tratta in sostanza dell'obbligo di operare in concreto al fine di ridurre al minimo i rischi mediante l'utilizzazione di sistemi di sicurezza *costantemente adeguati nel tempo*".

Le misure idonee sono quindi "*non individuate*, ma *individuabili* sulla base delle soluzioni tecniche concretamente disponibili, e la loro mancata predisposizione comporta la responsabilità per i danni eventualmente cagionati".

8.2.1 La natura dei dati e le caratteristiche del trattamento

Una prima osservazione concerne il fatto che viene preteso un *diverso grado di diligenza*, che varia in funzione della *natura dei dati* e delle *specifiche caratteristiche* del trattamento.
E' ovvio che, per custodire un banale elenco di dati anagrafici di taluni abitanti di una città, non è necessario l'uso di una cassaforte con dieci combinazioni, né l'adozione di altro accorgimento, che non sia di riporre l'elenco nel cassetto dotato della solita finta serraturina di finto metallo. Chi custodisce un elenco contenente nomi cognomi ed indirizzi di persone affette da gravi problemi di salute, con dovizia descritti, è invece tenuto ad adottare più efficaci accorgimenti, a salvaguardia della sicurezza.

8.2.2 La classificazione delle misure di sicurezza

L'insieme delle misure di sicurezza viene concettualmente suddiviso in tre sottoinsiemi, distinguendo le *misure*:

- *organizzative*, che si sostanziano nella definizione di una serie di norme e procedure, miranti a regolamentare l'aspetto organizzativo del processo di sicurezza. A titolo esemplificativo, si riportano le misure prestampate nel *vecchio* modello di notifica al Garante:
  - analisi dei rischi
  - prescrizione di linee – guida di sicurezza e altre istruzioni interne
  - assegnazione di incarichi e redazione di appositi mansionari
  - formazione professionale
  - classificazione dei dati
  - registrazione delle consultazioni
  - documentazione dei controlli periodici
  - verifiche periodiche su dati o trattamenti non consentiti o non corretti
  - distruzione controllata dei supporti
  - piano di *disaster recovery*

- *fisiche,* il cui scopo è di proteggere le aree, le apparecchiature, i dati e le persone da eventi di natura accidentale (es. incendi) e da intrusioni, di personale non autorizzato o di terzi. Nel *vecchio* modello di notifica al Garante sono prestampate le seguenti misure:
  - vigilanza della sede
  - ingresso controllato nei locali ove ha luogo il trattamento
  - sistemi di allarme e/o di sorveglianza antintrusione
  - registrazione degli accessi
  - autenticazione degli accessi
  - custodia in classificatori o armadi non accessibili
  - custodia in armadi blindati e/o ignifughi o deposito in cassaforte
  - custodia dei supporti in contenitori sigillati
  - dispositivi antincendio
  - continuità dell'alimentazione elettrica
  - controllo sull'operato degli addetti alla manutenzione
  - verifica della leggibilità dei supporti
- *logiche*, il cui campo di applicazione riguarda la protezione delle informazioni, con particolare riferimento a quelle gestite con i sistemi informativi (dati, applicazioni, sistemi e reti), sia in relazione al loro corretto utilizzo, che in relazione alla loro gestione e manutenzione nel tempo. Nel *vecchio* modello di notifica al Garante sono prestampate le seguenti misure:
  - identificazione dell'incaricato e/o dell'utente
  - autenticazione dell'incaricato e/o dell'utente
  - controllo degli accessi a dati e programmi
  - registrazione degli accessi
  - controlli aggiornati antivirus
  - sottoscrizione elettronica
  - cifratura dei dati memorizzati e/o di quelli trasmessi
  - annotazione della fonte dei dati
  - annotazione del responsabile dell'operazione
  - rilevazione di intercettazioni
  - monitoraggio continuo delle sessioni di lavoro
  - sospensione automatica delle sessioni di lavoro
  - verifiche periodiche su dati o trattamenti non consentiti o non corretti
  - verifiche automatizzate dei requisiti dei dati
  - controllo sull'operato degli addetti alla manutenzione
  - controllo dei supporti consegnati in manutenzione.

8.2.3 L'aggiornamento delle misure di sicurezza

In merito alle misure che si devono in concreto adottare, il testo legislativo si limita genericamente a prevedere che si debbano applicare gli strumenti e le conoscenze resi disponibili dal *progresso tecnico*: non è quindi sufficiente impiantare una serie di misure di sicurezza una volta per tutte, ma ci si deve preoccupare di *aggiornarle costantemente*.

Tale principio, che è generale e vale quindi per tutte le misure di sicurezza, incluse quelle *fisiche* in senso stretto, assume particolare rilievo per le misure logiche legate al mondo informatico, in relazione al continuo progresso cui esso è soggetto, anche per quanto riguarda la creazione e circolazione di programmi concepiti per violare la altrui sicurezza.

8.2.4 Il risarcimento per danni

NUOVO CODICE	L 675/1996
15[1] Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.	**18[1]** Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.
15[2] Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.	**29[9]** Il danno non patrimoniale è risarcibile anche nei casi di violazione dell'articolo 9.

Se dalla mancata od insufficiente adozione di idonee misure di sicurezza derivano danni a terzi, si è soggetti all'obbligazione del risarcimento, secondo i termini particolarmente severi previsti dal sistema - privacy.
Il risarcimento dei danni, causati ad altri per effetto del trattamento di dati personali, è disciplinato dal combinato disposto delle seguenti norme:
Articolo 15 comma 1 codice privacy: *Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.*

*Articolo 2050 c.c. - Responsabilità per l'esercizio di attività pericolose****:*** ***Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee ad evitare il danno.***

*Articolo 2059 c.c. - Danni non patrimoniali****: Il danno non patrimoniale deve essere risarcito solo nei casi determinati dalla legge.***
*Articolo 15 comma 2 codice privacy****: Il danno non patrimoniale è risarcibile anche nei casi di violazione dell'articolo 11 (modalità del trattamento e requisiti dei dati personali).***

Si sottolinea che, ai fini della responsabilità civile, **non è sufficiente** porre in essere le misure di sicurezza *minime* previste dall'articolo 33 del codice, che sono invece sufficienti per non incorrere nelle disposizioni penali, ma si deve adottare ***misure idonee***, con riferimento allo stato della tecnologia.

8.2.4.1 I danni patrimoniali

Dal tenore letterale della norma emerge che chiunque è responsabile, dei danni che ha causato, trattando dati personali: tale disposizione trova applicazione *anche per chi tratta i dati per fini esclusivamente personali.* Se ad esempio si perde una agendina in metropolitana, contenente i dati di una persona, e tale persona riceve un danno dall'uso che di tali dati fa chi ha trovato l'agendina, chi l'ha smarrita è tenuto al risarcimento.
A maggiore ragione, la disposizione colpisce direttamente chiunque, nell'ambito dei soggetti che trattano dati personali, per fini diversi da quelli prettamente personali, causi danni ad altri: non solo titolari, responsabili ed incaricati del trattamento, ma anche le persone che trattino i dati senza averne ufficialmente titolo.

Per quanto concerne i confini della responsabilità, l'espresso richiamo fatto dall'articolo 15 comma 1 all'articolo 2050 c.c., pur non intendendo classificare il trattamento dei dati come "attività pericolosa", rende applicabile ad esso i *criteri di risarcimento* previsti dall'articolo 2050 c.c.
Il che significa innanzitutto che ci si trova nel campo della responsabilità oggettiva, per cui il titolare del trattamento *non risponde solo dei danni causati direttamente*, ma anche di quelli provocati dalla sua organizzazione: in tale contesto, è pacifico che il titolare risponda dell'operato dei suoi dipendenti, siano essi responsabili o incaricati del trattamento, o lo pongano in atto senza avere alcun titolo. Ad esempio, un'impresa risponde dei danni causati dalla fuga di dati personali non solo se essa è avvenuta per mano del direttore EDP, nominato dall'impresa quale responsabile del trattamento, ma anche se tali dati sono stati trafugati dal fattorino, che è riuscito a violare il sistema di sicurezza e ad impossessarsene.

Più controversa è la questione, se il titolare risponda dei danni provocati da un "responsabile esterno", regolarmente nominato: l'opinione corrente è che anche in questo caso si configuri una responsabilità sussidiaria del titolare.
Il richiamo all'articolo 2050 c.c. introduce altri elementi gravosi, per chi tratta i dati, quali:

- l'inversione dell'onere della prova: chi ha subito il danno *non deve provare* la responsabilità oggettiva del titolare del trattamento, ma toccherà a questi provare di avere adottato *tutte le misure idonee* ad evitare il danno
- la limitazione della prova: la portata della norma va oltre l'inversione dell'onere della prova, poiché essa non considera sufficiente la prova di avere adottato le misure ragionevolmente imposte dalla diligenza, ma richiede la prova di avere adottato *tutte le misure di sicurezza offerte dalla tecnica*. La norma dispone quindi una responsabilità per qualsiasi

danno oggettivamente evitabile, in base allo stato della tecnica al momento in cui l'evento che ha causato il danno si è verificato.

8.2.4.2 Il danno non patrimoniale

Per i trattamenti che integrano la violazione dell'articolo 11 *(modalità del trattamento e requisiti dei dati personali*) è prevista la risarcibilità non solo del danno patrimoniale, ma anche del **danno non patrimoniale** sofferto dal soggetto interessato: esso consiste in un danno biologico di natura psichica, che si concretizza in sofferenze, patemi, risentimento, compressioni o turbamenti della personalità, dolore. Si ricorda che l'articolo 11 è il *cuore della privacy*, che la carenza di idonee misure di sicurezza *può portare di fatto a violare:* in esso sono contenuti i principi di finalità, di esattezza, di pertinenza, di non eccedenza, l'obbligo dell'aggiornamento dei dati e il diritto all'oblio.

Si supponga che, a causa della carenza delle misure di sicurezza adottate da un ospedale, venga trafugata una cartella dalla quale emerge che una persona è affetta da virus HIV, e che in relazione a tale informazione tale persona venga molestata e ricattata da chi si è fraudolentemente impossessato della cartella: l'ospedale risponderà anche del danno non patrimoniale, a nulla valendo il fatto di non essere l'autore diretto di molestie e ricatti.

L'attuale tendenza giurisprudenziale è di accordare *cospicui risarcimenti*, a fronte dei danni non patrimoniali: ciò avviene anche perché la determinazione del *quantum* è fatalmente rimessa al discrezionale apprezzamento del giudice, a causa dell'impossibilità di riferirsi a parametri materiali di valutazione.

8.2.5 Le regole per i fornitori di servizi di comunicazione elettronica

NUOVO CODICE	DLGS 171/1998
32[1] Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico adotta ai sensi dell'articolo 31 idonee misure tecniche e organizzative adeguate al rischio esistente, per salvaguardare la sicurezza dei suoi servizi, *l'integrità dei dati relativi al traffico, dei dati relativi all'ubicazione e delle comunicazioni elettroniche rispetto ad ogni forma di utilizzazione o cognizione non consentita.*	**2[1]** Il fornitore di un servizio di telecomunicazioni accessibile al pubblico adotta le misure tecniche ed organizzative di cui all'articolo 15, comma 1, della legge per salvaguardare la sicurezza del servizio e dei dati personali.
32[2] Quando la sicurezza del servizio o dei dati personali richiede anche l'adozione di misure che riguardano la rete, il fornitore del servizio di comunicazione elettronica accessibile al pubblico adotta tali misure congiuntamente con il fornitore della rete pubblica di comunicazioni. In caso di mancato accordo, su richiesta di uno dei fornitori, la controversia è definita dall'Autorità per le garanzie nelle comunicazioni *secondo le modalità previste dalla normativa vigente.*	**2[2]** Quando la sicurezza del servizio o dei dati personali richiede anche l'adozione di misure che riguardano la rete, il fornitore del servizio le adotta congiuntamente con il fornitore della rete pubblica di telecomunicazioni. In caso di mancato accordo, su richiesta di uno dei fornitori, la controversia è definita dall'Autorità per le garanzie nelle comunicazioni, *ai sensi dell'articolo 18 del decreto del Presidente della Repubblica 19 settembre 1997, n. 318, sentito il Garante.*
32[3] Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico informa gli abbonati *e, ove possibile, gli utenti*, se sussiste un particolare rischio di violazione della sicurezza della rete, indicando, *quando il rischio è al di fuori dell'ambito di applicazione delle misure che il fornitore stesso è tenuto ad adottare ai sensi dei commi 1 e 2*, tutti i possibili rimedi e i relativi costi presumibili. Analoga informativa è resa al Garante e all'Autorità per le garanzie nelle comunicazioni.	**2[3]** Il fornitore di un servizio di telecomunicazioni accessibile al pubblico ha l'obbligo di informare gli abbonati quando sussiste un particolare rischio di violazione della sicurezza della rete, indicando i possibili rimedi e i relativi costi. Analoga informativa è resa all'Autorità per le garanzie nelle comunicazioni e al Garante.

Il codice ripropone nella sostanza una norma, in precedenza presente nel Dlgs 171/1998, atta a delineare i particolari obiettivi che, in termini di sicurezza, devono essere perseguiti dai fornitori di un **servizio di comunicazione elettronica accessibile al pubblico** (ad esempio, compagnie telefoniche, piuttosto che fornitori di accessi ad Internet), anche congiuntamente con i soggetti che gestiscono la rete pubblica di comunicazioni, della quale si avvalgono per offrire i propri servizi.

Il comma 1 precisa innanzitutto che, nell'ambito delle complessive misure idonee di sicurezza, che devono essere adottate, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico deve dedicare una particolare attenzione a quelle atte a salvaguardare, dalle forme di utilizzazione o cognizione non consentite:

- la sicurezza dei **servizi offerti** al pubblico
- l'integrità dei **dati relativi al traffico**: con tale termine si intende *qualsiasi dato sottoposto a trattamento, ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione*
- l'integrità dei **dati relativi all'ubicazione**: con tale termine si intende *ogni dato trattato in una rete di comunicazione elettronica, che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico*
- l'integrità delle **comunicazioni elettroniche**.

Come corollario, il comma 3 impone al fornitore il **dovere di informare**, in ogni caso gli abbonati e, ove possibile, gli utenti (cioè coloro che di fatto utilizzano il servizio, indipendentemente dalla qualità di abbonato), circa l'esistenza di **particolari rischi di violazione della sicurezza della rete**.
In tale informativa, che deve essere *resa per conoscenza* anche al Garante e all'Autorità per le garanzie nelle comunicazioni, il fornitore deve precisare:

- se, ed in quale misura, prende direttamente in carico la adozione dei sistemi di sicurezza, necessari al fine di fronteggiare i rischi in esame, eventualmente in collaborazione con il fornitore della rete di comunicazioni
- per quanto concerne i rischi, a fronte dei quali il fornitore non è invece tenuto a prendere direttamente in carico la adozione dei sistemi sicurezza, tutti i possibili rimedi, ed i relativi costi presumibili.

Il secondo comma dell'articolo 32 prevede infine che, quando la sicurezza del servizio o dei dati personali richiede anche l'adozione di **misure che riguardano la rete**, il fornitore del servizio di comunicazione elettronica accessibile al pubblico deve adottare tali misure *congiuntamente* con il fornitore della rete pubblica di comunicazioni: nel caso in cui tali soggetti non dovessero raggiungere un accordo, la controversia è definita dall'Autorità per le garanzie nelle comunicazioni, su richiesta di uno dei fornitori in esame.

8.3 Le misure minime di sicurezza

NUOVO CODICE	DPR 318/1999
4[3a] Si intende per “misure minime” il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza, che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti *nell’articolo 31*.	**1[1a]** Si intende per "misure minime" il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza, che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti *dall'articolo 15, comma 1, della L 675/1996*
NUOVO CODICE	**L 675/1996**
33[1] *Nel quadro dei più generali obblighi di sicurezza di cui all’articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell’articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.*	**15[2]** *Le misure minime di sicurezza da adot**t**are in via preventiva sono individuate con regolamento emanato con decreto del Presidente della Repubblica, ai sensi dell'articolo 17, comma 1, lettera a), della legge 23 agosto 1988, n. 400, entro centottanta giorni dalla data di entrata in vigore della presente legge, su proposta del Ministro di grazia e giustizia, sentiti l'Autorità per l'informatica nella pubblica amministrazione e il Garante.*

Mentre per le misure idonee di sicurezza il legislatore impone le linee guida generali, disegnando in parallelo il sistema di responsabilità, ma non entra nel merito delle misure che devono essere in concreto adottate, la normativa entra molto più nei dettagli delle cosiddette *misure minime di sicurezza*, che la relazione al precedente Dpr 318/1999 definisce *quei requisiti minimi di sicurezza, la cui violazione costituisce la sicura esposizione a rischio del bene-privacy protetto dalle norme*. Violazioni *alla presenza delle quali, per la loro assoluta contraddizione con i requisiti minimi ormai generalmente riconosciuti, si deve ritenere che si verifichi un livello non tollerabile di rischio di lesione del diritto alla tutela dei dati personali, e quindi tali da giustificare l’adozione di un apparato sanzionatorio penale*.

Il nuovo codice privacy **ridisegna** la mappa delle misure minime di sicurezza, nei seguenti termini:

- il codice si limita ad imporre, nell'articolo 33, l'obbligo per tutti i soggetti che trattano dati personali di adottare le misure minime, richiamando inoltre quanto dispone l'articolo 58, sulle particolari misure di sicurezza, che i *servizi di informazione e sicurezza* (di cui all'articolo 58 comma 1: CESIS, SISMI, SISDE) sono tenuti ad adottare
- le concrete misure, che devono essere adottate, sono individuate, nella generalità dei casi, da un *disciplinare tecnico*, che costituisce l'*Allegato B)* del codice privacy. Tale disciplinare è aggiornato periodicamente, con decreto del Ministro della giustizia, di concerto con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore
- le concrete misure, che devono essere adottate dai *servizi di informazione e sicurezza*, di cui all'articolo 58 (CESIS, SISMI, SISDE), sono invece stabilite e periodicamente aggiornate con decreto del Presidente del Consiglio dei Ministri.

8.3.1 L'aggiornamento delle misure minime

NUOVO CODICE	L 675/1996
36[1] *Il disciplinare tecnico di cui all'allegato B), relativo alle misure minime di cui al presente capo, è aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.*	**15[3]** *Le misure di sicurezza di cui al comma 2 sono adeguate, entro due anni dalla data di entrata in vigore della presente legge e successivamente con cadenza almeno biennale, con successivi regolamenti emanati con le modalità di cui al medesimo comma 2, in relazione all'evoluzione tecnica del settore e all'esperienza maturata.*

Nel commentare le nuove disposizioni in merito alla cadenza, con cui il *disciplinare tecnico* deve essere aggiornato, viene spontaneo tirare un sospiro di sollievo, constatando che ora è semplicemente previsto che l'aggiornamento sia *periodico*, *in relazione all'evoluzione tecnica e all'esperienza maturata nel settore*

Il legislatore, o chi per esso, non sarà quindi più assoggettato alle *pessime figure*, alle quali è stato esposto in vigenza della precedente formulazione, che imponeva l'aggiornamento biennale delle misure minime di sicurezza (scadenza, ovviamente, mai rispettata in sette anni di legislazione privacy, nel corso dei quali l'unico provvedimento intervenuto è il Dpr 318/1999, che con l'entrata in vigore del codice privacy viene abrogato, per fare posto alle nuove disposizioni).

8.3.2 Le sanzioni penali per la omessa adozione delle *misure minime*

NUOVO CODICE	L 675/1996
169[1] Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni o con l'ammenda *da diecimila euro a cinquantamila euro.*	**36[1]** Chiunque, essendovi tenuto, omette di adottare le misure necessarie a garantire la sicurezza dei dati personali, in violazione delle disposizioni dei regolamenti di cui ai commi 2 e 3 dell'articolo 15, è punito con l'arresto sino a due anni o con l'ammenda *da lire dieci milioni a lire ottanta milioni.*
169[2] All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili.	**36[2]** All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, in quanto applicabili.

Il nuovo codice conferma la disciplina sanzionatoria, in precedenza innovata, rispetto alle disposizioni originarie della L.675/1996, dal Dlgs 467/2001, ai sensi della quale la mancata adozione delle misure minime di sicurezza è punita come segue:

- la sanzione penale non consiste più esclusivamente nella reclusione, come avveniva sino al 31 gennaio 2002, ma si può *in alternativa* optare per l'ammenda
- all'autore del reato viene concessa la facoltà di *mettersi in regola*, con l'adozione delle prescritte misure di sicurezza, pagando una ammenda ridotta ed ottenendo il beneficio dell'estinzione del reato.

8.3.2.1 L'evoluzione delle sanzioni

E' importante osservare che, affinché scattino le sanzioni penali, *è sufficiente che vi sia omissione*, nell'adozione delle misure di sicurezza, senza che dal fatto debba concretamente derivare un danno per i terzi; l'omessa adozione delle misure di sicurezza è inoltre punita anche se il fatto è commesso semplicemente per colpa, e cioè per imprudenza, imperizia, negligenza, inosservanza di leggi, regolamenti, ordini e discipline.

Ciò premesso, si evidenzia che la norma punisce *chiunque, essendovi tenuto, omette di adottare le misure minime, volte ad assicurare un livello minimo di protezione dei dati personali*.

In origine, il reato era punito con la reclusione *sino ad un anno*, che saliva *da due mesi a due anni*, nei casi in cui dal fatto fosse derivato nocumento. In ogni caso, se il fatto era commesso per colpa, si applicava la pena meno severa della reclusione *fino ad un anno*.

La versione *in vigore dal 1° febbraio 2002* ha affiancato, alla generalizzata previsione dell'arresto *sino a due anni*, mantenuta dal codice privacy, la ***facoltà di optare*** per l'ammenda: tale ammenda è stata incrementata, dal codice privacy, e diviene ora *da diecimila euro a cinquantamila euro*.

8.3.2.2 Il ravvedimento operoso

Il secondo comma prevede che all'autore del reato, all'atto dell'accertamento dello stesso o, nei casi complessi, anche con successivo atto del Garante, venga impartita una prescrizione, ***fissando un termine*** per adottare le prescritte misure minime di sicurezza. Tale termine non può eccedere il periodo di tempo tecnicamente necessario, per adottare le misure minime di sicurezza richieste, che è prorogabile solo in caso di particolare complessità o per oggettive difficoltà dell'adempimento. Il termine non può in ogni caso essere superiore a sei mesi.

Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento della prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari ad un quarto del massimo dell'ammenda stabilita per la contravvenzione (quindi ***euro 12.500***).

8.3.2.3 I soggetti interessati

Chi è tenuto ad adottare le misure minime di sicurezza, e quindi è passibile di subire le sanzioni per le eventuali omissioni? Il *titolare del trattamento* e/o chi è da questi nominato *responsabile*, in una misura diversa in relazione al contenuto dell'incarico.

È innanzitutto facoltà del titolare *provvedere direttamente* alla realizzazione delle misure di sicurezza ed al monitoraggio quotidiano del loro funzionamento: in questi casi, nella lettera di nomina di eventuali responsabili si escluderebbe qualsiasi coinvolgimento nella realizzazione delle misure di sicurezza, per cui i responsabili stessi non sarebbero passibili di sanzioni.

Ma questo è un caso raro: nella realtà i responsabili vengono nominati soprattutto per le loro competenze tecniche, con particolare riguardo alla sicurezza (lo stesso articolo 29 del codice privacy, elencando i requisiti che deve possedere il responsabile del trattamento, fa esplicito riferimento alle competenze in merito al profilo della sicurezza). In tali casi i responsabili *rispondono in prima persona* delle omissioni penalmente sanzionate. Ed i titolari? anche se in questi casi essi hanno provveduto a nominare un responsabile, con ampia delega in materia di sicurezza, si può tuttavia configurare una loro *corresponsabilità*, la cui misura deve essere valutata in base alle circostanze concrete:

- si supponga che il titolare delle Brambilla Sas, il noto Commendator Brambilla, abbia una capacità eccezionale nel produrre stupendi articoli artigianali, ma rifiuti per partito preso di prendere in mano una penna. Persona diligente, sentendo parlare della privacy decide di nominare una primaria casa di software come responsabile del processo di sicurezza, conscio che all'interno della Brambilla sas nessuno capisce alcunché delle diavolerie del giorno d'oggi. In questo caso, è palese che della omessa adozione delle misure di sicurezza risponderebbe penalmente il solo responsabile, la casa di software, non potendosi pretendere dal Commendator Brambilla altra diligenza, che non sia quella di sborsare svariate migliaia di euro l'anno per avere un supporto tecnico di eccellenza.

  A questa conclusione, già pacifica in vigenza della precedente normativa, il nuovo codice offre un decisivo elemento di supporto: il punto 25. del disciplinare tecnico in materia di misure minime di sicurezza prevede infatti che *il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione, riceve dall'installatore una descrizione scritta dell'intervento effettuato, che ne attesta la conformità alle disposizioni del presente disciplinare tecnico*. Della eventuale mancata adozione delle misure minime, previste dal disciplinare tecnico, viene quindi a rispondere in prima persona il soggetto esterno, che ha provveduto alla esecuzione ed installazione delle misure di sicurezza

- e se invece titolare del trattamento fosse una primaria casa di software, che abbia provveduto a nominare responsabile, con la più ampia gamma di incarichi – ivi inclusa l'intera problematica della sicurezza – l'ultimo e più sbarbato programmatore assunto, fresco uscito dalla scuola? In questo caso, ferme restando le responsabilità dello sbarbato, che ha accettato un incarico pur non avendo le competenze necessarie, anche la casa di software sarebbe chiamata penalmente in causa, in qualità di titolare che ha peccato di diligenza nella nomina del responsabile.

In generale, per valutare in che misura la delega può considerarsi effettiva, ponendo quindi il titolare delegante al riparo dalle sanzioni penali, occorre valutare le circostanze concrete, tra le quali si segnalano per rilevanza:

- il fatto che si tratti di imprese di grosse dimensioni
- il fatto che al delegato vengano attribuite tutte le risorse necessarie all'espletamento delle funzioni e venga concessa autonomia organizzativa
- il fatto che i soggetti delegati possiedano una provata competenza tecnica: sotto tale aspetto, l'attribuzione delle funzioni non deve avere finalità elusive e fraudolenti.

9 Definizione di compiti, ruoli e procedure

Il processo della sicurezza richiede che, prima ancora di pensare all'adozione delle concrete misure, vengano definite una serie di norme e procedure, miranti a regolamentare gli aspetti organizzativi del processo medesimo, con riferimento:

- alla **definizione di ruoli**, compiti e responsabilità per la gestione di tutte le fasi del trattamento dei dati personali, con particolare riferimento alla necessità di garantire la loro sicurezza
- alla adozione di specifiche **procedure**, che vadano a completare e rafforzare le contromisure tecnologiche adottate.

La prima e più generalizzata misura di sicurezza è quindi prettamente ***di carattere organizzativo***: tale precetto è talmente rilevante che, anche in vigenza della precedente normativa, lo stesso legislatore non si è limitato ad imporre ai soggetti che trattano dati personali determinati adempimenti, ma si è spinto sino al punto di disciplinare *chi debba fare che cosa*, e quali responsabilità conseguentemente abbia, introducendo *ex lege* alcune figure organizzative, con riferimento al trattamento dei dati personali.

Il nuovo codice privacy accentua ulteriormente tali aspetti, perché con gli articoli 34 e 35 qualifica come misura minima di sicurezza, che deve quindi essere obbligatoriamente adottata da tutti i soggetti che trattano dati personali, l'**aggiornamento periodico dell'individuazione** dell'ambito di trattamento consentito:

- **ai singoli incaricati**, indipendentemente dal fatto che il trattamento avvenga o meno con l'utilizzo di strumenti elettronici
- agli **addetti alla gestione o manutenzione** degli strumenti elettronici.

Nel presente capitolo si esaminano i ruoli, previsti dalla normativa privacy, di ***titolare***, ***responsabile*** ed ***incaricato*** del trattamento: in tale contesto, una particolare attenzione verrà dedicata alle figure specificamente introdotte dalla normativa sulla sicurezza.
Successivamente, si analizzano le implicazioni legate alla necessità di redigere, e di aggiornare periodicamente, un vero e proprio *mansionario privacy*.

9.1 Il titolare del trattamento

NUOVO CODICE
4[1f] Ai fini del codice privacy si intende per "titolare" la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. **28[1]** Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.

La lettera f) del comma 1 dell'articolo 4 definisce come titolare *la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza*.
Da questa definizione si comprende immediatamente come al titolare spetti, per presunzione assoluta di legge, la **direzione delle attività di trattamento dei dati personali**: a tale soggetto competono infatti le decisioni strategiche di fondo su *come* (*modalità*) e *perché* (*finalità*) raccogliere e trattare i dati, nonché sull'*organizzazione* del trattamento e *sulle risorse (strumenti) da dedicarvi*, anche per garantire la *sicurezza*.
Il titolare si identifica con la persona fisica, la persona giuridica, la pubblica amministrazione o qualsiasi altro ente, associazione od organismo cui **oggettivamente** spettano tali decisioni di fondo: valga l'esempio della ditta individuale Brambilla, dove notoriamente non si muove foglia che il Commendatore non voglia. Il Comm. Brambilla, volente o nolente, è il titolare del trattamento, e non potrà delegare in alcun modo le responsabilità insite in tale ruolo, neppure adducendo il fatto di non avere mai visto un computer.

Al fine di individuare, nelle situazioni concrete, chi venga dalla legge considerato come titolare, il Garante ha fornito alcuni importanti chiarimenti, alcuni dei quali sono stati ufficialmente recepiti dal nuovo codice privacy:

- una persona fisica è titolare quando effettua un trattamento *in proprio* (es. un imprenditore individuale o un libero professionista) e non, ad esempio, quando agisce in qualità di amministratore o rappresentante di una persona giuridica
- nel caso in cui il trattamento sia effettuato da una persona giuridica o da qualsiasi altro ente, associazione od organismo, per titolare va intesa l'*entità nel suo complesso* (es. l'impresa, la società, l'associazione), e non la persona fisica che l'amministra o la rappresenta (es. il direttore generale, il legale rappresentante, l'amministratore delegato, il presidente, eccetera)
- nel caso di strutture articolate in una struttura centrale e in una o più unità od organismi periferici, il titolare è di regola la struttura nel suo complesso. Se però l'unità o l'organismo periferico esercitano un potere decisionale *del tutto autonomo*, sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza, il titolare diviene l'unità o l'organismo periferico stesso, per quanto riguarda i dati da esso trattati. Si prenda l'esempio di due società che giuridicamente si fondono, ma che per un periodo più o meno lungo mantengono una completa autonomia, nelle operazioni che coinvolgono il trattamento di dati personali: in tale caso permarrà, sotto il profilo che interessa, la presenza di due distinti ed autonomi "titolari" del trattamento dei dati
- si possono verificare anche casi di *contitolarità di un medesimo trattamento*, da parte di più soggetti: ciò accade quando due soggetti od organismi, autonomi fra loro, gestiscono in comune il trattamento e condividono interamente ed effettivamente i poteri decisionali in ordine alle finalità e modalità (es. una banca dati comune a due professionisti)
- in via di principio, una contitolarità si può verificare anche tra una sede centrale ed una sua succursale, qualora si verifichino i presupposti di cui al punto precedente.

Il titolare non può sottrarsi, anche se delega taluno, o al limite tutti gli aspetti gestionali ad altri soggetti, al compito di vigilare sul fatto che le norme privacy vengano diligentemente rispettate e che **le misure di sicurezza vengano attuate**.

Conseguentemente, è il soggetto che per primo è tenuto al risarcimento degli eventuali danni, nonché quello su cui grava in prima istanza la spada di Damocle delle ricche e variegate sanzioni penali, di cui il sistema – privacy è assai ben fornito.

L'eventuale nomina di responsabili del trattamento non consente al titolare di sottrarsi alle proprie responsabilità, dovendo anzi in questo caso tale soggetto rispondere delle proprie scelte *in eligendo* (credibilità della nomina dei responsabili, avendo riguardo ai criteri di idoneità) ed *in vigilando* (controllo sull'operato dei responsabili), ma rende semplicemente possibile la condivisione degli oneri, derivanti dalle azioni illecite compiute dai responsabili.

9.2 Il responsabile del trattamento

NUOVO CODICE	
4[1g] Ai fini del codice privacy si intende per "responsabile" la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.	
NUOVO CODICE	**L 675/1996**
29[1] Il responsabile è designato dal titolare *facoltativamente*. **29[2]** Se designato, il responsabile è *individuato* tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.	**8[1]** Il responsabile, *se designato*, deve essere *nominato* tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
29[3] Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.	**8[3]** Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.
29[4] I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.	**8[4]** I compiti affidati al responsabile devono essere analiticamente specificati per iscritto.
29[5] Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.	**8[2]** Il responsabile procede al trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 1 e delle proprie istruzioni.

Nell'ambito della gestione dei trattamenti, il ***titolare ha facoltà*** di nominare **uno o più responsabili**, anche mediante suddivisione dei compiti.

I confini generali di tale ruolo vengono delineati dal combinato disposto degli articoli 4 e 29 del codice, ai sensi dei quali si definisce responsabile il *soggetto preposto dal titolare al trattamento dei dati personali, che deve essere individuato tra i soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento****, ivi compreso il profilo relativo alla sicurezza***. Tale soggetto deve quindi possedere una competenza insieme tecnica, legale in materia di privacy ed organizzativa.

L'individuazione di un responsabile del trattamento non si riferisce tanto alla possibilità di designare un soggetto, al quale il titolare possa trasferire, delegandole, le proprie responsabilità giuridiche, quanto piuttosto alla possibilità di affidare *specifici incarichi di ordine organizzativo e direttivo* ad un soggetto professionalmente qualificato e capace. Dal testo legislativo si evince che il responsabile non si limita ad essere il mero esecutore delle istruzioni impartitegli dal titolare, poiché le caratteristiche di esperienza, capacità tecnica, affidabilità e conoscenza della legge, poste come condizioni necessarie per la sua nomina, lo qualificano come soggetto in grado di integrare, da un punto di vista pratico e tecnico, le scelte strategiche che il titolare, non necessariamente dotato delle capacità tecniche idonee, ha intrapreso in ordine al trattamento dei dati personali.

Il responsabile deve procedere al trattamento attenendosi alle istruzioni impartite dal titolare che, anche attraverso verifiche periodiche, deve vigilare sulla puntuale osservazione delle disposizioni di legge e delle istruzioni impartite.

Il ruolo di responsabile può essere affidato a persone fisiche, persone giuridiche ed a qualsiasi altro ente, associazione od organismo, ***facenti o meno parte*** della organizzazione del titolare: quest'ultimo, se ritiene di farlo, può quindi nominare un proprio dipendente, un consulente esterno o una società terza.

La nomina deve avvenire ed essere accettata **per iscritto**, ed in essa si devono chiaramente specificare le istruzioni generali, impartite dal titolare, e descrivere analiticamente i compiti che al responsabile vengono da questi affidati. Indicativamente, in tale documento si devono individuare dettagliatamente:

- i dati personali e le banche dati di riferimento, oggetto di trattamento da parte del responsabile
- i trattamenti da svolgere, in funzione di ciascuna tipologia di dati personali, tenendo conto delle finalità del trattamento
- le misure di sicurezza da applicare
- i limiti di autonomia decisionale, nell'attività di gestione delle risorse (umane, tecniche, economiche), per effettuare il trattamento dei dati personali: a tale riguardo, è opportuno che al responsabile venga attribuita la possibilità di gestire in maniera autonoma un budget di spesa, dedicato agli adeguamenti richiesti per ottemperare alle disposizioni legislative e regolamentari
- i limiti di autonomia decisionale, in merito all'organizzazione tecnica ed umana per il trattamento dei dati personali
- i limiti di autonomia decisionale, in merito alle procedure di trattamento dei dati personali
- le responsabilità, che derivano dalle operazioni di trattamento: a tale riguardo, il responsabile risponde entro i limiti dei compiti e dell'esecuzione delle attività di trattamento di sua competenza, individuate dal titolare.

E’ opportuno che il conferimento della nomina di responsabile avvenga in sede di **consiglio di amministrazione**, o di consiglio direttivo in caso di organismi diversi da aziende dotate di personalità giuridica.

9.2.1 Chi nominare responsabile

In generale, nella nomina dei responsabili le organizzazioni utilizzeranno criteri che riflettono la loro struttura organizzativa. Ad esempio:

- una banca tenderà a nominare un responsabile per ogni filiale
- una società, impostata con criteri funzionali, nominerà il direttore del personale come responsabile dei dati personali relativi ai dipendenti; quello amministrativo per il trattamento dei dati di clienti e fornitori
- vi saranno poi figure di responsabili, cui viene attribuito l’incarico con riguardo ad una intera area di problematiche, quale ad esempio quella della sicurezza nel trattamento dei dati personali.

9.2.2 Il responsabile per la sicurezza

In caso di nomina di questa particolare figura, la sua funzione è in genere quella di *progettare, realizzare e mantenere in efficienza* misure di sicurezza tali, da soddisfare le linee strategiche di indirizzo definite dal titolare. In tale ambito, i principali compiti possono essere, a titolo indicativo, i seguenti:

- definire i requisiti di sicurezza da adottare, per proteggere il complesso degli archivi, delle procedure e dei sistemi informatici esistenti: in particolare, dovranno essere definiti diversi livelli di requisiti funzionali, in relazione alla *valorizzazione* del patrimonio informativo da proteggere
- definire un’architettura di sicurezza, che soddisfi i requisiti di cui sopra, con particolare riferimento alla armonizzazione delle misure di sicurezza con le architetture informatiche esistenti od in corso di implementazione
- realizzare la progettazione esecutiva del sistema di sicurezza, con particolare riferimento alla :
  - identificazione degli elementi da proteggere
  - identificazione delle minacce a cui detti elementi sono sottoposti
  - analisi dei rischi ed elaborazione della relativa *mappa*
  - analisi costi / benefici
- implementazione del sistema di sicurezza, come progettato e definito nei punti precedenti
- pianificazione ed esecuzione di test del sistema di sicurezza, attraverso adeguate prove di penetrazione
- definizione ed attuazione di piani e strumenti di monitoraggio continuo della sicurezza
- aggiornamento periodico del sistema di sicurezza, per renderlo sempre adeguato alle nuove minacce
- manutenzione del sistema di sicurezza, per assicurarne costante efficienza e disponibilità
- supporto alla formazione del personale dell’organizzazione, in tema di sicurezza

- emanazione di procedure interne inerenti la sicurezza (regolamentazione degli accessi fisici e logici agli archivi ed ai sistemi informativi, norme operative di utilizzo e gestione dei sistemi, gestione delle password, ecc).

Il compito di proporre, sviluppare e mantenere aggiornate le misure di sicurezza è di rilevante responsabilità e richiede alta professionalità e profonde conoscenze: per tale ragione, le organizzazioni meno strutturate possono decidere di avvalersi di un responsabile esterno, specializzato nella materia.

9.2.3 L'amministratore di sistema

Di tale figura, codificata dal Dpr 318/1999, che all'articolo 1 la definiva come *il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione*, nel nuovo codice non vi è più alcuna traccia. Come è facilmente intuibile, ciò non significa certo che una figura con tale compiti si sia estinta, nella moderna civiltà, in cui nelle organizzazioni vi sono più computers che persone.

Sotto il profilo formale, il Dpr 318/1999 tendeva a considerare questa figura come un incaricato (il soggetto cui è *conferito il compito*), non come un responsabile del trattamento.

In realtà, dato il novero delle problematiche che si devono affrontare nel campo dell'informatica, è opportuno che tale ruolo assurga a livello di responsabile, e venga di fatto assunto dal ***responsabile delle misure di sicurezza***.

Per rivestire tale ruolo, proprio delle organizzazioni che trattano dati con l'uso di elaboratori elettronici, occorre infatti possedere un buon bagaglio di conoscenze tecniche nel campo dei sistemi informativi. Molte organizzazioni, con particolare riferimento a quelle di più limitate dimensioni, possono quindi trovare conveniente ricorrere a specialisti esterni, invece che a personale interno.

9.3 L'incaricato del trattamento

NUOVO CODICE	
4[1h] Ai fini del codice privacy si intende per "incaricati" le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.	
NUOVO CODICE	**L 675/1996**
30[1] *Le operazioni di trattamento possono essere effettuate solo* da incaricati che operano *sotto la diretta autorità* del titolare o del responsabile, attenendosi alle istruzioni impartite.	**8[5]** Gli incaricati del trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi alle istruzioni del titolare o del responsabile.
30[2] *La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.*	**19[1]** *Non si considera comunicazione la conoscenza dei dati personali da parte delle persone incaricate per iscritto di compiere le operazioni del trattamento dal titolare o dal responsabile, e che operano sotto la loro diretta autorità.*

Il nuovo codice precisa che le operazioni di trattamento possono essere effettuate **solo** da persone che abbiano ricevuto **formale incarico**, con uno dei seguenti metodi:

- designazione per iscritto del singolo incaricato, con la quale si individua puntualmente l'ambito del trattamento consentito
- documentata preposizione di una persona ad una unità, per la quale sia stato individuato per iscritto l'ambito del trattamento, consentito agli addetti all'unità medesima.

Questa seconda modalità di incarico, ufficializzata nel nuovo codice dopo essersi affermata nella pratica, rappresenta un'indubbia forma di semplificazione: ad esempio, dopo avere analiticamente individuato per iscritto i trattamenti che l'ufficio *contabilità clienti* deve porre in essere, non è necessario redigere una apposita lettera di incarico della nuova impiegata, che entra a fare parte di tale ufficio. E' sufficiente che si documenti che la persona è stata preposta a tale ufficio, perché si possa considerare che alla stessa è stato dato un formale incarico, per effettuare il trattamento dei dati, necessario a svolgere le sue mansioni.

Il fatto che anche gli incaricati debbano essere **nominati formalmente**, in uno dei due modi sopra descritti, ha una importante valenza organizzativa: per ottemperare correttamente a quanto prescritto dalla privacy, chiunque debba procedere, nell'ambito delle organizzazioni, ad un qualsiasi trattamento di dati personali, deve essere *formalmente incaricato*.

Tale fatto ha ampie e diffuse implicazioni, nel senso che è divenuto sul piano pratico necessario formalizzare l'incarico per il trattamento a chiunque sappia leggere e scrivere, *tarando* i limiti di competenza in funzione delle mansioni svolte. Non si pensi ai soli compiti amministrativi, nell'ambito dei quali si ha per definizione a che fare con indirizzi di clienti, fornitori, dipendenti….. si rifletta invece sul fatto che, in relazione all'ampia accezione di trattamento dei dati personali fatta propria dalla legge, anche una persona che ha il compito di consegnare in città la corrispondenza procede ad un trattamento, per cui diviene un *incaricato del trattamento*, seppure in un senso molto limitato.

E' opportuno, per quanto non tassativamente previsto dalla norma, che l'atto di conferimento dell'incarico, o quello di preposizione di una persona ad una determinata unità, siano **sottoscritti** tanto dal soggetto che richiede il servizio di trattamento (titolare o responsabile), quanto dal soggetto incaricato, quale conferma di accettazione integrale del testo contrattuale e delle istruzioni impartite. Tale previsione trova specifico rafforzamento negli articoli 34 e 35, disciplinanti le misure minime di sicurezza, che esigono che vi sia un *aggiornamento periodico dell'individuazione dell'ambito di trattamento consentito ai singoli incaricati, o alle unità organizzative di cui essi fanno parte*, sia per i trattamenti effettuati con strumenti elettronici, che per quelli che avvengono senza l'ausilio di tali strumenti.

Per quanto concerne la natura del ruolo di incaricato, si evidenzia che si tratta di una *figura esecutiva*, poiché è il soggetto che materialmente esegue le singole operazioni di trattamento, con un potere decisionale limitato.

L'incaricato ha una assoluta mancanza di autonomia gestionale, nel lavoro di trattamento affidatogli, e, conseguentemente, nessun tipo di responsabilità penale od amministrativa, inerente la disciplina in materia di protezione dei dati, grava sull'incaricato. Le uniche responsabilità, che permangono a suo carico, sono connesse con la violazione delle clausole del contratto di servizio, attraverso il quale è stato conferito l'incarico: in altri termini, l'incaricato risponderà esclusivamente degli inadempimenti contrattuali, nella misura in cui il servizio non è conforme a quanto richiesto dal committente (in questo caso dal titolare o dal responsabile).

9.3.1 Chi può essere incaricato

In merito alla natura dei soggetti, che possono essere investiti del ruolo di incaricato, il Garante ha dato sin dagli inizi un'interpretazione restrittiva, prevedendo che l'incaricato debba essere sempre ed esclusivamente una **persona fisica**, e mai una struttura organizzativa complessa: da tale presa di posizione, che purtroppo il nuovo codice ha pensato bene di ufficializzare, derivano conseguenze spesso grottesche.

A tale riguardo, si ipotizzi di volere affidare ad una società esterna il lavoro di stampa di etichette, basato su un database di 5.000 indirizzi di clienti fornito dal committente, e di successiva spedizione di omaggi natalizi.
La società che effettua il lavoro non potrà essere incaricata, ai sensi della normativa privacy, ma dovrà essere *nominata responsabile*, con tanto di formalità ed implicazioni, in termini di condivisione delle responsabilità: tale fatto aveva conseguenze particolarmente onerose sino al 1° febbraio 2002 poiché, sino a quando non sono entrate in vigore le novità previste dal Dlgs 467/2001, la nomina avrebbe dovuto essere notificata al Garante. Grazie alle recenti semplificazioni, recepite anche dal nuovo codice, almeno tale adempimento è venuto meno.

Fermo restando che gli incaricati possono essere solo le persone fisiche, il Garante ha dato facoltà di individuarli sia nell'ambito dei soggetti che hanno un *rapporto di lavoro subordinato* con il titolare del trattamento, che in quello dei soggetti che hanno un *rapporto di lavoro autonomo o di collaborazione*, che infine in quello dei soggetti che *dipendono da altre organizzazioni*: nell'esempio sopra proposto, la società che affida l'operazione di etichettatura potrà così nominare, come incaricati del trattamento, le persone dipendenti della società che provvede ad etichettare, evitando quindi di dovere nominare quest'ultima come responsabile del trattamento.

Ciò ovviamente a condizione che, per quanto riguarda il trattamento dei dati personali che l'etichettatura implica, tali persone agiscano sotto la diretta autorità e controllo, del titolare o di un responsabile, della società che ha commissionato il lavoro.

9.3.2 Le prescrizioni in termini di sicurezza

La normativa sulla sicurezza prescrive che, nella lettera di incarico, o nel documento che individua per iscritto l'ambito di trattamento di una unità organizzativa, vengano fornite esplicite istruzioni in merito ai seguenti punti (tra parentesi si indica il paragrafo, del presente lavoro, nel quale l'argomento viene approfondito):

- procedure di classificazione dei dati (3.1.1)
- affidamento agli incaricati di documenti, contenenti dati personali, e modalità da osservare per la custodia degli stessi (5.1)
- modalità per elaborare e custodire le *password*, nonché per fornirne una copia al preposto alla custodia delle parole chiave (6.1)
- obbligo di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro (6.1)
- procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi (6.3.1 e 6.3.1.1)
- procedure per il salvataggio dei dati (6.3.2)
- custodia ed utilizzo dei supporti rimuovibili, contenenti dati personali (6.4)
- dovere di aggiornarsi, utilizzando il materiale e gli strumenti forniti dall'organizzazione, sulle misure di sicurezza (6.5.2).

9.3.3 Il preposto alla custodia delle parole chiave

È una figura di incaricato, originariamente introdotta dall'abrogando Dpr 28 luglio 1999 n. 318, che lo definisce come il *soggetto preposto alla custodia delle parole chiave*, che consentono l'accesso agli elaboratori elettronici. Il suo compito è quindi quello di custodire una copia delle parole chiave (*passwords*), che gli incaricati elaborano per accedere agli strumenti elettronici. Stante il tenore letterale della norma, è possibile nominare anche *più di un preposto*.

L'attualità di tale ruolo è stata ribadita, dal punto 10. del disciplinare tecnico, allegato al nuovo codice privacy, che detta le misure minime di sicurezza da applicare a partire dal 2004: *quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte, volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici, in caso di prolungata assenza o impedimento dell'incaricato, che renda indispensabile e indifferibile intervenire, per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la* ***custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia****, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.*

Per quanto il ruolo in oggetto configuri un semplice incarico, per cui non è necessario che esso venga assunto dal titolare, o attribuito ad un responsabile del trattamento, è buona norma, se si procede alla nomina di quest'ultimo, incaricarlo della gestione delle parole chiave.

9.3.4 Il soggetto incaricato della manutenzione del sistema

L'abrogando Dpr 318/1999 lo definiva come *la persona che viene incaricata per iscritto di compiere determinate operazioni, dall'amministratore del sistema, e che opera sotto la sua autorità*.
Con il nuovo codice è nominalmente sparito, accomunato in ciò nel destino del suo mentore (l'amministratore del sistema). Di fatto, è più presente che mai, in organizzazioni che sono sempre più informatizzate.
E' uno degli incarichi più *delicati* poiché, nell'espletamento delle loro mansioni, questi incaricati possono avere in genere accesso ai database, in cui è contenuta la maggiore parte dei dati di natura personale trattati dall'organizzazione.
La responsabilità *in eligendo* di chi sceglie questi soggetti, e provvede all'incarico, è quindi molto accentuata, se si considera che non è sempre possibile *blindare* i dati personali contenuti negli elaboratori, prima di affidarli in manutenzione: in particolare, nei frequenti casi in cui si verificano eventi che paralizzano l'attività degli stessi, può divenire di fatto impossibile porre in atto i necessari accorgimenti, per impedire ai soggetti incaricati della manutenzione di accedere ai dati personali contenuti negli elaboratori, anche di natura sensibile.
E' quindi più che mai opportuno porre l'accento, nella lettera di incarico, sul dovere di non effettuare alcun trattamento sui dati personali contenuti nell'elaboratore, fatta unicamente eccezione per i trattamenti di carattere temporaneo strettamente necessari per effettuare la manutenzione del sistema: questo sia nel caso in cui l'incarico venga affidato ad una persona interna all'organizzazione che, a maggiore ragione, in quello in cui il destinatario sia una persona fisica esterna alla stessa. Nel caso in cui la manutenzione venisse affidata ad una società esterna, è quindi opportuno ricevere dalla stessa i nominativi delle persone che provvederanno alla manutenzione, al fine di redigere una lettera di incarico delle stesse.

9.3.5 Il custode dell'archivio ad accesso controllato

Il punto 28. del disciplinare tecnico sulle misure minime di sicurezza, analogamente a quanto stabiliva il precedente Dpr 318/1999, impone di archiviare i documenti contenenti dati sensibili, o a carattere giudiziario, in *archivi ad accesso controllato*, con le seguenti caratteristiche:

- tali archivi devono essere costituiti da luoghi, o da mobili, chiudibili a chiave
- le persone che vengono ammesse agli archivi, dopo l'orario di chiusura degli stessi, devono essere identificate e registrate.

E' quindi necessario nominare uno o più incaricati, per la custodia di tali archivi, che controllino l'accesso agli stessi e tengano il registro delle persone che vi accedono, dopo l'orario di chiusura.

9.4 La predisposizione e l'aggiornamento del mansionario privacy

TRATTAMENTO EFFETTUATO CON STRUMENTI ELETTRONICI
NUOVO CODICE PRIVACY

34[1] Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici.

DISCIPLINARE TECNICO

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

TRATTAMENTO EFFETTUATO SENZA L'AUSILIO DI STRUMENTI ELETTRONICI
NUOVO CODICE PRIVACY

35[1] Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative.

DISCIPLINARE TECNICO

27. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

Il nuovo codice, ed il relativo disciplinare tecnico, impongono ai soggetti che trattano dati personali di predisporre, gestire e custodire un *mansionario privacy*: non si deve a tale fine pensare che sia necessario impegnare giorno e notte decine di cervelli, in una sfibrante attività di ingegnerizzazione di organigrammi privacy, con continui spostamenti di responsabili ed incaricati dalla casella A4 alla casella N6, la notte del 12 maggio, e viceversa, all'alba del 13.

Lasciando le battaglie navali alle realtà più complesse, nella maggiore parte dei casi la base di partenza per costruire il mansionario privacy è costituita dalla semplice predisposizione di dossier, in cui ordinare tutte le delibere e le lettere di nomina e di incarico, nonché i documenti con i quali si individua

l'ambito del trattamento, che devono porre in essere le singole unità organizzative.

Il criterio primario di ordinamento non deve ovviamente essere quello della stratificazione temporale, per cui alla nomina del responsabile per la sicurezza, avvenuta in data 12 luglio, segue in rapida successione quella della persona incaricata di trattare i dati dei clienti, avvenuta in data 13 luglio, e quindi quella della persona che in data 14 luglio ha portato via metà dei computer, per tentare di resuscitarli da improvvisa morte.
Occorre invece separare innanzitutto le delibere di attribuzione di particolari responsabilità, nell'ambito del ruolo di titolare, dalle nomine di responsabili e dalle lettere di incarico, provvedendo poi, all'interno di tali categorie, ad utilizzare i criteri di classificazione che, in relazione alla specifica realtà, appaiono più opportuni.

Ciò per facilitare il secondo passo, che deve essere fissato con *cadenza almeno annuale*: prendere regolarmente in mano il dossier, al fine di aggiornare delibere e contenuti, alla luce delle modifiche intervenute nell'organizzazione o nel quadro normativo. L'importanza di procedere in tale senso è stata ribadita, in occasione dell'approvazione del codice privacy, che impone:

- di aggiornare periodicamente l'individuazione dell'ambito del trattamento consentito ai singoli incaricati, o alle unità organizzative, a nulla rilevando quali siano gli strumenti utilizzati (l'adempimento va quindi posto in essere sia per i trattamenti effettuati con strumenti elettronici, che per quelli effettuati senza l'ausilio degli stessi)
- in aggiunta, per i trattamenti effettuati con strumenti elettronici, di aggiornare periodicamente l'individuazione dell'ambito del trattamento consentito agli addetti alla gestione o alla manutenzione di tali strumenti.

Il *mansionario privacy* non deve essere necessariamente elaborato in modo *personalizzato*, incaricato per incaricato, ma si può procedere come segue:

- si definiscono innanzitutto le classi omogenee di incarico, e dei relativi profili di autorizzazione (ad esempio, una classe omogenea sarà costituita da coloro che sono autorizzati ad *accedere ai dati, di natura comune e sensibile, relativi al personale impiegato*)
- successivamente, si *domiciliano* tutti gli incaricati, ciascuno nella classe omogenea di appartenenza (per cui, ad esempio, nella classe omogenea sopra individuata confluiranno gli *impiegati dell'ufficio personale*).
-

Ad esempio, si potranno individuare le seguenti classi omogenee di incarico:

a) trattamento di dati comuni del personale
b) trattamento di dati sensibili e giudiziari del personale
c) trattamento di dati comuni di clienti
d) trattamento di dati sensibili di clienti
e) trattamento di dati di potenziali clienti
f) trattamento di dati di fornitori

- Mario Rossi, impiegato anziano della contabilità, potrà trattare i dati a), b), c) ed f)
- Barbara Verdi e Luigi Bianchi, impiegati giovani della contabilità, potranno trattare i dati a), c) e f)
- Giovanna Neri e Giorgio Rosso, dell'ufficio personale, potranno trattare i dati a) e b)
- Sandro Verde, impiegato anziano dell'ufficio clienti, potrà trattare i dati c), d) ed e)
- Marco Bianca e Daniela Rossa, impiegati giovani dell'ufficio commerciale, potranno trattare i dati d) ed e).
-

Per riassumere visivamente il tutto, si elabora uno schema, riportando nella colonne i possibili trattamenti, nelle righe i nomi delle persone, e barrando una crocetta in corrispondenza dei trattamenti autorizzati:

	a)	**b)**	**c)**	**d)**	**e)**	**f)**
Mario Rossi	xxx	xxx	xxx			xxx
Barbara Verdi	xxx		xxx			xxx
Luigi Bianchi	xxx		xxx			xxx
Giovanna Neri	xxx	xxx				
Giorgio Rosso	xxx	xxx				
Sandro Verde			xxx	xxx	xxx	
Marco Bianca				xxx	xxx	
Daniela Rossa				xxx	xxx	

Periodicamente, con cadenza almeno annuale, si deve mettere mano al *mansionario privacy*, per la parte che riguarda la definizione dei dati cui gli incaricati sono autorizzati ad accedere, e dei trattamenti che sono autorizzati a porre in essere, al fine di verificare la sussistenza delle condizioni che giustificano tali autorizzazioni.

La stessa operazione deve essere compiuta, per le autorizzazioni rilasciate ai soggetti, il cui incarico è legato alla gestione o manutenzione degli strumenti elettronici.

In tale modo, si potrà sempre disporre del quadro aggiornato e completo di **chi fa cosa**, nell'ambito dell'organizzazione, in materia di privacy.

10 Le coordinate per definire le misure minime di sicurezza

Analogamente a quanto avveniva in vigenza del Dpr 318/1999, anche nel nuovo codice, e nel relativo disciplinare tecnico, le misure minime di sicurezza che devono essere adottate dipendono dal combinarsi di due variabili:

- la **natura dei dati** che vengono trattati
- gli **strumenti che vengono utilizzati** per trattare i dati.

10.1 La natura dei dati trattati

A tale riguardo vi è una distinzione di fondo, in funzione del fatto che ci si limiti a trattare dati personali ***comuni***, ovvero che vengano trattati anche dati:

- ***sensibili***: la lettera d) del comma 1 dell'articolo 4 del codice definisce in tale modo *i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale*
- ***giudiziari***: tali sono considerati, dalla lettera e) del comma 1 dell'articolo 4 del codice, *i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u) del Dpr 313/2002, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.*

Per i casi in cui vengano trattati **dati sensibili o giudiziari** sono in generale imposte ***misure più severe***, rispetto a quanto accade per il trattamento di dati comuni, in relazione al fatto che trattasi dei dati potenzialmente più lesivi della privacy dei soggetti cui si riferiscono.

10.1.1 Le procedure per la classificazione dei dati

Dal fatto che le misure minime di sicurezza sono diverse, in funzione della natura dei dati che vengono trattati, discende la necessità di adottare le ***opportune procedure***, che permettano di stabilire in ogni circostanza quale sia la natura dei dati che si stanno trattando: agli incaricati del trattamento deve quindi essere spiegato cosa si intende per dati sensibili e per dati giudiziari, invitandoli a rivolgersi prontamente ad un responsabile, qualora si imbattano in un dato personale di tale natura, il cui trattamento non rientri nelle normali mansioni, previste dalla lettera di incarico.
Banalmente, l'impiegato di un ospedale, i cui compiti prevedono il trattamento di dati idonei a rivelare le patologie dei pazienti, non sarà certo tenuto a recarsi ogni cinque minuti dal responsabile, esclamando con aria trafelata "*Capo, sto trattando dati sensibili*". Diverso è il caso di un impiegato della funzione commerciale, di una casa vinicola, che, nel corso di una indagine presso alcuni potenziali consumatori, si fosse sentito rispondere da qualcuno "S*ono musulmano osservante"*, piuttosto che "*Sono alcolista*": tali risposte dovrebbero indurre l'impiegato a rivolgersi al responsabile, per avere lumi su come trattare tali dati, anche con riferimento alle misure di sicurezza da osservare nel trattamento.

10.2 Gli strumenti utilizzati per il trattamento

Il nuovo codice mantiene la distinzione di fondo, già presente nel Dpr 318/1999, tra trattamenti effettuati con:

- strumenti **elettronici**, termine nel quale la lettera b) del comma 3 dell'articolo 4 fa rientrare *gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento*
- strumenti **diversi da quelli elettronici**: agendine in cui sono annotati nomi, pesanti faldoni nei quali sono racchiuse pratiche, schedari da non aprire in condizioni di corrente ventosa, nonché simili, e tuttora assai diffusi nonostante si sia in piena rivoluzione *virtuale*, mezzi tradizionali di annotazione, conservazione e consultazione di informazioni e dati.

10.2.1 L'evoluzione per i trattamenti effettuati con mezzi elettronici

Al fine di disciplinare le misure di sicurezza, il precedente Dpr 318/1999 *distingueva nettamente*, nell'ambito degli strumenti elettronici, quelli:

- **non in rete**, cioè non accessibili da altri elaboratori, terminali o, più in generale, da altri strumenti elettronici
- accessibili, da altri elaboratori o più in generale da altri strumenti elettronici, solo attraverso **reti non disponibili al pubblico**: è il caso ad esempio di una rete aziendale, che ha solo collegamenti interni via cavo

- accessibili mediante una **rete** di telecomunicazioni **disponibile al pubblico**.

Alla luce di questa classificazione, erano sorte alcune incertezze, in merito alla circostanza che uno strumento elettronico potesse, o meno, essere considerato essere *in rete*, e se questa fosse *privata* (cioè non disponibile al pubblico) o *pubblica*. A tale riguardo, la relazione di accompagnamento al Dpr 318/1999 ha spiegato che "la distinzione si fonda sulla utilizzazione o meno, per la comunicazione, di reti di comunicazione disponibili al pubblico: essa, a livello di prima approssimazione, riguarda da un lato i sistemi che utilizzano una rete proprietaria, sulla quale possono viaggiare unicamente i dati del titolare del sistema, e dall'altro gli elaboratori che utilizzano *anche solo per alcuni tratti* reti di telecomunicazione disponibili al pubblico. In quest'ottica, vengono a rientrare in questa seconda categoria anche le reti cosiddette geografiche, quando l'interconnessione tra sistemi non accessibili al pubblico venga effettuata mediante una tratta, anche se limitata, di rete pubblica".

La relazione proseguiva spiegando che "la distinzione trova il suo fondamento nel diverso livello di rischio, conseguente alla utilizzazione di un mezzo di trasporto dei dati comunque accessibile anche da parte di altri soggetti: in caso di condivisione di un identico tratto di linea telefonica, anche se i dati viaggiano separati, la possibilità di accesso è infatti sicuramente più semplice, rispetto ad un sistema di interconnessione autonomo, nel quale viaggiano unicamente i dati del titolare".

Sulla base di queste considerazioni, si è dovuto concludere che *anche un singolo elaboratore*, che non fosse fisicamente in rete con altri, ma disponesse di modem e di connessione Internet, dovesse essere considerato come *accessibile mediante una rete di telecomunicazioni disponibile al pubblico*, con la conseguenza di dovere applicare ad esso le più severe misure di sicurezza, previste per tale ipotesi, rispetto a quanto stabilito per gli elaboratori non in rete, o collegati tra loro mediante rete privata.

Nel disciplinare tecnico, allegato al nuovo codice, viene a **perdere qualunque rilievo la distinzione**, presente nel precedente Dpr 318/1999, tra trattamenti effettuati con strumenti elettronici non accessibili da altri elaboratori, terminali o in generale strumenti, e trattamenti con strumenti elettronici *accessibili in rete*, e, nell'ambito di questi ultimi, l'ulteriore distinzione tra l'accessibilità attraverso reti disponibili o non disponibili al pubblico. ***Per l'utilizzo di tutti gli elaboratori, viene quindi imposta l'adozione delle misure di sicurezza più severe, che in precedenza erano riservate ai soli trattamenti con elaboratori in rete.***

Per i soggetti che trattano dati personali, con l'utilizzo di strumenti elettronici, sarà quindi in generale necessario procedere ad un ***adeguamento delle misure di sicurezza***, nel corso del 2004, per ottemperare a quanto disposto dal nuovo codice, e dal relativo disciplinare tecnico in materia di misure minime di sicurezza.

10.3 L’elenco dei trattamenti di dati personali

Le due coordinate sopra esposte (*natura dei dati* e *strumenti utilizzati*) costituiscono la base di partenza, per elaborare **l’elenco dei trattamenti** di dati personali, posto in essere dall’organizzazione: tale fase, che è sempre e comunque necessaria, per comprendere quali misure di sicurezza debbano essere adottate, deve essere ***formalizzata nel documento programmatico sulla sicurezza*** (punto 19.1 del disciplinare), da parte dei soggetti che sono tenuti a redigerlo.

Operativamente, tale elenco può essere sintetizzato in una matrice, nella quale si incrociano:

- **i tipi di dati personali che vengono trattati**. E’ a tale riguardo opportuno entrare in un grado di dettaglio maggiore, di quello offerto dalla semplice distinzione dati comuni / sensibili / giudiziari. Una particolare attenzione deve essere dedicata al *rischio per la privacy* insito nel trattamento, per cui una banca dati contenente informazioni di carattere genetico non può essere accomunata ad un’altra banca dati, che contiene dati sulle patologie dei pazienti: pur essendo sensibili entrambe le categorie di dati, quelli di carattere genetico sono da trattare *con le pinze*, anche sotto il profilo della sicurezza. Altro esempio è costituito dai dati sui pazienti affetti da virus HIV, che sono tutt’altra cosa, rispetto all’elenco di coloro che sono stati sottoposti ad appendicite, pur rientrano entrambe le tipologie di dati in quelli idonei a rivelare le condizioni di salute
- **gli strumenti che vengono utilizzati per il trattamento**. Anche in questo caso, non ci si può limitare a distinguere gli strumenti elettronici, da quelli diversi, ma si deve entrare in un maggiore grado di dettaglio: in primo luogo, mantiene piena validità, *nella sostanza*, la circostanza che un elaboratore sia o meno in rete, e se questa sia privata o pubblica, nonostante dal punto di vista delle misure minime da adottare la distinzione non abbia più rilevanza *formale*. Per tornare al caso del database, contenente i dati sui pazienti affetti da HIV, è evidente che la sua presenza in un computer in rete pubblica aumenta tendenzialmente i rischi per la sicurezza, rispetto all’ipotesi in cui esso venga trattato con un elaboratore che non è in rete. Altro criterio di distinzione, che potrebbe essere opportuno adottare, è quello che si basa sulla *localizzazione* degli strumenti: ad esempio, una rete di computer, dislocati in uffici ai quali si accede dopo avere varcato cinque porte blindate, offre maggiori garanzie di sicurezza di un’altra rete, avente caratteristiche tecniche analoghe, i cui terminali sono però dislocati in uffici poco protetti, nei quali vi è un notevole passaggio.

Di seguito si presenta un semplice esempio di *elenco dei trattamenti di dati personali*, sotto forma di matrice.

Sull'**asse verticale** si indicano i tipi di dati personali che vengono trattati, in ordine tendenzialmente crescente di *pericolosità per la privacy*, come segue:

1	dati comuni di potenziali clienti professionali e fornitori, ottenuti da fonti pubbliche
2	dati relativi a clienti professionali, di natura comune
3	dati relativi a fornitori, di natura comune
4	dati del personale impiegato, anche di natura sensibile
5	dati relativi a pazienti, di natura anche sensibile
6	dati relativi a pazienti affetti da virus HIV
7	dati di natura genetica, relativi a pazienti ed a terzi

Sull'**asse orizzontale** si indicano gli strumenti impiegati, anch'essi in ordine tendenzialmente crescente di pericolosità per la privacy, come segue:

A	schedari ed altri supporti cartacei
B	elaboratori non in rete, localizzati in uffici l'accesso ai quali è oggetto di particolari protezioni
C	videosorveglianza
D	elaboratori non in rete, localizzati in uffici l'accesso ai quali non è oggetto di particolari protezioni
E	elaboratori e strumenti elettronici in rete privata
F	elaboratori non in rete con altri, ma dotati di accesso ad Internet
G	elaboratori e strumenti elettronici in rete pubblica

Nella matrice, elaborata incrociando le due coordinate, si **evidenzia con il simbolo XXX** la circostanza di porre in essere il trattamento di determinati dati personali, con l'utilizzo di determinati strumenti:

TIPI DI DATI TRATTATI								
	7	XXX					XXX	XXX
	6	XXX					XXX	XXX
	5	XXX		XXX	XXX	XXX		
	4	XXX	XXX			XXX		
	3				XXX	XXX		XXX
	2				XXX	XXX		XXX
	1	XXX			XXX		XXX	XXX
		A	**B**	**C**	**D**	**E**	**F**	**G**
		STRUMENTI IMPIEGATI PER IL TRATTAMENTO						

In particolari ipotesi, può essere necessario aggiungere ulteriori coordinate, alle due in base alle quali è stata elaborata la matrice. Ad esempio, in un'impresa che si articola in strutture divisionali, le singole unità potrebbero gestire in modo separato alcune banche di dati (da quelle dei clienti, a quelle dei fornitori, per arrivare in taluni casi anche alla separazione dei dati relativi ai dipendenti). In questi casi, potrebbe essere opportuno elaborare distinte matrici, come segue:

- la prima per le banche dati gestite dalla divisione X
- la seconda per le banche dati gestite dalla divisione Y
- la terza per le banche dati gestite dalla divisione Z
- la quarta per le banche dati gestite a livello centralizzato.

L’elenco dettagliato dei trattamenti, che l’organizzazione pone o intende porre in essere, è un punto di partenza di fondamentale importanza, per delineare ed attuare le misure di sicurezza privacy, sulla base dell’analisi dei rischi, della quale si occuperà il prossimo capitolo.

In questa sede è opportuno evidenziare che il procedimento non è di carattere esclusivamente univoco, ma può anche andare in senso inverso: può infatti accadere che, sulla base dell’analisi dei rischi, e dell’esame delle misure di sicurezza che tali rischi impongono di adottare, si decida di trattare i dati in modo diverso, rispetto a quello di partenza. Ad esempio, una società potrebbe realizzare di non essere in grado di configurare un sistema di sicurezza tale, da potere trattare alcuni dati sensibili con strumenti elettronici in rete pubblica, decidendo quindi di rinunciare ad avvalersi della stessa, per il trattamento di tali dati, ed optando per la loro gestione tramite elaboratori che non sono in rete.

Ad esempio, nel caso in esame appare particolarmente critica la circostanza di trattare dati relativi a pazienti affetti da virus HIV (6) e di natura genetica (7) con elaboratori dotati di accesso ad Internet (F) e con elaboratori in rete pubblica (G): al termine dell’analisi, si potrebbe quindi decidere di rimuovere il collegamento ad Internet (passando quindi da F a B o, al limite, a D) e di trasferire i dati dalla rete pubblica a quella privata (passando quindi da G a E).

10.3.1 La banca dati dei sistemi informativi

Un aspetto strettamente correlato, con la definizione degli strumenti con cui si trattano i dati, è quello di predisporre ed aggiornare una banca dati di tutte le dotazioni hardware, software e di trasmissione dati, di cui è dotata l’organizzazione: è importante che questo archivio venga tenuto aggiornato con le sostituzioni, riparazioni e con i consumi delle apparecchiature.
Questa banca dati dei sistemi informativi, se correttamente gestita, permette di avere una visione precisa del patrimonio informativo, arricchita di informazioni estremamente utili e statistiche sul grado di affidabilità e uso dei sistemi: di conseguenza, sarebbe di grande aiuto, oltre che per definire la mappa complessiva dei trattamenti, al fine di adottare le misure di sicurezza, anche nei processi di acquisto ed in quelli di pianificazione degli investimenti.

11 L’analisi dei rischi

Un passaggio fondamentale, per configurare ed attuare in modo corretto il sistema di sicurezza privacy, è di effettuare l’analisi dei rischi, legati alla gestione dei dati, partendo dall’*elenco dei trattamenti di dati personali*, elaborato nel paragrafo 3.3 del precedente capitolo: solo avendo un quadro chiaro dei rischi, cui è sottoposto il trattamento dei dati, si può infatti costruire la mappa delle misure di sicurezza, necessarie per fronteggiarli.
L’analisi dei rischi deve essere ***formalizzata***, nei casi in cui il titolare è tenuto alla redazione del documento programmatico di sicurezza, uno dei punti del quale è costituito dall’*analisi dei rischi che incombono sui dati* (punto 19.3 del disciplinare tecnico). Anche nei casi in cui non si è tenuti a redigere tale documento, è comunque opportuno procedere ad una formalizzazione dell’analisi dei rischi, alla luce della quale si potrà poi valutare l’idoneità dei sistemi di sicurezza già adottati, e di quelli di cui si intende procedere all’adozione.

L’analisi dei rischi si articola nelle seguenti fasi:
1. valutazione delle minacce che gravano sui singoli trattamenti di dati personali
2. valutazione dell’impatto che, per l’organizzazione, ha il verificarsi di eventi negativi, nell’ambito dei singoli trattamenti
3. identificazione del grado di rischio da coprire, e decisioni conseguenti.

11.1 Valutazione delle minacce

TIPI DI DATI TRATTATI	A	B	C	D	E	F	G
7	XXX					XXX	XXX
6	XXX					XXX	XXX
5	XXX		XXX	XXX	XXX		
4	XXX	XXX			XXX		
3				XXX	XXX		XXX
2				XXX	XXX		XXX
1	XXX			XXX		XXX	XXX

STRUMENTI IMPIEGATI PER IL TRATTAMENTO

Utilizzando la matrice elaborata al termine del capitolo precedente, si evidenzia che il rischio complessivo, che grava su ogni *tipologia di trattamento* (le caselle contraddistinte da XXX) è il risultato del combinarsi del rischio legato da una parte ai tipi di dati, oggetto di trattamento, dall'altra agli strumenti che vengono impiegati per trattare tali dati.

Per quanto concerne i **tipi di dati**, essi possono in talune ipotesi costituire la ***fonte primaria di rischio***: si pensi ad esempio al database della clientela, il cui trafugamento è passibile di arrecare nocumento non solo all'organizzazione che lo possiede, ma anche ai clienti, ai quali i dati si riferiscono.
In funzione dell'*appetibilità* dei dati trattati, nonché della *idoneità* degli stessi ad arrecare danno ai soggetti cui si riferiscono, i vari tipi di dati si considereranno portatori di un diverso grado di rischio, che potrà essere evidenziato in termini numerici (es. 9 per i dati genetici, 1 per dati comuni scaricati da Internet, dove sono liberamente accessibili), o in termini qualitativi (es. rischio *elevatissimo* per i dati genetici, *modesto* per i dati comuni scaricati da Internet).
Nel caso preso ad esame, si ipotizzi che venga attribuito il seguente coefficiente di rischio:

		RISCHIO
1	dati comuni di potenziali clienti professionali e fornitori, ottenuti da fonti pubbliche	**1**
2	dati relativi a clienti professionali, di natura comune	**7**
3	dati relativi a fornitori, di natura comune	**3**
4	dati del personale impiegato, anche di natura sensibile	**2**
5	dati relativi a pazienti, di natura anche sensibile	**6**
6	dati relativi a pazienti affetti da virus HIV	**7**
7	dati di natura genetica, relativi a pazienti ed a terzi	**9**

Si noti che in alcuni casi è determinante il fattore legato alla appetibilità dei dati (ad esempio, quelli relativi a clienti professionali, ai quali è stato attribuito il punteggio 7, nonostante non siano particolarmente *delicati* in

termini di privacy, in relazione alla importanza della loro riservatezza, per l'organizzazione); in altri casi assume invece primaria importanza la tutela della privacy degli interessati (con particolare riferimento ai dati sensibili relativi ai pazienti). Il punteggio massimo di 9 è stato attribuito ai dati di natura genetica.

Per quanto concerne gli **strumenti impiegati per il trattamento**, si deve considerare che essi possono essere oggetto di una o più delle seguenti categorie di minacce:

- eventi *naturali* a carattere distruttivo (es. incendi, allagamenti, corti circuiti)
- penetrazione di terzi, con conseguenti furti e danni
- guasti tecnici delle apparecchiature
- penetrazione logica e nelle reti di comunicazione
- atti di sabotaggio ed errori umani, da parte del personale dell'organizzazione.

Di seguito si commentano brevemente i rischi più frequenti, cui sono sottoposte alcune delle principali categorie di strumenti:

Risorse Hardware: rientrano in questa categoria CPU, terminali, workstation, personal computer, stampanti, disk drive, linee di comunicazione, server, router. Le principali minacce a cui questi dispositivi sono sottoposti sono legate ai mal funzionamenti, dovuti a guasti o sabotaggi, eventi naturali quali allagamenti e incendi, furti e intercettazione. Quest'ultima minaccia interessa gli apparati di rete, cioè le linee di comunicazione, i router ed i server: è infatti possibile effettuare il monitoraggio indebito, o la alterazione della trasmissione di dati, effettuata da questi apparati, sia che questa avvenga tra terminali, tra computer, tra stazioni di lavoro periferiche e sistemi centrali di elaborazione. Un altro caso può riguardare i video, intercettando le onde elettromagnetiche emesse dai quali si può procedere alla ricostruzione remota dell'immagine.

Risorse Software: rientrano in questa categoria Sistemi Operativi e Software di Base (utility, diagnostici), Software Applicativi, Gestori di basi di dati, Software di rete, i programmi in formato sorgente e oggetto, ecc. Le minacce principali legate all'uso di questi prodotti sono:

- la presenza di errori involontari, commessi in fase di progettazione e/o implementazione, che consentono ad utenti non autorizzati l'esecuzione di operazioni e programmi riservati a particolari categorie di utenti
- la presenza di un codice malizioso, inserito volontariamente dai programmatori dell'applicazione stessa, al fine di poter svolgere operazioni non autorizzate sul sistema, o per danneggiare lo stesso. Rientrano in questa categoria di minacce i virus, i trojan horse, le bombe logiche, le backdoor
- attacchi di tipo *denial of service*, che vengono generalmente portati a servizi di rete, ma sono facilmente estendibili a un qualunque servizio. Si tratta di attacchi non distruttivi, il cui obiettivo è saturare la capacità di risposta di un servizio, con il fine ultimo di renderlo inutilizzabile agli altri utenti del sistema.

Documentazioni Cartacee: le principali minacce a cui tali elementi sono sottoposti sono la distruzione e/o l'alterazione ad opera di eventi naturali, di azioni accidentali e di comportamenti intenzionali.
Supporti di memorizzazione: si tratta dei supporti su cui vengono tenute le copie dei software installati, dei file di log, dei back-up e dei dati personali. Oltre alle minacce cui sono sottoposte le documentazioni cartacee, tali dispositivi sono soggetti a:

- deterioramento nel tempo
- inaffidabilità del mezzo fisico, che in alcuni casi può presentare difetti di costruzione che ne compromettono il buon funzionamento nel tempo.

Per ogni categoria di strumenti, si dovrà procedere innanzitutto ad una *descrizione dei concreti elementi di rischio*, nella specifica situazione dell'organizzazione, ad alla conseguente espressione di un *giudizio riassuntivo* sul grado di rischio cui sono sottoposti (ad esempio, *elevato* per i trattamenti effettuati in rete pubblica, con terminali facilmente accessibili; *medio* per i trattamenti effettuati con una rete privata, i cui terminali sono situati in locali protetti da porte blindate).
E' evidente che esiste una *relazione inversa* tra il grado di rischio, cui sono sottoposti gli strumenti, e l'insieme delle misure atte a proteggerli, che vengono adottate: a tale riguardo, si fa presente che, se l'analisi dei rischi è finalizzata ad adottare nuove e più efficaci misure di sicurezza, al termine di tale processo il grado di rischio, che grava su alcuni o su tutti gli strumenti impiegati, è destinato ad abbassarsi. In questi casi è opportuno che, in sede di analisi dei rischi, si proceda ad una duplice valutazione del grado di rischio che grava sugli strumenti, procedendo a stimarlo:

- sia nello *stato iniziale*, prima cioè che vengano adottate le nuove misure di sicurezza
- che nello *stato finale*, allorché le nuove misure previste saranno operative.

Si riportano i giudizi, sul grado di rischio nello *stato iniziale*, nell'esempio oggetto d'analisi:

		RISCHIO
A	schedari ed altri supporti cartacei	**2**
B	elaboratori non in rete, localizzati in uffici l'accesso ai quali è oggetto di particolari protezioni	**4**
C	videosorveglianza	**3**
D	elaboratori non in rete, localizzati in uffici l'accesso ai quali non è oggetto di particolari protezioni	**6**
E	elaboratori e strumenti elettronici in rete privata	**4**
F	elaboratori non in rete con altri, ma dotati di accesso ad Internet	**8**
G	elaboratori e strumenti elettronici in rete pubblica	**5**

Nel caso in esame, le strutture fisiche di protezione delle aree e dei locali in cui si effettua il trattamento sono *idonee*, per cui il fattore di rischio legato ad eventi naturali di ordine distruttivo ed a penetrazione di terzi è basso (ciò spiega la ragione per cui, ad esempio, agli schedari ed agli altri supporti cartacei, che sono soggetti essenzialmente a tali tipologie di rischi, può essere associato un valore molto basso).

L'azienda è inoltre dotata di misure di *sicurezza logica* molto avanzate, a livello centralizzato: per tale ragione viene attribuito un grado di rischio maggiore agli elaboratori che non sono in rete, la gestione della cui sicurezza è più frammentata, rispetto a quanto accade per gli elaboratori e strumenti in rete.

Nella matrice in esame vengono ora inseriti i punteggi espressivi del rischio, in funzione dei dati trattati (primo numero) e degli strumenti utilizzati per il trattamento (secondo numero):

	7 (9)	9 - 2					9 - 8	9 - 5
	6 (7)	7 - 2					7 - 8	7 - 5
TIPI DI	**5** (6)	6 - 2		6 - 3	6 - 6	6 - 4		
DATI	**4** (2)	2 - 2	2 - 4			2 - 4		
TRATTATI	**3** (3)				3 - 6	3 - 4		3 - 5
	2 (7)				7 - 6	7 - 4		7 - 5
	1 (1)	1 - 2			1 - 6		1 - 8	1 - 5
		A (2)	**B** (4)	**C** (3)	**D** (6)	**E** (4)	**F** (8)	**G** (5)

STRUMENTI IMPIEGATI PER IL TRATTAMENTO

11.2 L'impatto degli eventi negativi

L'analisi condotta nel punto precedente si conclude con una serie di considerazioni di *carattere qualitativo*, che possono in generale essere sufficienti, come base di partenza per il processo di adozione delle ***misure minime*** di sicurezza, ai fini della normativa privacy: essendo tali misure imposte dalla normativa, pena l'assoggettamento a sanzioni penali, non è infatti necessario addentrarsi in analisi costi (*per l'adozione delle misure*) / benefici (*copertura dei costi legati agli eventi negativi*).

Le considerazioni che seguono, nel presente e nel prossimo paragrafo, sono quindi finalizzate a stabilire quali possano essere i vantaggi, legati alla adozione di ***ulteriori misure di sicurezza***, addizionali a quelle minime: a tale fine, può essere utile ricorrere a stime di carattere quantitativo, per determinare se il costo dei meccanismi di protezione bilancia il valore del bene a rischio.

Per procedere alla stima dei costi degli eventi negativi, i criteri di più diffusa adozione sono i seguenti:

- *Reddito netto generato dai beni/dati da proteggere*
- *Altri parametri per calcolare l'utilità dei beni/dati da proteggere*: qualora l'indicatore di cui al punto precedente non fosse significativo, come può ad esempio accadere nel caso di un servizio pubblico, possono essere utilizzati altri parametri, espressivi ad esempio del numero di utenti che utilizzano i beni/dati in questione, moltiplicati per un fattore che indichi quale è l'utilità che gli utenti ottengono dal loro uso

- *Perdita annuale attesa dovuta alla perdita dei beni/dati da proteggere*, che indica una stima del danno creato, nel momento in cui si verificano le minacce a cui essi sono sottoposti. Nel computo di tale stima vanno conteggiati il danno all'immagine, le violazioni alle normative esistenti, il mancato profitto, ecc…
- *Costo di ricostruzione dei beni/dati da proteggere*, inclusivo non solo delle spese vive, sostenute nei confronti di terze economie, ma anche del costo-opportunità legato alle perdite di tempo causate all'organizzazione ed ai mancati profitti, nel periodo occorrente per il ripristino.

11.3 La gestione dei rischio

Sulla base di quanto emerge dalle precedenti fasi, l'organizzazione deve decidere in che misura procedere all'**abbattimento del rischio**, adottando l'insieme delle contromisure di natura fisica, logica ed organizzativa, che possono fornire protezione in differenti maniere:

- ridurre la minaccia
- ridurre la vulnerabilità
- ridurre l'impatto di eventi accidentali
- rilevare un evento accidentale
- aiutare nel recovery di un evento accidentale.

A tale riguardo, si possono individuare due soglie:

- quella costituita dall'insieme delle ***misure minime di sicurezza***, che deve in ogni caso essere raggiunta, qualunque sia il costo, per ottemperare a quanto previsto dalla normativa privacy
- quella più elevata, costituita dal raggiungimento delle ***misure idonee di sicurezza***: al fine di decidere in che misura adottarle, diviene rilevante il rapporto costi / benefici.

I costi delle ***misure di sicurezza addizionali***, rispetto a quelle ***minime*** richieste dalla norma, deve essere stimato considerando:

- sia gli **esborsi monetari**: il costo di sviluppo, il costo di implementazione complessivo, il costo di manutenzione e di supporto annuale
- che gli eventuali **costi impliciti**, espressivi degli impatti negativi che le misure di sicurezza possono avere sull'organizzazione, nei seguenti termini:
  - *impatto che la misura di sicurezza ha sugli utenti del servizio* per cui viene approntata. Per stimare il livello di accettazione della soluzione da parte degli utenti finali vanno considerati una serie di parametri quali: come la soluzione impatta sul modo di operare dell'utente, il numero di utenti coinvolti, quali inconvenienti potrebbe causare (ritardi, difficoltà, ecc.), eventuali incrementi nei costi del servizio

- *livello di accettazione della misura di sicurezza da parte dei propri dipendenti*. Gli indicatori che possono essere considerati per valutare questo fattore sono: il numero di dipendenti coinvolti, gli inconvenienti che tale soluzione potrebbe causare al loro modo usuale di operare (ritardi, difficoltà, ecc.), il grado di preparazione e il tempo a disposizione dei dipendenti per implementare efficacemente questa soluzione.

L'ultimo passo è di abbattere i benefici, legati all'adozione delle misure di sicurezza, stimati nel precedente paragrafo 4.2 (*mancato verificarsi degli eventi negativi*), elaborando un **coefficiente** (da 0% a 100%) in base a due ordini di considerazioni:

- in primo luogo, le misure di sicurezza identificate hanno un diverso grado di copertura delle minacce: 0% indica che una determinata misura non elimina la minaccia, 100% indica che essa la elimina totalmente
- in secondo luogo, non è detto che, in caso di mancata adozione delle misure di sicurezza, le minacce si concretizzino: in considerazione di tale fatto, il baciato dalla fortuna attribuirà un coefficiente vicino allo 0%; lo sfortunato cronico tenderà ad avvicinarsi invece al 100%.

Ad esempio, una soluzione che elimini metà del rischio, per uno sfortunato medio, si vedrà attribuire un ***coefficiente*** complessivo di 50% x 50% = 25%.

L'adozione delle ***ulteriori misure di sicurezza*** sarà conveniente solo se si verifica la seguente condizione:

Costo delle misure di sicurezza addizionali	**<**	**C**osto degli eventi negativi **x** **C**oefficiente

12 I trattamenti senza l'ausilio di strumenti elettronici

Pur essendo prescritte dall'articolo 35 del codice privacy, per il trattamento dei dati personali con *strumenti diversi da quelli elettronici*, le misure di sicurezza descritte nel presente capitolo devono essere adottate in modo pressoché generalizzato**, per due ordini di ragioni:**

- si osserva innanzitutto che tutte le organizzazioni, anche quelle tecnologicamente più progredite, effettuano in genere alcuni trattamenti (per quanto residuali possano essere) con mezzi "tradizionali"
- in secondo luogo, si tratta di disposizioni che, seppure dettate per la ipotesi più semplicistica, di trattamento *manuale* dei dati, devono trovare a maggiore ragione applicazione anche per i trattamenti effettuati con mezzi elettronici. Ad esempio, le cautele imposte per archiviare un elenco cartaceo, contente dati sensibili, devono essere osservate **anche per la custodia di un supporto magnetico**, nel quale tali dati dovessero essere stati memorizzati.

<table>
<tr><th colspan="2">NUOVO CODICE PRIVACY</th></tr>
<tr><td colspan="2">35[1] Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.</td></tr>
<tr><th>DISCIPLINARE TECNICO</th><th>DPR 318/1999</th></tr>
<tr><td>27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.</td><td>9[1] Nel caso di trattamento di dati personali, effettuato, con strumenti diversi da quelli elettronici, sono osservate le seguenti modalità :
a) nel designare gli incaricati del trattamento per iscritto e nell'impartire le istruzioni, si deve prescrivere che gli incaricati abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati;
b) gli atti e i documenti contenenti i dati devono essere conservati in archivi ad accesso selezionato e, se affidati agli incaricati del trattamento,</td></tr>
</table>

	devono essere da questi ultimi conservati e restituiti al termine delle operazioni affidate.
28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.	**9[2]** Nel caso di trattamento di dati sensibili e giudiziari, oltre a quanto previsto nel comma 1, devono essere osservate le seguenti modalità : a) se affidati agli incaricati del trattamento, gli atti e i documenti contenenti i dati sono conservati, fino alla restituzione, in contenitori muniti di serratura;
29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.	b) l'accesso agli archivi deve essere controllato e devono essere identificati e registrati i soggetti che vi vengono ammessi dopo l'orario di chiusura degli archivi stessi.
	10[1] I supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di dati personali sensibili e giudiziari devono essere conservati e custoditi con le modalità di cui all'articolo 9.

La norma disciplina gli aspetti riguardanti:

- l'affidamento di atti o documenti contenti dati personali agli incaricati, e la custodia da parte di questi (lettera b) del comma 1 dell'articolo 35 del codice, cui danno concreta attuazione i punti 27 e 28 del disciplinare tecnico)
- la creazione e gestione degli archivi, nei quali riporre e custodire atti e documenti contenti dati personali, quando gli stessi non sono utilizzati per lo svolgimento delle operazioni affidate agli incaricati (lettera c) del comma 1 dell'articolo 35 del codice, cui dà attuazione il punto 29 del disciplinare tecnico).

12.1 L'affidamento agli incaricati e la custodia di atti e documenti

Il punto 27. del disciplinare tecnico pone l'accento sulla necessità che vengano impartite **istruzioni scritte**, su come debbano avvenire il controllo e la custodia di atti e documenti, contenenti dati personali di qualsiasi natura (ivi inclusi, quindi, quelli comuni).
Si noti che nel disciplinare non è più riproposta la disposizione, presente nel Dpr 318/1999, per cui agli incaricati deve essere prescritto, per iscritto, di *accedere ai soli dati personali, la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati*: è però opportuno che, nella lettera di incarico, una simile previsione venga mantenuta, in quanto finalizzata a scoraggiare possibile trattamenti *scorretti* di dati personali (si pensi a quanto sarebbe inopportuno che un impiegato dell'ufficio commerciale, che nulla ha a che fare con l'amministrazione del personale, accedesse alle buste paga di tutti i colleghi).
Gli incaricati del trattamento devono quindi prelevare dagli archivi i soli atti e documenti loro affidati, che devono *controllare e custodire*, durante l'intero ciclo necessario per lo svolgimento delle operazioni di trattamento, per poi restituirli all'archivio, al termine di tale ciclo.
Sul piano pratico, *affidare i documenti* agli incaricati ha un significato elastico: il titolare, o il responsabile del trattamento, indicheranno all'incaricato quale genere di documenti sia necessario, ai fini del trattamento, lasciando all'incaricato stesso l'incombenza di accedere all'archivio per reperirli. Non è inoltre necessario che le istruzioni agli incaricati, su quali documenti debbano essere reperiti, vengano date per iscritto, per ogni singolo caso, ma è buona norma specificare, in sede di conferimento dell'incarico, quali siano gli archivi cui l'incaricato può avere accesso, per lo svolgimento dei propri compiti.
Per quanto riguarda il *controllo e la custodia*, da parte degli incaricati, la prima e più generalizzata prescrizione è che gli atti e i documenti, contenenti dati personali, non devono essere lasciati liberi di vagare senza controllo ed a tempo indefinito per gli uffici, ma occorre che gli incaricati, cui essi sono affidati per lo svolgimento delle loro mansioni, provvedano in qualche modo a controllarli e custodirli, per poi restituirli al termine delle operazioni loro affidate. Questa è una prescrizione di carattere generale, che attiene alla buona organizzazione degli uffici, per cui deve trovare applicazione anche per gli atti ed i documenti contenenti solo dati di natura comune. Fermo restando tale principio, per gli atti ed i documenti contenenti dati sensibili o giudiziari il punto 28. del disciplinare aggiunge la previsione, per cui il controllo e la custodia devono avvenire in modo tale, che ai dati *non accedano persone prive di autorizzazione*. A tale fine, è quindi necessario che l'incaricato del trattamento venga dotato di cassetti con serratura, o di altri accorgimenti aventi funzione equivalente, nei quali riporre i documenti contenti dati sensibili o giudiziari prima di assentarsi dal posto di lavoro, anche temporaneamente (ad esempio, per recarsi in mensa).
In tali cassetti i documenti potranno essere riposti al termine della giornata di lavoro, qualora l'incaricato debba utilizzarli anche nei giorni successivi; al termine del trattamento l'incaricato dovrà invece restituirli all'archivio.

12.2 L’archiviazione di atti e documenti

A differenza di quanto avveniva in precedenza, la norma non detta più alcuna regola, per l’archiviazione di atti e documenti contenenti solo dati di natura comune**. In questa ipotesi, il Dpr 318/1999 prevedeva vi fosse l’obbligo di conservazione in *archivi ad accesso selezionato*: essi dovevano essere cioè dislocati in luoghi bene identificati, che non era necessario chiudere a chiave, ai quali si doveva dare istruzione avessero facoltà di accedere solo gli incaricati del trattamento. Mentre i locali della mensa aziendale non sarebbero evidentemente stati all’uopo adatti, sarebbe ad esempio stato sufficiente creare una serie di armadi e scaffalature, in prossimità degli uffici.**

Il nuovo disciplinare tecnico impone l’adozione di particolari misure solo per gli atti e documenti contenenti **dati sensibili e giudiziari**, prevedendo che gli archivi debbano essere **controllati**, ponendo in essere i seguenti accorgimenti:

- il primo, che ha l’obiettivo di fare in modo che agli archivi accedano *sempre e comunque* i soli soggetti autorizzati, consiste nell’adozione di almeno una delle seguenti soluzioni:
  - dotare gli archivi di strumenti elettronici per il controllo degli accessi (ad esempio, tesserino magnetico distribuito agli incaricati autorizzati)
  - dare incarico ad alcune persone, di vigilare gli archivi: il che si può realizzare non solo apponendo una persona, specificamente addetta a tale controllo, soluzione eccessivamente dispendiosa per le realtà di modeste dimensioni, ma anche adottando opportuni accorgimenti di carattere organizzativo. Ad esempio, dando incarico per iscritto ad un gruppo di impiegati, *aventi la scrivania prospicente l’archivio*, di fare in modo che almeno uno di loro sia sempre presente, durante tutto l’orario di apertura dell’archivio, e controlli chi vi accede
  - nel caso in cui non venga adottata alcuna delle soluzioni di cui sopra, si deve autorizzare preventivamente le persone ad accedere agli archivi (in genere, ciò si abbina ad altri accorgimenti, che possono consistere semplicemente nel tenere l’archivio chiuso a chiave, dando la stessa a chi è autorizzato ad accedere, ed invitandolo a richiudere a chiave, ed eventualmente a restituire la stessa, al termine dell’accesso)

- il secondo, che trova applicazione per gli accessi che avvengono *dopo l'orario di chiusura*, consiste nell'obbligo di *identificare* e *registrare* le persone che accedono agli archivi, adottando ad esempio una delle seguenti soluzioni:
  - dotare gli archivi di strumenti elettronici per il controllo degli accessi, che siano in grado di abbinare al possessore l'informazione in merito all'attività svolta (ad esempio, tesserino magnetico, distribuito agli incaricati autorizzati, dall'utilizzo del quale si può risalire all'informazione che l'impiegato Rossi è entrato nell'archivio alle 23.30 di un determinato giorno)
  - affidare la chiave dell'archivio, dopo l'orario di chiusura, al titolare o ai responsabili del trattamento, o in alternativa ad uno o più soggetti incaricati per iscritto, i quali annoteranno in un apposito registro i nominativi di chi ha richiesto di accedere all'archivio, al di fuori del periodo di apertura
- in ogni caso, si deve desumere che l'archivio contenente i dati in esame deve potere essere *chiuso*, perché altrimenti non si potrebbero porre in essere le prescrizioni di cui ai punti precedenti.

12.3 I supporti non informatici

L'articolo 10 del Dpr 318/1999 conteneva la prescrizione per cui i *supporti non informatici* (generalmente schedari), contenenti la riproduzione di informazioni relative al trattamento di dati sensibili o giudiziari, dovevano essere custoditi e conservati con le medesime modalità, previste per la generalità degli atti e documenti. Il nuovo codice, sulla base della considerazione che tali supporti sono a tutti gli effetti considerabili come atti o documenti, non ripropone la disposizione, in quanto ridondante.

13 I trattamenti con strumenti elettronici

Nel presente capitolo si analizzano le misure minime di sicurezza prescritte dall'articolo 34 del codice privacy, e sviluppate nei punti da 1. a 26. del disciplinare tecnico, per i trattamenti effettuati con strumenti elettronici: in tale categoria rientrano *gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento*.

La novità di portata più generale, rispetto a quanto previsto dall'abrogando Dpr 318/1999, è che, ai fini dell'adozione delle misure minime di sicurezza, viene a *perdere ogni rilevanza* la distinzione tra elaboratori non in rete ed elaboratori in rete e, nell'ambito di questi ultimi, tra elaboratori in rete privata ed elaboratori in rete pubblica.

13.1 Adozione di un sistema di autenticazione informatica

<table>
<tr><th colspan="2">NUOVO CODICE PRIVACY</th></tr>
<tr><td colspan="2">34[1] Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell’allegato B), le seguenti misure minime:
a) autenticazione informatica;
b) adozione di procedure di gestione delle credenziali di autenticazione;
4[3] Ai fini del presente codice si intende per:
c) “autenticazione informatica”, l’insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell’identità;
d) “credenziali di autenticazione”, i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l’autenticazione informatica;
e) “parola chiave”, componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;</td></tr>
<tr><th>DISCIPLINARE TECNICO</th><th>DPR 318/1999</th></tr>
<tr><td>Sistema di autenticazione informatica</td><td></td></tr>
<tr><td>1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.</td><td>2[1] (Per tutti gli elaboratori) Devono essere adottate, anteriormente all'inizio del trattamento, le seguenti misure:
a) prevedere una parola chiave per l'accesso ai dati, fornirla agli incaricati del trattamento e, ove tecnicamente possibile in relazione alle caratteristiche dell'elaboratore, consentirne l'autonoma sostituzione, previa comunicazione ai soggetti preposti ai sensi della lettera b);</td></tr>
<tr><td>2. Le credenziali di autenticazione consistono in un codice per l’identificazione dell’incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell’incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell’incaricato, eventualmente associata a un codice identificativo o a una parola chiave.</td><td></td></tr>
</table>

3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione. **4.** Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato. **5.** La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi. **6.** Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.	**4[1]** Nel caso di trattamenti effettuati con gli elaboratori in rete, oltre a quanto previsto dall'articolo 2 devono essere adottate le seguenti misure: a) a ciascun utente o incaricato del trattamento deve essere attribuito un codice identificativo personale per l'utilizzazione dell'elaboratore; uno stesso codice, fatta eccezione per gli amministratori di sistema relativamente ai sistemi operativi che prevedono un unico livello di accesso per tale funzione, non può, neppure in tempi diversi, essere assegnato a persone diverse (*Amministratori di sistema*: i soggetti cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione).
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. **8.** Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.	b) i codici identificativi personali devono essere assegnati e gestiti in modo che ne sia prevista la disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore o di mancato utilizzo dei medesimi per un periodo superiore ai sei mesi;
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.	

10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.	**2[1]** *(Per tutti gli elaboratori*) Devono essere adottate, anteriormente all'inizio del trattamento, le seguenti misure: b) individuare per iscritto, quando vi è più di un incaricato del trattamento e sono in uso più parole chiave, i soggetti preposti alla loro custodia o che hanno accesso ad informazioni che concernono le medesime.
11. Le disposizioni sul sistema di autenticazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.	**4[2]** Le disposizioni di cui al comma 1, lettere a) e b), non si applicano ai trattamenti dei dati personali di cui è consentita la diffusione.

Il primo ordine di prescrizioni, dettate dal primo comma dell'articolo 34 del codice privacy, impone che vengano adottati gli opportuni sistemi, al fine di consentire l'accesso agli strumenti elettronici solo ***a chi è autorizzato***, tramite:

lettera a) l'impostazione di un **sistema di autenticazione informatica**, che l'articolo 4, comma 3, lettera c) del codice definisce come *l'insieme degli strumenti elettronici e delle procedure per la* ***verifica dell'identità***, che può avvenire:

- sia in modo diretto (ad esempio, con una tecnica biometrica, dall'iride alle impronte digitali, che individua in modo diretto la persona)
- che in modo indiretto (ad esempio, tramite un tesserino magnetico, che individua la persona indirettamente, per effetto del fatto che essa lo possiede; o mediante un codice, che individua la persona indirettamente, per il fatto che essa lo conosce e digita)

***lettera b*)** l'adozione di procedure di gestione delle **credenziali di autenticazione**, che l'articolo 4, comma 3, lettera d) definisce come *i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica*. Non è quindi più ammesso, in alcuna circostanza, che i medesimi dati o dispositivi siano conosciuti da, o correlati a, più persone, come in alcuni casi poteva avvenire in vigenza del Dpr 318/1999.
L'*entrata* negli strumenti elettronici non deve mai essere libera, ma ad essi devono potere accedere solo le persone autorizzate, alle quali sia stata a tale fine attribuita una *chiave* personalizzata: in tale senso, il punto 1. del disciplinare tecnico stabilisce che *il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione, che consentano il superamento di una procedura di autenticazione, relativa a uno specifico trattamento o a un insieme di trattamenti*. Gli strumenti elettronici devono quindi essere dotati di dispositivi che permettano di *chiuderli informaticamente a chiave*, in modo che vi possano accedere solo gli incaricati che hanno la chiave. Non è in alcun caso consentito che si possa accedervi liberamente, cioè semplicemente accendendoli. Unica eccezione, al verificarsi della quale le norme in commento non trovano applicazione, si ha nel caso in cui con gli strumenti elettronici si trattino esclusivamente dati personali *destinati alla diffusione*.

Da qualche anno a questa parte, si è constatato che il meccanismo delle parole chiave non è sufficientemente adeguato, a garantire un soddisfacente livello di sicurezza nella fase di autenticazione: le principali debolezze sono legate alla scelta di parole chiave estremamente facili da indovinare, da parte degli incaricati, ed alla possibilità di intercettarle quando transitano in rete. Per fare fronte a questi problemi, sono stati individuati dei meccanismi di *autenticazione forte*, che consentono di rendere molto più sicura tale procedura, basandosi sul riconoscimento di un *attributo posseduto* dall'incaricato, che può essere costituito da:

- una *caratteristica fisica*, quale l'impronta digitale, la forma della mano, l'iride, la retina, o una *caratteristica comportamentale*, quale la firma o la voce: in questo caso si parla di dispositivi di autenticazione *biometrici*
- una *parola chiave generata dinamicamente*, da un apposito dispositivo personalizzato per ciascun incaricato: in questo caso si parla di *one-time password*
- un *certificato digitale*, che attesta l'identità dell'utente, solitamente memorizzato su smart card. L'importanza di tale meccanismo, che si sta avviando a divenire quello di più generalizzata applicazione, è legata anche al fatto che esso può essere utilizzato anche per realizzare la *firma digitale* sui documenti, con ciò garantendo la loro autenticità, l'integrità dei messaggi, la non ripudiabilità e la confidenzialità.

Il disciplinare tecnico tiene conto, contrariamente a quanto faceva il Dpr 318/1999, delle novità tecnologiche che si sono affermate negli ultimi anni: ci si riferisce in particolare alla possibilità che, ai fini della realizzazione di un sistema di autenticazione, si possa prescindere completamente dall'impiego delle parole chiave, che il Dpr 318/1999 non contemplava.

Le nuove norme ammettono che, per realizzare la ***credenziale di autenticazione*** (cioè la *chiave* per accedere allo strumento elettronico), si possa ricorrere ad uno o più dei seguenti sistemi:

- associare un codice per l'identificazione dell'incaricato (*username)*, attribuito da chi amministra il sistema, ad una parola chiave riservata (*password*), conosciuta solamente dall'incaricato, che egli stesso provvederà ad elaborare, mantenere riservata e modificare periodicamente
- attribuire un dispositivo di autenticazione, in possesso ed uso esclusivo, all'incaricato (ad esempio, un tesserino magnetico, o una smart card)
- associare l'attribuzione di un dispositivo di autenticazione, posseduto ed utilizzato esclusivamente dell'incaricato, ad un codice identificativo o ad una parola chiave
- predisporre un dispositivo che rileva una caratteristica biometrica dell'interessato (ad esempio, le impronte digitali)
- associare un dispositivo, che rileva una caratteristica biometrica dell'incaricato, ad un codice identificativo o ad una parola chiave.

I successivi punti da 3. a 10. del disciplinare prescrivono le misure da osservare, per l'attribuzione e la gestione delle credenziali per l'autenticazione, in modo significativamente più restrittivo di quanto avveniva in vigenza del Dpr 318/1999: ci si riferisce in particolare alla regola, per cui *ad ogni incaricato* le credenziali per l'autenticazione (***anche più di una***) devono essere ***assegnate o associate individualmente***. Da tale regola consegue che non è più ammesso che due o più incaricati possano accedere agli strumenti elettronici utilizzando la medesima credenziale, come il Dpr 318/1999 consentiva invece nei seguenti casi:

- per l'accesso ad *elaboratori non in rete*, nelle ipotesi in cui le caratteristiche dell'elaboratore non consentivano l'autonoma sostituzione delle parole chiave da parte degli incaricati
- per l'accesso ad *elaboratori in rete*, limitatamente agli amministratori di sistema, cui è conferito il compito di sovrintendere al sistema stesso e di consentirne l'utilizzazione, nelle sole ipotesi in cui il sistema operativo prevedeva un unico livello di accesso per tale funzione.

Il punto 4. prevede che agli incaricati debbano essere *impartite precise istruzioni* su come:

- elaborare la *password*, e conservare la segretezza sulla stessa e sulle altre componenti riservate della credenziale di autenticazione (*username*), qualora per l'attribuzione delle credenziali di autenticazione si utilizzino le parole chiave
- custodire in modo diligente i dispositivi, in possesso ed uso esclusivo dell'incaricato, con i quali egli può accedere ad uno o più strumenti informatici (ad esempio, il tesserino magnetico o la smart card).

In merito al primo aspetto, il punto 5. codifica quali siano i requisiti minimi, che gli incaricati devono utilizzare nell'elaborare e modificare la *parola chiave* (*password*), che permette loro di accedere agli strumenti:

- deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non permetta una tale lunghezza, da un numero di caratteri pari al massimo consentito. E' buona norma che, di questi caratteri, da un quarto alla metà siano di natura *numerica*
- non deve contenere riferimenti agevolmente riconducibili all'interessato (non solo nomi, cognomi, soprannomi, ma neppure date di nascita proprie, dei figli o degli amici)
- non deve consistere in nomi del mondo Disney (*pippo*, *pluto*, *paperino*), e tanto meno nel nome e cognome *principe*, nel mondo italiano delle password, la mitica *pippobaudo*.

L'incaricato deve *provvedere a modificare la password*, con la seguente tempistica:

- ***immediatamente*, non appena la riceve per la prima volta, da chi amministra il sistema**
- **successivamente, *almeno* ogni sei mesi. Il termine scende a tre mesi, se la parola chiave dà accesso ad aree in cui sono contenuti dati sensibili o giudiziari.**

Il punto 6 impone che il codice per l'identificazione (*username*), che l'amministratore del sistema provvede a fornire all'incaricato, quale componente della *chiave* per accedere all'elaboratore, e successivamente a gestire, deve essere ***univoco***: esso non può essere assegnato ad altri incaricati, neppure in tempi diversi. La regola, che il Dpr 318/1999 imponeva ai soli elaboratori in rete, si estende quindi anche a quelli che non lo sono.

Il settimo e l'ottavo punto estendono a tutti gli strumenti elettronici le ipotesi, già previste dal Dpr 318/1999 per i soli elaboratori in rete, in cui si rende obbligatorio *disattivare le credenziali di autenticazione* (ad esempio, cancellando la funzionalità di una *username*, o ritirando un tesserino magnetico). La disattivazione deve avvenire nei seguenti casi:

- immediatamente, nel caso in cui l'incaricato perda la qualità, che gli consentiva di accedere allo strumento: ciò non accade solo se la persona cessa di lavorare, presso il soggetto che tratta i dati personali, ma può ad esempio avvenire anche se l'incaricato viene trasferito da un ufficio all'altro, con conseguente cambio delle mansioni e degli ambiti di trattamento dei dati personali, che rendesse necessaria l'attribuzione di una nuova *chiave*
- in ogni caso, entro sei mesi di mancato utilizzo. Fa ovviamente eccezione il caso delle *chiavi* che sono state *preventivamente autorizzate* per soli scopi di gestione tecnica, il cui utilizzo assume generalmente caratteristiche di sporadicità (ad esempio, potrebbero essere utilizzate solo una volta l'anno, nel quadro della verifica globale, sulla funzionalità complessiva del sistema).

Il punto 9 impone di impartire istruzioni agli incaricati, di non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento. Da tale prescrizione non consegue l'obbligo di *terminare la sessione* di lavoro, al computer, ogni volta che ci si deve allontanare, anche solo per cinque minuti. Si devono però mettere in atto accorgimenti tali, per cui *anche in quei cinque minuti* il computer non resti:

- *incustodito*: può essere sufficiente che un collega rimanga nella stanza, durante l'assenza di chi sta lavorando con lo strumento elettronico, anche se la stanza rimane aperta
- **e** *accessibile*: può essere sufficiente chiudere a chiave la stanza, dove è situato lo strumento elettronico, durante l'assenza, anche se nella stessa non rimane nessuno.

Non si devono invece mai verificare situazioni in cui lo strumento elettronico viene lasciato attivo, durante una sessione di trattamento, senza che la stanza in cui è ubicato venga chiusa, né vi sia nei paraggi almeno una persona di fiducia.

Il decimo punto si sofferma sui casi in cui l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante l'uso della componente riservata della *credenziale di autenticazione* (*password*), che l'incaricato ha provveduto ad elaborare e mantenere segreta, con la conseguenza che nessun altro deve conoscerla.

La regola generale, in questi casi, è che nessun altro, neppure il titolare del trattamento, può accedere allo strumento elettronico, utilizzando la *credenziale di autenticazione dell'incaricato*. Eccezione a tale regola si ha solo se verificano *congiuntamente* le seguenti condizioni:

- prolungata assenza o impedimento dell'incaricato
- l'intervento è indispensabile e indifferibile
- vi sono concrete necessità, di operatività e di sicurezza del sistema.

E' evidente che il titolare deve prendere le opportune misure, per essere in grado di accedere ai dati ed agli strumenti, al verificarsi delle condizioni sopra esposte. A tale fine, agli incaricati devono essere fornite istruzioni scritte, affinché essi:

- predispongano una *copia della parola chiave*, provvedendo quindi a trascriverla, facendo però in modo che l'informazione resti segreta (ad esempio, inserendola in una busta chiusa e, possibilmente, sigillata)
- consegnino tale copia ad un soggetto, che sia stato previamente incaricato della sua custodia (*l'incaricato per la custodia delle parole chiave*, figura già introdotta dal precedente Dpr 318/1999)
- solo al verificarsi delle condizioni, sopra esposte, che rendono necessario accedere allo strumento elettronico, utilizzando la copia della parola chiave, il titolare o un responsabile potranno richiedere la busta che la contiene, all'incaricato per la custodia. Dell'accesso effettuato si dovrà provvedere ad informare, tempestivamente, l'incaricato cui appartiene la parola chiave.

Il punto 11 prevede che le disposizioni sul sistema di autenticazione, analizzate nel presente paragrafo, *non si applicano ai trattamenti dei dati personali destinati alla diffusione*: la disposizione è ovvia, perché nell'ipotesi in esame si tratterebbero esclusivamente dati che, per definizione, sono *conoscibili da chiunque*, per cui non necessitano di alcuna forma di tutela.

13.2 Adozione di un sistema di autorizzazione

<table>
<tr><th colspan="2">NUOVO CODICE PRIVACY</th></tr>
<tr><td colspan="2">34[1] Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell’allegato B), le seguenti misure minime:
c) utilizzazione di un sistema di autorizzazione;
4[3] Ai fini del presente codice si intende per:
f) “profilo di autorizzazione”, l’insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
g) “sistema di autorizzazione”, l’insieme degli strumenti e delle procedure che abilitano l’accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.</td></tr>
<tr><th>DISCIPLINARE TECNICO</th><th>DPR 318/1999</th></tr>
<tr><td>Sistema di autorizzazione</td><td></td></tr>
<tr><td>12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.</td><td>5[1] Per il trattamento dei dati sensibili e giudiziari effettuato con elaboratori accessibili in rete, l'accesso per effettuare le operazioni di trattamento è determinato sulla base di autorizzazioni assegnate, singolarmente o per gruppi di lavoro, agli incaricati del trattamento o della manutenzione. Se il trattamento è effettuato con elaboratori accessibili in rete pubblica, sono oggetto di autorizzazione anche gli strumenti che possono essere utilizzati per l'interconnessione mediante reti disponibili al pubblico.
5[2] L'autorizzazione, se riferita agli strumenti, deve individuare i singoli elaboratori attraverso i quali è possibile accedere per effettuare operazioni di trattamento.</td></tr>
<tr><td>13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all’inizio del trattamento, in modo da limitare l’accesso ai soli dati necessari per effettuare le operazioni di trattamento.</td><td>5[4] L'autorizzazione all'accesso deve essere limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento o di manutenzione.
5[5] La validità delle richieste di accesso ai dati personali è verificata prima di consentire l'accesso stesso.
5[6] Non è consentita l'utilizzazione di un medesimo codice identificativo personale per accedere</td></tr>
</table>

	contemporaneamente alla stessa applicazione da diverse stazioni di lavoro.
14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.	**5[3]** Le autorizzazioni all'accesso sono rilasciate e revocate dal titolare e, se designato, dal responsabile. Periodicamente, e comunque almeno una volta l'anno, è verificata la sussistenza delle condizioni per la loro conservazione.
11. Le disposizioni sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.	**5[7]** Le disposizioni di cui ai commi da l a 6 non si applicano al trattamento dei dati personali di cui è consentita la diffusione.

Il secondo ordine di prescrizioni, previste dal comma 34, disciplina l'impostazione del sistema di autorizzazione, che la lettera g) del comma 3 dell'articolo 4 definisce come *l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente*. A tale fine, è previsto l'obbligo di:
lettera c) utilizzare un sistema di autorizzazione
lettera d) aggiornare periodicamente l'individuazione dell'ambito del trattamento consentito ai singoli incaricati, e agli addetti alla gestione o alla manutenzione degli strumenti elettronici.

Banalmente, con il sistema di ***autenticazione***, di cui al precedente paragrafo 6.1, si accerta l'identità della persona, per *farla entrare* nel computer. Con il sistema di ***autorizzazione*** si stabilisce a quali *aree (dati)* del computer l'incaricato può accedere, dopo che è entrato, e quali *azioni* (*trattamenti*) può compiere.

La prima differenza che balza all'occhio, rispetto all'analoga disposizione contenuta nel Dpr 318/1999, è riconducibile all'utilizzo, nel punto 12. del disciplinare, dell'espressione ***quando*** *sono individuati profili di autorizzazione di ambito diverso.* In alcuni casi, l'individuazione di tali profili può quindi avvenire, nel nuovo sistema, su base facoltativa, per cui *non vi è sempre e comunque l'obbligo* di individuare profili di autorizzazione diversi, per gli incaricati: ad esempio, in un'impresa nella quale lavorano cinque impiegati in tutto, si può decidere di non impostare alcun profilo di autorizzazione, per cui ognuno potrà accedere a tutti i dati personali, contenuti nella rete aziendale. Il Dpr 318/1999 era, su tale punto, più rigido, perché imponeva che fosse adottato un sistema di autorizzazione, senza alcuna eccezione, in caso di trattamento di dati sensibili o giudiziari mediante elaboratori in rete pubblica.

D'altra parte, si deve però considerare che, per ottemperare correttamente alle disposizioni privacy, con particolare riferimento a quella che impone di dare accesso ai soli dati personali necessari per svolgere le mansioni lavorative, è generalmente necessario **predisporre, per gli incaricati, profili di autorizzazione che coprano ambiti diversi: ad esempio, anche in una organizzazione relativamente piccola non sarebbe in alcun modo giustificabile che un impiegato dell'ufficio vendite potesse accedere ai dati personali relativi ai dipendenti, per cui si è di fatto costretti ad impostare diversi profili di autorizzazione.**

Se si decide, per scelta o per obbligo, di attribuire diversi *profili di autorizzazione*, l'amministratore del sistema deve studiare ed impostare un vero e proprio ***sistema di autorizzazione***, osservando le regole previste dai punti 13. e 14.

Analogamente a quanto prevedeva il Dpr 318/1999, il punto 13. ribadisce che il profilo di autorizzazione non deve essere necessariamente studiato per ogni singolo incaricato, ma può essere impostato anche per *classi omogenee di incaricati* (ad esempio, attribuendo un determinato profilo di autorizzazione a tutti gli impiegati della contabilità, ed attribuendone un altro a coloro che lavorano nell'ufficio personale).

L'obiettivo di fondo, in ogni caso, deve essere quello di *limitare preventivamente* l'accesso, di ciascun incaricato o di ciascuna classe omogenea di incaricati, ai soli dati necessari per effettuare le operazioni di trattamento, che si rendono indispensabili per svolgere le mansioni lavorative.

Per quanto concerne l'attribuzione dei profili, il Dpr 318/1999 imponeva che le autorizzazioni all'accesso dovessero essere rilasciate e revocate dal titolare e, se designato, dal responsabile: il nuovo disciplinare non si pronuncia sul punto, pur rimanendo ovvio che la materia rimane di competenza del titolare, o di chi ha incarichi di responsabilità (generalmente, l'*amministratore del sistema*).

Analoga alle previgenti disposizioni è la previsione, contenuta nel punto 14., per cui periodicamente, e comunque almeno annualmente, deve essere verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Il punto 11. chiarisce infine che non vi è obbligo di predisporre un sistema di autorizzazione, nel caso in cui il trattamento riguardi solo dati personali *destinati alla diffusione*: la disposizione è ovvia, perché nell'ipotesi in esame l'incaricato tratterebbe esclusivamente dati che, per definizione, sono *conoscibili da chiunque*, per cui non necessitano di alcuna forma di tutela.

13.3 Misure di protezione e per il ripristino dei dati

NUOVO CODICE PRIVACY
34[1] Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime: e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici; f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

L'articolo 34 del codice privacy impone di:
lettera e) proteggere gli strumenti elettronici ed i dati, rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici
lettera f) adottare procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi.

Si tratta di due facce della stessa medaglia, in quanto:
- da un lato, si devono proteggere strumenti e dati da trattamenti illeciti, accessi non consentiti e programmi intrusivi
- dall'altro, si devono adottare le opportune procedure, affinché al verificarsi di tali eventi, o di altri eventi anche accidentali di ordine distruttivo, le conseguenze siano minimizzate.

13.3.1 La protezione di strumenti e dati

DISCIPLINARE TECNICO	DPR 318/1999
16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.	**4[1c]** Nel caso di trattamenti effettuati con gli elaboratori in rete, gli elaboratori devono essere protetti contro il rischio di intrusione ad opera di programmi di cui all'art. 615-quinquies del codice penale, mediante idonei programmi, la cui efficacia ed aggiornamento sono verificati con cadenza almeno semestrale.
20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.	
17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.	

Il punto 16. del disciplinare prevede *l'obbligo generalizzato* (che il Dpr 318/1999 limitava invece ai soli elaboratori in rete) di proteggere i dati personali *contro il rischio di intrusione e dall'azione di programmi di cui all'art. 615-quinquies del codice penale,* aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento. Si tratta dei *virus ed amici*, dai quali la norma impone di difendersi, attivando idonei strumenti elettronici, da aggiornare con cadenza almeno semestrale (cadenza peraltro ridicola, se si pensa che, in molti casi, neppure l'aggiornamento settimanale è adeguato).

Il punto 20. aggiunge l'obbligo di adottare una ulteriore misura, in caso di trattamento di *dati sensibili o giudiziari*, imponendo di proteggerli *dall'accesso abusivo*, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici. Ai sensi dell'articolo 615-ter del codice penale, pone in essere un accesso abusivo chi *si introduce abusivamente in un sistema informatico o telematico, protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo*.

E' opportuno soffermarsi sulle differenze tra l'ipotesi di cui al punto 16. (*virus ed amici*) e quella in esame, in realtà sempre più sfumate, sotto l'aspetto delle possibili conseguenze pratiche:

- **nell'ipotesi di cui al punto 16., l'intruso è essenzialmente un *programma* che, per quanto pericoloso possa essere, non ha dietro una regia criminale che lo guida passo dopo passo**
- **nell'ipotesi in esame, l'intruso è invece la *mente criminale*, che utilizza una determinato programma, per accedere ad un sistema, e compiervi azioni illecite (tra le quali, per inciso, vi potrebbe essere il disseminare i simpatici programmi, di cui al punto 16.).**

La norma prevede che, nel caso in cui si trattino dati sensibili o giudiziari, non ci si possa limitare a difendersi dai programmi, ma si debbano utilizzare idonei strumenti elettronici (ad esempio, *firewall*), per proteggersi contro l'ipotesi, ancora più pericolosa, in cui la *mente criminale* stessa tenti di accedere direttamente.

> I Firewall sono dei sistemi hardware e software, dislocati nei punti di interconnessione tra reti TCP/IP distinte (ad esempio, tra la rete interna ed internet), che hanno il compito di controllare gli accessi alle risorse di rete interconnesse: tale controllo è effettuato filtrando i messaggi in transito e facendo passare solo quelli che rispondono ai requisiti definiti dalle politiche di sicurezza. Per la protezione dalla diffusione di software "maligno" tra le reti interconnesse, è opportuno che il Firewall disponga anche di opportune funzioni antivirus.

L'efficacia dei sistemi Firewall è strettamente correlata alla corretta configurazione e gestione dei diritti di privilegio, che devono essere accuratamente definiti e correttamente implementati: ai fini della verifica dell'efficacia e dell'efficienza, della soluzione Firewall implementata, è molto importante la verifica sia della corretta implementazione che della adeguata gestione, che va effettuata prima del rilascio in esercizio del sistema Firewall ed ogni qualvolta intervengano modifiche al sistema informativo. La verifica viene eseguita attraverso la conduzione di test di penetrazione del sistema di sicurezza, nonché attraverso la valutazione di adeguatezza delle procedure di gestione in essere.
E' superfluo evidenziare che l'obbligo di dotare gli strumenti elettronici di tali dispositivi non si estende agli elaboratori che non sono in rete, né dispongono di accesso ad Internet.

Il punto 17. prevede che, *in tutti i casi*, ci si debba dotare anche di programmi, la cui funzione è di:

- prevenire la vulnerabilità degli strumenti elettronici, non solo e non necessariamente per effetto di attacchi esterni
- correggere i difetti insiti negli strumenti stessi.

Tra i principali punti di debolezza di un sistema informatico vanno sicuramente annoverati il sistema operativo e le applicazioni, sfruttando gli eventuali errori (*bug*) presenti nei quali degli estranei potrebbero, tra l'altro, riuscire a guadagnare l'accesso al sistema. Le contromisure da adottare sono essenzialmente di due tipi:

- l'aggiornamento costante dei prodotti, non appena viene scoperto un *bug*: tale procedura è nota come installazione di *patch*
- la verifica periodica dell'installazione e della configurazione dei prodotti software.

Sono disponibili dei programmi, in grado di verificare automaticamente eventuali inconsistenze e inesattezze nella configurazione dei sistemi operativi e dei servizi di rete: la norma prevede che gli ***aggiornamenti di tali programmi*** debbano essere effettuati con cadenza almeno annuale (che diviene semestrale, in caso di trattamento di dati sensibili o giudiziari), nell'ambito di un *test generale* per verificare il corretto funzionamento dell'intero sistema.

13.3.1.1 Virus e programmi analoghi: approfondimenti

Fonte: AIPA – Linee guida per la definizione di un piano per la sicurezza dei sistemi informativi automatizzati nella pubblica amministrazione

I computer virus sono i rappresentanti più noti di una categoria di programmi, scritti per generare intenzionalmente una qualche forma di danneggiamento ad un computer o a una rete, che possono dare luogo a:

- danni all'hardware
- danni al software
- danneggiamento di dati
- perdita di tempo, impiegato a ripristinare le funzioni del sistema
- infezione di altri sistemi.

Una particolare categoria è costituita dai *macro virus* e dai cosiddetti *worm*, che sono in grado di :

- *infettare* altri programmi, cioè creare copie di sé stessi su altri programmi presenti nel sistema
- insediarsi nella tabella di partizione e nel settore di boot del disco rigido, dove attendono il verificarsi di un determinato evento, per potere assumere il controllo di alcune funzioni del sistema operativo, con il fine di svolgere le azioni dannose per cui sono stati programmati
- inserire operazioni automatizzate (c.d. macroistruzioni) in documenti di testo, di archivio o di calcolo, dagli effetti indesiderati e nocivi
- autoreplicarsi all'interno del sistema, al fine di saturarlo.

Le azioni di danneggiamento possono andare dalla modifica del contenuto di alcuni file, residenti sull'hard disk, alla completa cancellazione dello stesso; cosi come all'alterazione del contenuto del video o della impostazione hardware della tastiera.

La migliore difesa, contro tali programmi, consiste nel ***definire una architettura antivirus*** composta da regole comportamentali e da procedure operative, a protezione dell'intero sistema informatico: tutti gli utenti del sistema sono tenuti a conoscere e rispettare le regole emesse dall' organizzazione, e l'amministratore di sistema è tenuto a mantenere costantemente operative e aggiornate le procedure software predisposte.

Fattori di incremento del rischio e comportamenti da evitare

I seguenti comportamenti causano un incremento dei livelli di rischio informatico:

- riutilizzo di dischetti già adoperati in precedenza
- uso di software gratuito (o shareware) prelevato da siti internet o in allegato a riviste o libri
- uso di dischetti preformattati
- collegamento in rete, nel quale il client avvia solo applicazioni residenti nel proprio disco rigido
- collegamento in rete, nel quale il client avvia anche applicazioni residenti sul disco rigido del server
- uso di modem per la posta elettronica e prelievo di file da BBS o da servizi commerciali in linea o da banche dati
- ricezione di applicazioni e dati dall'esterno
- utilizzo dello stesso computer da parte di più persone
- collegamento in Internet con download di file eseguibili o documenti di testo da siti WEB o da siti FTP
- collegamento in Internet e attivazione degli applets di Java o altri contenuti attivi
- file attached di posta elettronica.

Norme basilari di comportamento

Al fine di evitare problemi correlati ad infezioni informatiche, dovranno essere rispettate le seguenti prescrizioni:

a) i floppy disk, sia quando vengono forniti sia quando vengono ricevuti, devono essere sottoposti a scansione, da parte del programma antivirus
b) è obbligatorio sottoporre a controllo tutti i floppy disk di provenienza incerta, prima di eseguire o caricare uno qualsiasi dei files in esso contenuti
c) non si deve utilizzare il proprio "disco sistema" su di un altro computer, se non in condizione di "protezione in scrittura"
d) proteggere in "scrittura" tutti i propri floppy disk di sistema, o contenenti programmi eseguibili
e) se si utilizza un computer che necessita di un "bootstrap" da floppy, usare un floppy disk protetto in scrittura
f) non attivare mai da floppy un sistema basato su hard disk, a meno di utilizzare un disco di sistema, protetto in scrittura e sicuramente non infetto

g) limitare la trasmissione di files eseguibili (.COM, .EXE, .OVL, .OVR) e di sistema (.SYS) tra computers in rete
h) non utilizzare i server di rete come stazioni di lavoro
i) non aggiungere mai dati o files ai floppy disk contenenti programmi originali.

Regole operative

1. Tutti i computer dell'organizzazione devono essere dotati di programmi antivirus
2. L'organizzazione deve assicurarsi che i computer delle società esterne, qualora interagiscano con proprio sistema informatico, siano dotati di adeguate misure di protezione antivirus
3. Il personale, delle ditte addette alla manutenzione dei supporti informatici, deve usare solo dischetti preventivamente controllati e certificati singolarmente ogni volta
4. Ogni P.C. deve essere costantemente sottoposto a controllo anti-virus
5. I dischetti provenienti dall'esterno devono essere sottoposti a verifica, da attuare con un P.C. non collegato in rete (macchina da quarantena), ed inoltre devono essere individuate le aree dell' organizzazione che, in relazione alla loro particolare attività, sono da considerare a più alto rischio, nei riguardi dell'infezione da virus
6. All'atto della individuazione di una infezione il virus deve essere immediatamente rimosso
7. Tutti gli utenti del sistema informatico devono sapere a chi rivolgersi per la disinfezione, e l'informazione dell'infezione deve essere mantenuta riservata
8. Il personale deve essere a conoscenza che la diffusione dei virus è punita dall'art. 615 quinquies del Codice Penale
9. Il software acquisito deve essere sempre controllato contro i virus e verificato, perché sia di uso sicuro, prima che sia installato.

Caratteristiche di base del software antivirus

Il software antivirus deve essere sottoposto a costante e frequente aggiornamento (almeno due volte al mese) ed in particolare:

a) gli aggiornamenti devono essere resi disponibili non solo per posta ma anche tramite BBS o Internet
b) deve essere particolarmente efficace contro i virus della nostra area geografica
c) deve potere effettuare automaticamente una scansione ogni volta che viene avviato un programma
d) deve potere effettuare una scansione automatica del floppy disk
e) deve accorgersi del tentativo di modificare le aree di sistema
f) deve essere in grado di effettuare scansioni a intervalli regolari e programmati
g) deve essere in grado di effettuare la scansione all'interno dei file compressi
h) deve mantenere il livello di protezione in tempo-reale
i) deve eseguire la scansione in tempo-reale
j) deve poter eseguire la rimozione del codice virale in automatico
k) in caso di impossibilità di rimozione, i file non pulibili devono essere spostati in una subdirectory predefinita

l) deve essere attivo nella protezione per Applet di ActiveX e Java contenenti un codice malizioso
m) deve essere in grado di effettuare la rilevazione/pulizia dei *virus da macro* sconosciuti
n) deve essere in condizione di rilevare e rimuovere i virus da macro senza file pattern, con un grado di riconoscimento superiore al 97 %
o) deve essere in grado di riconoscere i codici virali anche in file compattati utilizzando qualsiasi programma di compressione e in qualsiasi ambiente operativo.

Considerato che, in *sistemi basati su reti locali o su reti geografiche*, aumenta il pericolo di diffusione dei virus, ove possibile il sistema antivirus deve essere centralizzato e predisposto a svolgere almeno le funzioni di:

1. distribuzione degli aggiornamenti, sia dei motori di scansione che degli eventuali file "pattern"
2. controllo e monitoraggio degli eventi virali
3. automatico spostamento in directory di "quarantena" di virus informatici risultati non pulibili
4. avviso all'amministratore di sistema di rilevazione di virus e indicazione del file "infetto".

13.3.1.2 Il controllo sullo stato della sicurezza

La *verifica dell'efficacia e della validità* delle misure di sicurezza adottate è un punto fondamentale, nel processo per la sicurezza: in un contesto tecnologico in rapidissima evoluzione, è necessario avere le massime garanzie circa la adeguatezza delle misure di sicurezza adottate, nei confronti del sempre più vasto, articolato ed aggiornato panorama delle minacce possibili.

E' opportuno che l'attività di verifica si sostanzi in due attività distinte, sia per compiti, che per organizzazione:

- ***monitoraggio***: è l'attività di verifica *continua* della efficacia delle misure di sicurezza realizzate, al fine di intercettare il più presto possibile eventuali attacchi ai danni del sistema, non previsti in fase di definizione delle contromisure, o resi possibili da errori presenti o commessi in fase di installazione delle misure di sicurezza e degli apparati hardware e software ad esse collegati.
  Deve essere effettuata, *sotto la responsabilità della struttura che progetta e realizza le misure di sicurezza*, durante la progettazione, implementazione ed esercizio delle misure stesse.

Il metodo principale per effettuare il monitoraggio è costituito dalla raccolta ed analisi dei *log file*, nei quali i software di sicurezza installati, i sistemi operativi e le applicazioni scrivono tutte le principali operazioni svolte dagli utenti per il loro tramite. Attraverso questa analisi, che nelle organizzazioni complesse deve essere necessariamente effettuata adottando strumenti automatici di reportistica e di sintesi, è possibile individuare i tentativi, riusciti o meno, di accesso al sistema e l'esecuzione di operazioni sospette

- ***audit di sicurezza***: con tale termine si intende l'attività di verifica, effettuata da *una struttura diversa* da quella che ha implementato le misure di sicurezza, che potrà avvenire in modo estemporaneo, anche con verifiche casuali e non annunciate: la *periodicità è in genere annuale*, che può scendere a semestrale, o addirittura a trimestrale, nel caso delle organizzazioni più complesse.
  Obiettivo dell'audit di sicurezza è di verificare che tutte le misure implementate, sia quelle tecnologiche che quelle organizzative, svolgano correttamente le funzionalità per cui sono state adottate.

  I test specifici di verifica, delle ***misure tecnologiche***, possono essere effettuati con l'ausilio dei moderni strumenti di "network scanning": essi effettuano una approfondita analisi del sistema in esame, con lo scopo di individuare il livello di release e di patches dei sistemi operativi, dei middleware, degli applicativi installati e la configurazione dei relativi parametri di sicurezza, per confrontare poi queste informazioni con un database di "security flaws", denunciate dai produttori o individuati dalla comunità internazionale degli utenti**.** E' particolarmente importante affiancare a queste attività una serie di attacchi di tipo intrusivo (*test di penetrabilità*), che prevedano ad esempio tentativi esaustivi di individuazione delle password.
  Per quanto riguarda le ***misure organizzative***, va verificato il loro effettivo rispetto, da parte di tutti gli utenti coinvolti.
  Gli audit di sicurezza, richiedendo un notevole livello di specializzazione tecnica e necessitando di un elevato grado di imparzialità e di indipendenza, dalle organizzazioni aziendali coinvolte, vengono in genere affidati ad *organizzazioni esterne specializzate*: data la particolare delicatezza di queste attività, le organizzazioni esterne incaricate devono essere scelte per comprovata competenza ed esperienza professionale specifica, avallata da certificazioni, referenze e riconoscimenti verificabili.

Con riferimento alla normativa, sulle misure minime di sicurezza, e fermo restando che l'attività di *monitoraggio* è obbligatoria, in quanto necessaria per verificare il corretto funzionamento delle misure adottate, ci si chiede se sia implicitamente previsto anche l'obbligo di effettuare l'*audit di sicurezza*: in tale senso, tale attività potrebbe essere considerata un implicito completamento, del processo periodico di aggiornamento dei programmi per elaboratore, volto a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti, previsto dal punto 17. del disciplinare.
A parere di chi scrive, la risposta è negativa, nel senso che non è sempre e comunque imposto di procedere all'audit di sicurezza, la cui effettuazione si rende comunque opportuna per le organizzazioni più strutturate, nel quadro del processo di adozione e controllo delle misure *idonee* di sicurezza.

13.3.2 Le procedure per il ripristino dei dati

DISCIPLINARE TECNICO	DPR 318/1999
18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.	
23. Per i dati sensibili e giudiziari, sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.	

Per quanto concerne il salvataggio dei dati, al fine di consentirne il *recupero*, al verificarsi di eventi atti a distruggerli, il punto 18. prescrive che, in tutti i casi, debbano essere impartite istruzioni organizzative e tecniche, che prevedono il salvataggio dei dati *con frequenza almeno settimanale.* Si evidenzia che tale cadenza appare sovente inadeguata: meglio sarebbe procedere ai salvataggi ogni due giorni, o addirittura con cadenza giornaliera.

Per i dati *sensibili e giudiziari*, il punto 23 aggiunge la prescrizione, per cui l'organizzazione deve essere in grado di provvedere in ogni caso al ripristino dei dati *entro sette giorni*: in taluni casi, ciò può comportare la necessità di impiantare un vero e proprio *piano di continuità operativa*, con particolare riferimento alle ipotesi in cui la perdita dei dati sarebbe di rilevante nocumento, per le persone cui essi si riferiscono (ad esempio, è il caso delle cartelle cliniche).

13.3.2.1 Dal salvataggio dei dati al piano di continuità operativa

Fonte: AIPA – Linee guida per la definizione di un piano per la sicurezza dei sistemi informativi automatizzati nella pubblica amministrazione

I dati di un sistema sono sottoposti ad una serie di rischi, che ne minacciano continuamente la disponibilità, che possono andare dai mal funzionamenti hardware agli atti di vandalismo, perpetrati da intrusori informatici. E' possibile ridurre al minimo gli effetti, spesso disastrosi, di tali eventi, predisponendo una serie di accorgimenti tecnologici, quali ad esempio:

- *Sistemi RAID (Redundant array of inexpensive disks)*: si tratta di hard disk multipli, visti però dal sistema operativo come un singolo disco. La principale proprietà di questi dispositivi è quella di garantire la disponibilità e l'integrità dei dati, anche nel caso di guasto hardware di uno dei dischi che compongono il sistema
- *Back-up*: si tratta di una serie di procedure attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema,

su dispositivi opportuni. In caso di guasto hardware dei dischi è quindi possibile *ripristinare* il sistema nello stesso stato in cui si trovava, nel momento dell'ultimo back-up.

I back-up dovrebbero essere automatizzati e giornalieri, e la gestione dei supporti dovrebbe scongiurare i disastri derivanti da cause fisiche (incendi, allagamenti): è importante quindi predisporre armadi ad isolamento termico e/o magnetico, nonché copie multiple dei back-up (si consideri che anche i dispositivi di back-up possono guastarsi), da tenersi in luoghi differenti e distanti tra loro

- *Piano di continuità operativa*, che costituisce la forma più sofisticata di protezione dai rischi.

Il Piano di Continuità Operativa

Il piano di continuità operativa ha lo scopo di garantire la continuità e la disponibilità, degli strumenti e dei dati, in ipotesi di danneggiamenti causati da eventi accidentali, sabotaggi, disastri naturali. L'obiettivo del Piano di Continuità Operativa è quello di ripristinare i servizi informatici entro un tempo prestabilito, in funzione dei livelli di servizio attesi, e di rendere minime le perdite causate dall'interruzione dell'attività.

Ciò significa che il Piano di Continuità Operativa non deve essere inteso come misura alternativa, a quelle di prevenzione, ma è un completamento di queste ultime, al fine di :

- garantire la continuità dei principali processi, assicurando l'erogazione dei servizi essenziali
- limitare gli impatti degli eventi a carattere distruttivo sulla posizione finanziaria.

Il Piano di Continuità Operativa si occupa del controllo delle interruzioni di operatività, al fine di prevenirne e minimizzarne l'impatto, individuando un insieme specifico di contromisure di sicurezza, in grado di sostenere le operazioni critiche dell'organizzazione, anche attraverso infrastrutture alternative.

Lo scopo è quello di raggiungere e mantenere un sistema di operazioni che prevenga i rischi e, in caso di accadimento dell'evento distruttivo, ne limiti l'impatto sulla continuità dell'operatività: a tale fine, sarebbe opportuno attivare un processo di sviluppo e mantenimento di specifici piani, che includano misure di identificazione e riduzione del rischio orientate a limitare le conseguenze di un impatto dannoso, e ad assicurare un rapido ripristino delle operazioni essenziali.

Il processo di pianificazione della Continuità Operativa dovrebbe essere visto come un quadro di riferimento per la gestione di più procedure di ripristino, orientate a coprire scenari di impatto differenziati, in relazione ai diversi eventi dannosi: dalla semplice caduta di alimentazione fino agli eventi catastrofici che richiedono un vero e proprio Piano di *disaster recovery*.

La Continuità Operativa è un processo continuo che si articola in attività di analisi, progetto, attuazione e manutenzione di un piano che deve contemplare:

- identificazione e classificazione per priorità di ripristino di processi ed operazioni critici
- determinazione dei potenziali impatti di indisponibilità, rispetto ai diversi scenari di danneggiamento
- identificazione delle responsabilità ed adozione di contromisure tecniche ed organizzative
- documentazione dei processi e delle procedure concordate (di emergenza, di continuità, di ripristino)
- formazione specifica di tutto il personale sui processi e le procedure della Continuità Operativa
- test, manutenzione ed aggiornamento del piano.

La realizzazione del Piano di Continuità Operativa si basa quindi su contromisure, di carattere sia tecnologico che organizzativo, che indicano cosa fare, con quali risorse, e quali procedure seguire in condizioni di emergenza, che rendano il sistema informativo parzialmente o totalmente indisponibile.

I principali *aspetti tecnologici* riguardano:

- il recupero dei supporti di back-up
- il recupero delle transazioni perse
- il Disaster Recovery, nel caso di impatto per evento catastrofico. In questo caso la principale contromisura di carattere tecnologico consiste nel centro di back-up, che può essere realizzato in uno dei seguenti modi:
  - predisponendo una struttura tipo *scatola vuota*, di proprietà dell'organizzazione, o di tipo consortile o in service
  - raddoppiando il centro ed integrandolo in rete
  - creando un centro di recovery che può essere di proprietà dell'organizzazione, o di tipo consortile o in service.

  Dovrà inoltre essere predisposta una struttura di commutazione, che in caso di emergenza sia in grado di commutare l'utenza dal sistema principale a quello di back-up.

I principali *aspetti organizzativi* riguardano la definizione del piano dettagliato di chi fa cosa, dal momento della dichiarazione dello stato di emergenza a tutto il periodo (anche diversi mesi) durante il quale il centro primario potrebbe rimanere fuori servizio. Nulla deve essere lasciato al caso, per cui il piano dovrà comprendere:

- l'assegnazione delle responsabilità individuali
- le procedure di rilevamento e segnalazione
- il Piano di gestione dell'emergenza
- l'organizzazione della ripartenza delle operazioni essenziali (ripartenza automatica)
- il Piano di gestione della comunicazione verso le Direzioni, altre organizzazioni, il pubblico
- corsi di sensibilizzazione e formazione periodici

- la manutenzione del Piano: organizzazione di test regolari e revisioni di tutte le contromisure, le procedure ed i recovery plan.

L'*attività di manutenzione* del piano riveste particolare importanza, per evitare che il sistema stesso divenga rapidamente obsoleto ed inefficace a causa della:

- evoluzione tecnologica dei sistemi hardware e software, sia del proprio sistema informativo che, eventualmente, di quello del Centro di Back-up
- evoluzione organizzativa e logistica dell' organizzazione
- caduta di attenzione delle persone coinvolte
- cambiamento delle persone che occupano i ruoli interessati.

Se il piano non segue tempestivamente questi cambiamenti, perde di efficacia in breve tempo; l'unico modo per verificare che la manutenzione sia effettuata in modo adeguato è quello di programmare prove reali, o almeno "di carico", almeno due volte all'anno.

Si precisa che, nell'ambito delle misure minime di sicurezza, non è in generale previsto l'obbligo di adottare un piano di continuità operativa (salvi casi particolari, in cui la perdita di dati sarebbe di particolare nocumento per le persone cui essi si riferiscono), la cui complessità lo rende per inciso accessibile solo alle organizzazioni di rilevanti dimensioni: anche per esse, in considerazione del fatto che i Piani di Continuità in genere richiedono investimenti significativi, per la loro realizzazione, e' importante che essi vengano definiti, tenendo continuamente presente un corretto rapporto costi/benefici, *nei limiti della loro effettiva necessità*.

13.4 Custodia ed uso dei supporti rimovibili

DISCIPLINARE TECNICO	DPR 318/1999
21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati sensibili o giudiziari, al fine di evitare accessi non autorizzati e trattamenti non consentiti.	
22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.	**7[1]** Nel caso di trattamento dei dati sensibili e giudiziari effettuato con elaboratori in rete, i supporti già utilizzati per il trattamento possono essere riutilizzati qualora le informazioni precedentemente contenute non siano tecnicamente in alcun modo recuperabili, altrimenti devono essere distrutti.

Una particolare attenzione deve essere dedicata ai supporti rimovibili (es. dischetti), contenenti dati sensibili o giudiziari, nei seguenti termini:

- devono essere custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: ad esempio, si potranno impartire istruzioni, affinché essi vengano conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente *formattati*, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi
- una volta cessate le ragioni per la conservazione dei dati, i supporti non possono venire *abbandonati*, ma si devono porre in essere gli opportuni accorgimenti, finalizzati a rendere ***inintelligibili e non ricostruibili tecnicamente i dati*** in essi contenuti, al fine di impedire che essi vengano *carpiti* da persone non autorizzate al trattamento. Si devono quindi cancellare i dati, se possibile, o arrivare addirittura a distruggere il supporto, se necessario.

Nella sostanza, le prescrizioni in commento sono analoghe a quelle già introdotte dal Dpr 318/1999, con la differenza che con il nuovo codice esse sono imposte per i trattamenti effettuati con *tutti gli strumenti elettronici*, mentre il Dpr 318/1999 limitava l'obbligo ai casi di utilizzo di elaboratori *in rete*.

L'unica perplessità concerne il fatto che, analogamente a quanto veniva previsto dal precedente Dpr 318/1999, le misure in esame vengono imposte solo nel caso in cui i supporti contengano dati sensibili o giudiziari, invece di prevederne l'adozione generalizzata, per i supporti contenenti i dati personali di *qualsiasi natura*, anche comuni. Di fatto, si consiglia di seguire le prescrizioni in commento anche per i supporti contenenti solo dati comuni.

13.5 Il documento programmatico sulla sicurezza

CODICE PRIVACY	
34[1] Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime: g) tenuta di un aggiornato documento programmatico sulla sicurezza;	
DISCIPLINARE TECNICO	**DPR 318/1999**
19. Nel caso trattamento di dati sensibili o di dati giudiziari, si deve redigere un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:	**6[1]** Nel caso di trattamento dei dati sensibili e giudiziari effettuato mediante elaboratori accessibili in rete pubblica, deve essere predisposto e aggiornato un documento programmatico sulla sicurezza dei dati per definire:
19.4. le misure da adottare per garantire la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;	a) i criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi;
	c) i criteri e le procedure per la sicurezza delle trasmissioni dei dati, ivi compresi quelli per le restrizioni di accesso per via telematica;
19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;	d) l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire danni.

L'obbligo di redigere il documento programmatico di sicurezza viene generalizzato, a tutti in casi in cui si trattino dati ***sensibili o giudiziari con l'utilizzo di strumenti elettronici***, ***anche nell'ipotesi in cui tali strumenti non siano in rete*** (con il nuovo codice, è quindi sufficiente che tali dati siano trattati con un *singolo elaboratore*, perché si debba procedere alla redazione del documento). Il precedente Dpr 318/1999 limitava invece l'obbligo ai casi in cui tali dati erano trattati con elaboratori ***in rete pubblica***.

Alla redazione del documento in esame viene dedicato l'ottavo capitolo.
In questa sede è opportuno rilevare che, dall'obbligo di descrivere una determinata misura di sicurezza, ne consegue ovviamente che essa deve essere adottata. Da tale constatazione si desume che, oltre alle misure commentate nei precedenti paragrafi da 6.1. a 6.4, ai soggetti che devono redigere il documento programmatico sulla sicurezza è imposto l'obbligo di realizzare quanto segue:

- adottare misure che garantiscano la **protezione delle aree e dei locali** (punto 19.4 del disciplinare tecnico)
- effettuare **interventi formativi degli incaricati del trattamento** (punto 19.6 del disciplinare tecnico).

13.5.1 La protezione di aree e locali

E' l'insieme delle misura fisiche di sicurezza che hanno il compito di prevenire accessi fisici non autorizzati, danni o interferenze con lo svolgimento del lavoro con gli strumenti automatizzati: la protezione delle aree e dei locali, in cui sono situati gli elaboratori, deve essere quindi attivata sia contro eventi dannosi imprevedibili (inondazioni, corti circuiti, ecc.), che contro tentativi di intrusione.

Le contromisure si riferiscono alle protezioni perimetrali dei siti, ai controlli fisici all'accesso, alla sicurezza delle *computer room* rispetto a danneggiamenti accidentali o intenzionali, alla protezione fisica dei supporti.

Tale obiettivo viene raggiunto attraverso misure di controllo crescenti, correlate ai rischi e al valore dei beni e delle informazioni presenti nell'ambiente. Ne fanno parte le seguenti componenti:

- la classificazione delle aree aziendali (es: aree riservate, aree interne, aree pubbliche)
- l'accesso controllato alle aree considerate critiche
- la sicurezza fisica (impianti) e la sorveglianza di queste aree
- la tempestiva rilevazione di eventuali incidenti di sicurezza.

13.5.2 Gli interventi formativi degli incaricati

Gli **interventi formativi degli incaricati del trattamento** devono essere programmati in modo tale, che essi abbiano luogo *almeno* al verificarsi di una delle seguenti circostanze:

- già al momento dell'ingresso in servizio
- in occasione di cambiamenti di mansioni, che implichino modifiche rilevanti rispetto al trattamento di dati personali
- in occasione della introduzione di nuovi significativi strumenti, che implichino modifiche rilevanti rispetto al trattamento di dati personali.

Gli interventi formativi, che possono avvenire all'interno e/o presso soggetti esterni specializzati, devono essere finalizzati a rendere gli incaricati edotti dei seguenti aspetti:

- profili della disciplina sulla protezione dei dati personali, più rilevanti in rapporto alle relative attività, e conseguenti responsabilità che ne derivano
- rischi che incombono sui dati
- misure disponibili per prevenire eventi dannosi
- modalità per aggiornarsi sulle misure minime di sicurezza, adottate dal titolare.

13.5.2.1 L'introduzione e diffusione della cultura della sicurezza

Lungi dal concretizzarsi in *sonnacchiose riunioni*, di buon grado sopportate solo perché si è in uno stato di *semi-vacanza*, gli interventi formativi dovrebbero essere una importante componente della più vasta **cultura della sicurezza**, nel trattamento del patrimonio informativo dell'organizzazione, con particolare riferimento ai dati personali.
Si riassumono alcune considerazioni in merito, tratte dal già citato documento AIPA.

Sensibilizzazione e corresponsabilizzazione

> La sensibilizzazione alle tematiche della sicurezza, ed a costanti comportamenti coerenti con le disposizioni date in merito, deve interessare tutte le risorse umane dell'organizzazione, ad ogni livello di responsabilità ed attività: ciò al fine di diffondere una cultura generalizzata della sicurezza, che consenta tra l'altro di favorire la miglior efficacia ed efficienza delle misure prese, oltre che di sopperire ad eventuali mancanze delle stesse.

Le organizzazioni devono tenere presente che le attività relative alla sicurezza non rappresentano un appesantimento del lavoro quotidiano, ma una volta che entrano nel ciclo standard delle operazioni da compiere, contribuiscono a garantire il personale dal rischio di perdere, o comunque compromettere, parte del lavoro fatto.
A titolo di esempio, presentazioni, opuscoli, seminari, riunioni dei dirigenti con i propri collaboratori possono rappresentare opportunità per raggiungere quest'obiettivo.

Per la corresponsabilizzazione, si deve prevedere di:

- coinvolgere i dirigenti e le rappresentanze degli addetti, in tutte le fasi di definizione del piano per la sicurezza
- effettuare interventi di richiamo, e se necessario adottare gli adeguati provvedimenti disciplinari, in caso di inadempienze e/o superficialità in tema di sicurezza.

Analoghi processi devono essere previsti con eventuali partner e per i collaboratori esterni, privati e pubblici, persone fisiche e giuridiche, che interagiscono in modo significativo con l'organizzazione.

Formazione

L'introduzione di un sistema di sicurezza, come di qualunque altro elemento che modifichi le modalità lavorative all'interno di una qualsiasi realtà, ha sicuramente un forte impatto sull'organizzazione. La formazione interviene in due momenti ben precisi del processo di introduzione di un sistema di sicurezza:

- sensibilizzazione sulle problematiche della sicurezza e sulla loro importanza
- conoscenza delle misure di sicurezza da adottare, e da gestire ai diversi livelli di responsabilità.

A tale fine, occorre progettare due tipi di corsi, distinti a seconda dei destinatari:

- il primo, indirizzato alla direzione, deve prevedere cenni sulla normativa, indicazioni sulle politiche di sicurezza, analisi dei rischi
- l'altro, indirizzato al personale operativo, deve fornire indicazioni precise sui comportamenti da adottare, sia nelle operazioni quotidiane che nelle situazioni di emergenza.

La formazione, se ben orientata, progettata e realizzata, può essere lo strumento più efficace per realizzare la diffusione delle politiche, degli obiettivi e dei piani dell'organizzazione in tema di sicurezza e per minimizzare quella componente, sempre presente, che consiste nella resistenza al cambiamento.

Inoltre è necessario rivedere ed aggiornare annualmente i Piani di formazione in relazione alle mutate esigenze dell'organizzazione ed allo sviluppo delle tecnologie (di attacco alla sicurezza e di difesa).

13.5.3 La sicurezza nella trasmissione dei dati

A differenza di quanto prescriveva il Dpr 318/1999, non viene più imposto in modo specifico di *adottare criteri e procedure per la sicurezza delle* ***trasmissioni dei dati****, ivi compresi quelli per le restrizioni di accesso per via telematica*: l'adozione di tali criteri e procedure si renderà quindi necessaria nei soli casi in cui essa è indispensabile, per garantire l'integrità e la disponibilità dei dati (che sono peraltro sempre più frequenti, nella pratica, come è da ultimo attestato dall'obbligo di trasmettere in via digitale gli atti alle Camere di Commercio).

Per i fini in esame, è importante l'utilizzo della crittografia, ed in particolare della ***firma digitale***, basata su una *infrastruttura tecnologica di crittografia a chiave pubblica*. Essa offre, in sede di trasmissione dei dati, i seguenti servizi:

- **riservatezza**, al fine di impedire che terzi, portando attacchi nel corso della trasmissione dei dati, possano carpire indebitamente informazioni
- **integrità**, che permette di verificare, in fase di ricezione, se durante la trasmissione sono state indebitamente apportate modifiche, alle singole unità dei dati o alla sequenza delle stesse
- **autenticazione**, che garantisce il ricevente sull'autenticità del mittente e dei dati ricevuti
- **non ripudio**, che fornisce la prova incontestabile dell'avvenuta spedizione, o dell'avvenuta ricezione dei dati, con la duplice valenza di:
  - non ripudio *dell'origine*, atto a provare chi è il mittente di una spedizione
  - non ripudio *della destinazione*, atto a provare che la spedizione è arrivata ad uno specifico destinatario.

13.6 Ulteriori prescrizioni per gli organismi sanitari

CODICE PRIVACY
34[1] Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime: h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.
DISCIPINARE TECNICO
24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Agli organismi sanitari, siano essi pubblici o privati, e agli esercenti le professioni sanitarie, che trattano particolari dati sensibili (idonei a rivelare lo *stato di salute* o la *vita sessuale*), la lettera h) del comma 1 dell'articolo 34 impone l'adozione di *tecniche di cifratura* o di *codici identificativi*.
Il punto 24. del disciplinare tecnico sviluppa tale prescrizione, nei termini che seguono.

I dati idonei a rivelare lo stato di salute o la vita sessuale, contenuti in elenchi, registri o banche dati, tenuti con l'ausilio di strumenti elettronici, devono essere trattati con tecniche di cifratura, o mediante l'utilizzazione di codici identificativi o di altre soluzioni tecniche, che permettano di:

- rendere temporaneamente inintelligibili tali dati, anche a chi è autorizzato ad accedervi: letta al contrario, la disposizione può essere realizzata prevedendo che, per accedere a tali dati, chi ha l'autorizzazione deve compiere una particolare azione (ad esempio, inserire una ulteriore parola chiave), in mancanza della quale l'accesso ai dati è impedito. Per la protezione di dati conservati su file si possono utilizzare strumenti, genericamente chiamati *crypto file system*, che utilizzando tecniche crittografiche consentano di cifrare il contenuto dei file, in modo che lo stesso contenuto possa essere "letto" solo da utenti in possesso di un particolare codice
- identificare gli interessati solo in caso di necessità: si rende quindi necessario adottare i necessari accorgimenti, per potere trattare in modo *disgiunto* i dati in esame, dagli altri dati che permettono di identificare direttamente gli interessati.

Una ulteriore serie di precauzioni deve essere adottata, per i dati *relativi all'identità genetica*, che:

- possono essere trattati esclusivamente all'interno di locali protetti, accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi
- nel caso in cui debbano essere fisicamente trasportati, all'esterno dei locali riservati al loro trattamento, il trasporto deve avvenire in contenitori muniti di serratura o dispositivi equipollenti
- nel caso in cui vengano trasferiti in formato elettronico, il trasferimento deve essere cifrato.

13.7 Il certificato di conformità

DISCIPLINARE TECNICO
25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

I soggetti esterni che, professionalmente, assistono il titolare nella predisposizione ed installazione delle misure minime di sicurezza, devono rilasciare un **certificato di conformità**, alle disposizioni del *disciplinare tecnico*, nel quale devono inoltre descrivere quale sia stato l'intervento effettuato.
La disposizione è atta a garantire la serietà degli interventi, in quanto l'installatore viene in prima persona assoggettato alle responsabilità, di ordine non solo civile, ma anche penale, conseguenti all'eventuale inadeguatezza delle misure di sicurezza impiantate, rispetto a quanto richiesto dal disciplinare tecnico.

14 I dati personali affidati dal titolare all'esterno

Il nuovo codice privacy introduce una nuova prescrizione, atta a salvaguardare la sicurezza, nel caso di trattamenti di dati personali che il titolare *affida all'esterno della propria struttura*.
Che il titolare non potesse disinteressarsi di tali dati era già pacifico, in vigenza della L 675/1996: si richiamano a tale riguardo le considerazioni, esposte nel secondo capitolo, in merito ai confini generali della corresponsabilità di titolare e responsabile, che trova applicazione anche nelle ipotesi in cui questo sia un soggetto esterno.
La novità consiste nel fatto che il nuovo disciplinare tecnico impone al titolare di adottare ***precisi criteri***, atti a garantire che il soggetto esterno tratti i dati sensibili e giudiziari, che gli sono stati affidati, *adottando le misure minime di sicurezza* prescritte dalla norma.
La disposizione è dettata per i trattamenti effettuati *mediante l'utilizzo di strumenti elettronici*: a tale proposito, si deve avere riguardo alle modalità di trattamento *poste in essere dal soggetto esterno*, non a quelle del titolare. Ad esempio, si supponga che un soggetto tratti i dati sensibili del personale *esclusivamente su supporto cartaceo*, al fine di comunicare i periodi di malattia, ed informazioni analoghe sullo stato di salute dei dipendenti, alla società esterna che elabora le paghe: se questa società utilizza, in tale attività, strumenti elettronici, il datore di lavoro sarà tenuto ad accertarsi che essa adotti le misure minime di sicurezza, previste dalla normativa privacy.

Si evidenzia che, nell'ipotesi in cui il titolare del trattamento sia tenuto a redigere il *documento programmatico sulla sicurezza*, in esso andranno descritti i criteri adottati, per garantire l'adozione delle misure minime di sicurezza da parte del soggetto esterno, al quale i dati personali vengono affidati.

CODICE PRIVACY
34[1] Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime: g) tenuta di un aggiornato documento programmatico sulla sicurezza;
DISCIPLINARE TECNICO
19. Nel caso trattamento di dati sensibili o di dati giudiziari, si deve redigere un documento programmatico sulla sicurezza contenente idonee informazioni riguardo: 19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare.

14.1 I possibili criteri

Pur in assenza, per il momento, di chiarimenti ufficiali, si possono individuare alcune modalità, atte a rafforzare la garanzia che l'affidatario dei dati osservi le regole, in materia di misure minime di sicurezza.
Nella generalità dei casi, dovrebbe ad esempio essere sufficiente che:

- l'affidatario dichiari, su carta intestata, di avere redatto il documento programmatico sulla sicurezza, nel quale ha attestato di avere adottato le misure minime previste dalla legge. In casi particolari, potrebbe essere opportuno esigere dall'affidatario copia di tale documento
- se l'affidatario si è avvalso, per le problematiche inerenti la sicurezza, di un soggetto esterno, che di conseguenza ha rilasciato il *certificato di conformità*, può essere sufficiente ottenere copia dello stesso.

In casi specifici, nei quali l'affidamento dei dati assume una importanza particolare (per la natura particolarmente *delicata* degli stessi e/o perché vengono trasferite banche dati di notevole rilievo), è opportuno ricorrere a vere e proprie *clausole contrattuali*, che disciplinino gli aspetti legati alla gestione dei dati personali.

14.2 Le clausole contrattuali

Nel presente paragrafo di riporta una bozza delle clausole contrattuali, frutto dell'elaborazione di quelle predisposte dalla Commissione CEE, per ipotesi analoghe a quella in commento (Decisione della Commissione CE 2002/16/CE del 27 dicembre 2002). Nei casi in cui l'affidatario è residente in un Paese extra – Ue, che non offre idonee garanzie per il trattamento di dati personali, è obbligatorio adottare la formulazione integrale delle clausole contrattuali, contenute in tale decisione, che è riportata negli allegati al presente manuale.

Nome ed indirizzo dell'organizzazione affidante: …….(«**l'affidante**»)

e

Nome ed indirizzo dell'organizzazione affidataria: («**l'affidatario**»)

HANNO CONVENUTO

le seguenti clausole contrattuali («nel prosieguo: le clausole») al fine di prestare garanzie sufficienti per la tutela della riservatezza, delle libertà e dei diritti fondamentali delle persone, con riguardo al trasferimento dall'affidante all'affidatario dei dati personali indicati nell'appendice 1, che costituisce parte integrante delle presenti clausole.

Clausola 1 - Definizioni

Ai fini delle presenti clausole si applicano le definizioni dell'articolo 4 Dlgs 196/2003 («nel prosieguo: codice privacy»).

Clausola 2 - Particolari del trasferimento

I particolari del trasferimento sono indicati nell'appendice 1.

Clausola 3 - Obblighi dell'affidante

L'affidante dichiara e garantisce quanto segue:

a) che il trattamento dei dati personali, compreso il loro trasferimento, viene effettuato, e continuerà ad essere effettuato in conformità a tutte le disposizioni pertinenti della normativa sulla protezione dei dati;
b) che egli ha prescritto all'affidatario - e continuerà a farlo durante l'intero periodo in cui sono prestati i servizi di trattamento dei dati - di elaborare i dati personali trasferiti soltanto per suo conto e in conformità alla normativa sulla protezione dei dati e alle presenti clausole;
c) che l'affidatario fornisce sufficienti garanzie per quanto riguarda le misure minime di sicurezza, indicate nell'Allegato B del codice privacy;
d) che, alla luce della normativa sulla protezione dei dati, le misure di sicurezza sono idonee a proteggere i dati personali contro la distruzione accidentale o illecita, l'alterazione, e la trasmissione o l'accesso non autorizzati, in particolare qualora il trattamento comprenda la trasmissione di dati su rete, nonché contro ogni altra forma di trattamento illecito, e garantiscono un livello di sicurezza commisurato ai rischi connessi al trattamento ed alla natura dei dati che devono essere protetti, tenuto conto della più recente tecnologia e dei costi d'attuazione;

e) che provvederà all'osservanza delle misure di sicurezza.

Clausola 4 - Obblighi dell'affidatario

L'affidatario dichiara e garantisce quanto segue:

a) che tratterà i dati personali soltanto per conto dell'affidante e in conformità alle sue istruzioni, nonché alle presenti clausole; egli si impegna ad informare prontamente l'affidante qualora non possa per qualsiasi ragione ottemperare a tale disposizione; in tal caso l'affidante ha facoltà di sospendere il trasferimento e/o risolvere il contratto;
b) che ha applicato le misure tecniche e organizzative di sicurezza indicate nell'Allegato B del codice privacy, prima di effettuare il trattamento dei dati personali trasferiti;
c) che risponderà prontamente e adeguatamente a tutte le richieste dell'affidante, relative al trattamento dei dati personali soggetti a trasferimento;
d) che sottoporrà i propri impianti di trattamento, su richiesta dell'affidante, al controllo dell'affidante o di un organismo ispettivo composto da soggetti indipendenti, in possesso delle necessarie qualificazioni professionali, vincolati da obbligo di riservatezza e selezionati dall'affidante.

Clausola 5 - Responsabilità

Le parti convengono che se una di esse viene riconosciuta responsabile di una violazione delle clausole, commessa dall'altra, quest'ultima, nei limiti della sua responsabilità, è tenuta a indennizzare la prima per ogni costo, onere, danno, spesa o perdita sostenuti.

Tale indennizzo è subordinato al fatto che:

a) l'affidante informi prontamente l'affidatario in merito alle istanze presentate; e
b) l'affidarario abbia la possibilità di collaborare con l'affidante, nella difesa e nella risoluzione della controversia.

Clausola 6 - Obblighi al termine dell'attività di trattamento dei dati personali

1. Le parti convengono che al termine dell'attività di trattamento l'affidatario provvede, a scelta dell'affidante, a restituire a quest'ultimo tutti i dati personali trasferiti e le relative copie o a distruggere tali dati, certificando all'affidante l'avvenuta distruzione, salvo che gli obblighi di legge impediscano di restituire o distruggere in tutto o in parte i dati personali trasferiti. In questo caso, l'affidatario si impegna a garantire la riservatezza dei dati personali trasferiti e ad astenersi dal trattare di propria iniziativa tali dati.

2. L'affidatario si impegna a sottoporre a controllo i propri impianti di trattamento su richiesta dell'affidante, ai fini della verifica dell'esecuzione dei provvedimenti di cui al paragrafo 1.

Appendice 1 - Alle clausole contrattuali tipo

Affidante

(specificare brevemente le attività pertinenti al trasferimento):

……...

Affidatario

(specificare brevemente le attività pertinenti al trasferimento):

……...

Soggetti interessati dai dati

I dati personali trasferiti interessano le seguenti categorie di soggetti (specificare):

……...

Categorie di dati oggetto di trasferimento

I dati trasferiti interessano le seguenti categorie di dati (specificare):

……...

Categorie di dati sensibili e/o giudiziari

Il trasferimento interessa le seguenti categorie di dati sensibili e/o giudiziari (specificare):

……...

Operazioni di trattamento

I dati personali trasferiti saranno sottoposti alle seguenti attività principali di trattamento (specificare):

……

15 Il documento programmatico sulla sicurezza: come redigerlo

L'obbligo di redigere il documento programmatico sulla sicurezza viene generalizzato, a tutti in casi in cui si trattino dati ***sensibili o giudiziari con l'utilizzo di strumenti elettronici***, anche nell'ipotesi in cui tali strumenti non siano in rete (con il nuovo codice, è quindi sufficiente che tali dati siano trattati anche con un *singolo elaboratore*, perché si debba procedere alla redazione del documento). Viene inoltre fissato un termine generale, **entro il 31 marzo di ogni anno**, per la ***redazione*** e, negli anni successivi, l'***aggiornamento periodico*** di tale documento.

Per il solo anno 2004, il Garante ha **fissato al 30 giugno 2004** il termine ultimo(oggi prorogato al 31 dicembre), entro il quale redigere per la prima volta o aggiornare il documento (si veda la risoluzione del 22 marzo, negli Allegati al presente manuale). L'Autorità ha imposto tale scadenza a tutti i soggetti che trattano dati sensibili o giudiziari con elaboratori, per cui si osserva quanto segue:

- per i soggetti che erano già tenuti alla redazione del DPSS, in vigenza del Dpr 318/1999, il più lungo temine del 30 giugno è motivato dal fatto

che nel *nuovo* DPSS si devono includere informazioni aggiuntive, rispetto a quelle in precedenza richieste, e si deve inoltre dare conto di avere adottato, o di essere in procinto di adottare, misure di sicurezza che possono essere in parte *nuove*, rispetto a quelle previste dal Dpr 318/1999 stesso.
Per inciso, tali soggetti sono tenuti a redigere il DPSS per il 2004 entro il 30 giugno anche nell'ipotesi in cui, a tale data, sia trascorso meno di un anno dall'ultimo aggiornamento effettuato in base alle *vecchie* regole, previste dal Dpr 318/1999

- per i soggetti che non erano tenuti alla redazione del DPSS, in vigenza del Dpr 318/1999, ma lo sono ai sensi del nuovo codice privacy, la scadenza del 30 giugno 2004, imposta dal Garante, costituisce in realtà un *anticipo*, rispetto alla data che si sarebbe potuta ipotizzare, dalla lettura della norma (31 marzo 2005). Il Garante ritiene infatti che non sussistano margini per sostenere che, nel caso in esame, il DPSS possa essere redatto per la prima volta solo nel 2005
- la stessa regola vale per i soggetti che, disponendo di strumenti elettronici tecnicamente inadeguati, redigono entro il 31 dicembre 2004 un documento avente data certa, per differire a marzo 2005 il termine ultimo entro cui adottare le nuove misure minime di sicurezza. Se trattano dati sensibili o giudiziari con l'utilizzo di elaboratori, tali soggetti devono comunque rispettare il termine del 30 giugno(oggi prorogato al 31 dicembre) per redigere per la prima volta, o aggiornare, il DPSS, in quanto il Garante ha affermato che si tratta di una *misura da adottare con un documento, non di un accorgimento da applicare direttamente a strumenti elettronici, per cui non è possibile invocare un differimento al 2005, neppure in applicazione dello speciale meccanismo a proposito delle obiettive ragioni tecniche relative a strumenti elettronici*.

Una novità di ordine assoluto è prevista dal punto 26. del disciplinare tecnico, ai sensi del quale ***il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza****:* come è facilmente intuibile, tale disposizione è atta a rafforzare l'obbligo di redigere ed aggiornare il DPSS. Non a caso, esso è divenuto in questi giorni *di moda*, come attestano le numerose *vetrine* che ad esso stanno dedicando i principali quotidiani economici, dopo che nei primi quattro anni di esistenza era vissuto in uno stato di semi-clandestinità.

Un primo punto riguarda il significato che, per gli scopi in esame, si deve attribuire al termine ***bilancio di esercizio***, alla luce di un passaggio della risoluzione del 22 marzo 2004 del Garante, nella quale l'Autorità afferma che *i* ***soggetti*** *pubblici e privati devono riferire* nella relazione accompagnatoria: il fatto che il Garante non limiti il riferimento alle sole società pubbliche o private, ma lo estenda ai *soggetti* in generale, può fare ritenere che tale obbligo ricada non solo sulle società, tenute alla predisposizione del bilancio ai sensi del codice civile, ma anche su enti di natura diversa, comunque tenuti a predisporre un documento contabile annuale assimilabile ad un

bilancio societario. Tale interpretazione appare plausibile, alla luce delle finalità generali per cui è stato introdotto l'obbligo in esame.

Un secondo punto concerne il significato di ***relazione accompagnatoria del bilancio di esercizio***: se a tale termine viene data una interpretazione strettamente civilistica, con tale documento si deve intendere la relazione sulla gestione di cui all'articolo 2428 del codice civile, che deve essere tassativamente allegata al bilancio di esercizio solo dai soggetti che lo redigono *in forma ordinaria*. I soggetti che, potendo redigere il bilancio in *forma abbreviata* ai sensi dell'articolo 2435-bis del codice civile, si avvalgono dalla facoltà di non redigere la relazione sulla gestione, non dovrebbero invece essere tenuti a dare informazioni sul DPSS nella nota integrativa: tale documento è infatti considerato a tutti gli effetti una parte integrante del bilancio di esercizio, non un suo *accompagnamento*. Nulla osta ad una eventuale interpretazione in senso opposto, da parte del Garante: l'Autorità potrebbe infatti stabilire che, analogamente a quanto avviene per le informazioni richieste dai numeri 3) e 4) dell'articolo 2428 c.c., anche le informazioni in merito alla redazione del DPSS debbano essere incluse nella nota integrativa, qualora ci si avvalesse della facoltà di non redigere la relazione sulla gestione (si evidenzia che tale interpretazione non è stata, per il momento, fatta propria dal Garante, in sede di adozione del provvedimento del 22 marzo 2004).

Un terzo punto riguarda i soggetti che non sono tenuti a redigere il DPSS, poiché non trattano dati sensibili o giudiziari con l'utilizzo di strumenti elettronici: in questi casi, è opportuno che nella relazione accompagnatoria al bilancio di esercizio essi attestino di *non essere tenuti alla redazione del DPSS, in quanto non trattano dati sensibili o giudiziari con l'utilizzo di strumenti elettronici.*

Un quarto punto concerne quale debba essere il DPSS al quale si deve fare riferimento, nella relazione accompagnatoria del bilancio d'esercizio: se quello redatto nel periodo cui il bilancio si riferisce (es. nel corso del 2003, per la relazione accompagnatoria che viene predisposta nei primi mesi del 2004), ovvero l'ultimo redatto, prima dell'approvazione della relazione accompagnatoria: la risoluzione del Garante del 22 marzo 2004 fa propria questa seconda interpretazione, che appariva già pacifica in sede di lettura della legge. In tale ottica, la scadenza generale del 31 marzo non è casuale, ma è stata introdotta affinché le società con esercizio coincidente con l'anno solare redigano il DPSS prima di formalizzare la relazione accompagnatoria del bilancio, nella quale si dovrà quindi fare riferimento al DPSS *fresco di stampa*.

Regole particolari si applicano per la relazione accompagnatoria al bilancio di esercizio 2003, che molti soggetti si stanno accingendo a formalizzare in questi giorni, in relazione al *regime transitorio* fissato per il 2004 per la redazione del DPSS. Si esaminino quattro possibili casi, che si ottengono incrociando due coordinate:

- sulle righe si distinguono i soggetti che, alla luce delle vecchie regole, previste dal Dpr 318/1999, non erano tenuti alla redazione del DPSS (**NO**) da quelli che erano già obbligati alla redazioni dello stesso (**SI)**
- sulle colonne si tiene conto del comportamento di fatto tenuto dai soggetti, indicando **NO** se essi non hanno mari redatto il DPSS, **SI** se lo hanno redatto in vigenza della vecchia normativa:

SOGGETTI CHE IN PASSATO HANNO **EFFETTIVAMENTE REDATTO** IL DPSS		SOGGETTI **GIA' OBBLIGATI**, DAL DPR 318/19999, A REDIGERE O AGGIORNARE IL DPSS	
	SI	***CASO 2***	***CASO 3***
	NO	***CASO 1***	***CASO 4***
		NO	**SI**

Il ***CASO 1*** non presenta particolari problemi: i soggetti che non erano obbligati dal Dpr 318/1999 a redigere il DPSS, e che di conseguenza non l'hanno fatto, procederanno alla sua redazione entro il 30 giugno 2004(oggi prorogato al 31 dicembre), per riferire della circostanza nella prima relazione sulla gestione che formalizzeranno dopo tale data. Nella particolare ipotesi in cui tali soggetti avessero già redatto il DPSS, nei primi mesi del 2004, faranno riferimento ad esso nella relazione sulla gestione relativa all'anno 2003, che si stanno apprestando a formalizzare in questi giorni.

Il ***CASO 2***, definibile con il termine *mosca bianca*, è costituto dai soggetti che, pur non essendo tenuti negli anni trascorsi a redigere ed aggiornare il DPSS, sulla base del Dpr 318/1999, lo hanno fatto a titolo facoltativo: ad essi è data facoltà, mentre non vi è obbligo, di accennare nella relazione al bilancio di avere provveduto alla redazione del documento. Tale regola è generale, per cui troverà applicazione anche per i soggetti che, pur non essendo tenuti a redigere il DPSS neppure alla luce delle regole introdotte dal nuovo codice privacy, riterranno comunque di farlo.

Il ***CASO 3*** è costituito dai soggetti che, essendo già tenuti a redigere o ad aggiornare il DPSS, alla luce delle regole dettate dal previgente Dpr 318/1999, lo hanno regolarmente fatto: per questi casi la risoluzione del 22 marzo 2004 del Garante prevede che *essi dovranno riferire già a partire dalla relazione sul bilancio di esercizio per il 2003, con riferimento al DPSS già eventualmente aggiornato per il 2004, oppure menzionando l'adozione o aggiornamento avvenuto nel 2003 e indicando sinteticamente che si aggiornerà il DPSS entro il 30 giugno 2004*(oggi prorogato al 31 dicembre).
La presa di posizione del Garante spiazza i soggetti che, applicando il buon senso, hanno ritenuto di non aggiornare il DPSS negli ultimi mesi del 2003, per procedere alla sua redazione, alla luce delle nuove regole, nei primi mesi del 2004: applicando la logica, ed andando quindi oltre le carte e cartacce, era infatti palese l'inutilità di aggiornare nel novembre - dicembre 2003 un documento, che era destinato ad essere più o meno profondamente rinnovato nei primi mesi dell'anno successivo. Il Garante per la protezione dei dati personali, notoriamente affezionato a carte e cartacce, non ha

neppure preso in considerazione questa possibilità, nella sua risoluzione del 22 marzo 2004. Di conseguenza, i soggetti che hanno agito in questo modo sono di fatto tenuti a ***redigere il nuovo DPSS prima di formalizzare la relazione accompagnatoria del bilancio di esercizio***, per potere dichiarare in tale relazione di avere aggiornato il DPSS per il 2004. In caso contrario sarebbero in difetto, poiché non potrebbero menzionare di avere aggiornato il DPSS nel corso del 2003.

Il ***CASO 4****,* definibile con il termine *mosca nera,* è costituito dai soggetti che, pur essendo tenuti alla redazione ed aggiornamento del DPSS anche alla luce del Dpr 318/199, non hanno osservato tale obbligo. In questi casi si rende necessario ***redigere entro brevissimo termine*** **il DPSS per il 2004, alla luce delle regole previste dal nuovo codice, potendo così attestare nella relazione di prossima ufficializzazione di avere provveduto in tale senso**. In caso contrario i soggetti in esame sarebbero in difetto, poiché non potrebbero evidentemente menzionare, nella relazione accompagnatoria del bilancio di esercizio, di avere redatto o aggiornato il DPSS nel corso del 2003.

Il documento deve essere **redatto dal titolare del trattamento**, anche *attraverso il responsabile per la sicurezza*, se designato: ci si chiede se, in questa seconda ipotesi, nella quale il responsabile può essere anche un soggetto esterno all'organizzazione, il titolare possa evitare di firmare, o di approvare ufficialmente, in caso di presenza di un organo collegiale, il documento. La risposta è negativa, perché il titolare è sempre e comunque tenuto *in prima persona* ad assumersi le responsabilità inerenti la sicurezza privacy, ivi incluse quelle legate alla redazione del documento sulla sicurezza, ed alla corretta realizzazione e gestione delle misure in esso descritte.
Nel caso in cui la redazione avvenga *attraverso il responsabile*, l'onere di firmare il documento, assumendo le relative responsabilità, sarà a carico *anche di quest'ultimo*: nell'ipotesi in cui la redazione sia affidata ad un soggetto esterno, nominato responsabile per la sicurezza, troveranno inoltre applicazione le previsioni del punto 25. del disciplinare tecnico, per cui il soggetto esterno dovrà *attestare la conformità* del documento redatto, alle disposizioni del disciplinare tecnico stesso (si veda il paragrafo 6.7 del sesto capitolo).

Un particolare aspetto concerne l'opportunità di **attribuire al DPSS data certa**: tale adempimento non viene imposto né dalla legge, né dal provvedimento del 22 marzo 2004 del Garante (a differenza di quanto avviene, ad esempio, per il documento con il quale si attesta di disporre di strumenti elettronici tecnicamente inadeguati).
Se si ragiona su un piano logico, l'attribuzione della data certa al documento appare effettivamente inutile: ad esempio, se nel corso di un'ispezione il DPSS venisse prontamente esibito dal titolare, non si vedono le ragioni per le quali l'Autorità inquirente dovrebbe sindacare che la data apposta sullo stesso (es. 26 marzo) potrebbe essere fittizia.

D'altra parte, è notorio che, nel Paese dei *cavilli*, le Autorità sono bravissime nel *trovare simili ragioni*, anche dove non se ne vedrebbe la necessità, per cui è di fatto suggeribile attribuire al documento in esame data certa.
Tale requisito viene attribuito, in modo *automatico*, nei casi in cui si verbalizzi, anche nei libri sociali, l'approvazione del documento, allegando lo stesso al verbale.
Al di fuori di questi casi, si rende opportuno ricorrere ad uno dei metodi che il Garante ha suggerito, per ottenere l'attribuzione della data certa:

- ricorso alla cosiddetta ***autoprestazione, presso gli uffici postali***, con apposizione del timbro direttamente sul documento, anziché sull'involucro che lo contiene
- adozione, per le amministrazioni pubbliche, di una ***delibera*** di cui sia certa la data, in base alla concreta disciplina della formazione, numerazione e pubblicazione dell'atto
- apposizione della cosiddetta ***marca temporale*** sui documenti informatici
- apposizione di autentica, deposito del documento o vidimazione di un verbale ***presso un notaio***
- registrazione o produzione del documento presso un ***ufficio pubblico***.

Un ultimo aspetto riguarda il fatto che il DPSS ***non deve essere inviato al Garante***, ma deve essere tenuto negli uffici del titolare, per esibirlo in caso di eventuali richieste da parte delle Autorità.

<table>
<tr><th colspan="2">CODICE PRIVACY</th></tr>
<tr><td colspan="2">34[1] Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
g) tenuta di un aggiornato documento programmatico sulla sicurezza;</td></tr>
<tr><th>DISCIPLINARE TECNICO</th><th>DPR 318/1999</th></tr>
<tr><td>19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:</td><td>6[1] Nel caso di trattamento dei dati sensibili e giudiziari effettuato mediante elaboratori elettronici accessibili in rete pubblica, deve essere predisposto e aggiornato, con cadenza annuale, un documento programmatico sulla sicurezza dei dati per definire, sulla base:</td></tr>
<tr><td>19.1. l'elenco dei trattamenti di dati personali;
19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
19.3. l'analisi dei rischi che incombono sui dati;</td><td>-della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati
- dell'analisi dei rischi,</td></tr>
<tr><td>19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;</td><td>a) i criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi;
b) i criteri e le procedure per</td></tr>
</table>

	assicurare l'integrità dei dati;
	c) i criteri e le procedure per la sicurezza delle trasmissioni dei dati, ivi compresi quelli per le restrizioni di accesso per via telematica;
19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;	
19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;	d) l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire danni.
19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;	
19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.	
	6[2] L'efficacia delle misure di sicurezza adottate ai sensi del comma 1 deve essere oggetto di controlli periodici, da eseguirsi con cadenza almeno annuale.
26. Il titolare riferisce, nella relazione accompagnatoria del bilancio	

d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.	

15.1 La duplice natura del documento programmatico

Il documento in esame ha innanzitutto una importante *funzione interna*, di guida alla adozione ed al miglioramento delle misure di sicurezza: è quindi opportuno concepirlo come un vero e proprio **piano per la sicurezza**, estendendo il suo contenuto a ***tutti gli aspetti legati a tale problematica***, che vadano anche oltre gli elementi obbligatori prescritti dal punto 19. del disciplinare tecnico.
D'altra parte, si deve però considerare che la redazione del documento è imposta da una norma di legge: esso è quindi, in un certo senso, un documento *pubblico*, del quale potrebbe prima o poi essere richiesta l'esibizione, dal Garante per la protezione dei dati personali innanzitutto. Questa *seconda natura* configge profondamente con la prima, di essere un *documento – guida*, poiché il documento potrebbe in taluni casi divenire una *confessione,* di non avere attuato, in tutto o in parte, le misure minime di sicurezza imposte dalla legge. In relazione a tale fatto, è opportuno agire come segue:

- premurarsi innanzitutto di adottare le prescritte *misure minime*, entro la prossima scadenza, prevista per la redazione del documento programmatico sulla sicurezza
- in secondo luogo, se dovessero esservi ancora delle misure minime che non sono state adottate, è opportuno che si utilizzi molta *diplomazia,* in sede di redazione del documento, evitando di rimarcare tale circostanza.

15.2 L'approvazione del documento

Si presenta una bozza di delibera, per i casi in cui il documento debba essere approvato da un organo collegiale (es. consiglio di amministrazione).
In data XX XX 200X si riunisce il consiglio di amministrazione delle Società Sigma Spa per approvare il documento programmatico sulla sicurezza, per il trattamento dei dati personali, ai sensi dell'articolo 34, comma 1 lettera g) del codice in materia di protezione dei dati personali, approvato con il Dlgs 196/2003, e del punto 19. del relativo disciplinare tecnico in materia di misure minime di sicurezza.
…….
Si osserva che (*scegliere l'opzione*):

1. *tale documento viene redatto per la prima volta*, *in quanto la società non era in precedenza tenuta a tale adempimento*
2. *si tratta del periodico aggiornamento, essendo tale documento già stato redatto in passato (la precedente versione è stata approvata il……..)*

La redazione è stata curata dal responsabile per la sicurezza, che ha provveduto a firmare in originale il documento (*chiarire se si tratta di un responsabile interno, o di un soggetto esterno all'organizzazione*).

…….

Dopo esaurienti discussioni, il consiglio delibera di approvare il documento programmatico sulla sicurezza, che viene allegato sub B), *della cui redazione / del cui aggiornamento* si riferisce nella relazione sulla gestione, che accompagna il bilancio di esercizio.

15.3 Documento programmatico sulla sicurezza

ALLEGATO B
Documento programmatico sulla sicurezza nel trattamento dei dati personali

Scopo di questo documento è di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, da adottare per il trattamento dei dati personali effettuato dalla società Sigma Spa.

Il presente documento, redatto da…….in qualità di responsabile per la sicurezza, che provvede a firmarlo in calce, si articola nei seguenti punti:

1. elenco dei trattamenti di dati personali, posti in essere da Sigma Spa
2. caratteristiche delle aree e dei locali, nonché degli strumenti con cui si effettuano i trattamenti
3. analisi dei rischi che incombono sui dati
4. misure da adottare per garantire l'integrità e la disponibilità dei dati
5. criteri e modalità di ripristino dei dati, in seguito a distruzione o danneggiamento
6. analisi del mansionario privacy e degli interventi formativi degli incaricati
7. descrizione dei criteri da adottare, per garantire l'adozione delle misure minime di sicurezza, in caso di trattamenti di dati personali affidati all'esterno
8. controllo generale periodico sullo stato della sicurezza.

15.3.1 Elenco dei trattamenti di dati personali

(punto 19.1 del disciplinare tecnico)

Elaborare la matrice presentata nel terzo capitolo del manuale – paragrafo 3.3

BANCHE DI DATI

	A	B	C	D	E	F
Banca di dati 1						
Banca di dati 2						
Banca di dati 3						
Banca di dati 4						
Banca di dati 5						
Banca di dati 6						
Banca di dati 7						

STRUMENTI UTILIZZATI PER IL TRATTAMENTO

*Descrivere brevemente le caratteristiche delle **banche di dati trattati**, evidenziando in particolare le specificità di quelli sensibili / giudiziari.*

*Commentare gli aspetti salienti dell'impostazione adottata, in termini di **quali dati vengono trattati con quali strumenti**.*

15.3.2 Caratteristiche delle aree, dei locali, degli strumenti con cui si effettuano i trattamenti

*Descrivere, **con particolare riferimento alla sicurezza garantita**, le principali caratteristiche tecniche degli edifici e dei locali in cui sono situati gli strumenti elettronici e, più in generale, si effettua il trattamento.*

Descrivere gli strumenti elettronici con cui si effettuano i trattamenti, avendo un particolare riguardo alla distinzione tra:

- elaboratori non in rete, né dotati di accesso ad Internet
- strumenti collegati tra loro tramite rete non disponibile al pubblico
- elaboratori non in rete con altri, ma dotati di accesso ad Internet
- strumenti collegati tra loro tramite rete disponibile, anche in parte, al pubblico

Per la distinzione tra le diverse categorie, si veda il paragrafo 3.2.1 del manuale.

15.3.3 Analisi dei rischi che incombono sui dati

(punto 19.3 del disciplinare tecnico)

Fare riferimento al quarto capitolo del manuale – paragrafo 4.1. Non è invece necessario effettuare l'analisi presentata nei successivi paragrafi 4.2 e 4.3, nell'ambito della redazione del documento programmatico sulla sicurezza.

Dare un giudizio sul grado di rischio (basso, medio, alto, elevatissimo), legato alla gestione delle singole banche dati (es:banca contenente solo dati pubblici, reperiti da Internet: scarso; banca contenente dati di natura genetica: elevatissimo). Motivare brevemente le ragioni, che inducono ad attribuire il giudizio.

BANCA DI DATI	*GIUDIZIO SUL GRADO DI RISCHIO DEI DATI*
Banca di dati 1	*basso / medio / alto / elevatissimo*
Banca di dati 2	*basso / medio / alto / elevatissimo*
Banca di dati 3	*basso / medio / alto / elevatissimo*
Banca di dati 4	*basso / medio / alto / elevatissimo*
Banca di dati 5	*basso / medio / alto / elevatissimo*
Banca di dati 6	*basso / medio / alto / elevatissimo*
Banca di dati 7	*basso / medio / alto / elevatissimo*

Dare un giudizio sul grado di rischio (N nessun rischio, B basso, M medio, A alto), legato agli strumenti di utilizzati per il trattamento:

- *analizzando le principali categorie di rischi cui ciascuno di essi è esposto*
- *dando un giudizio conclusivo sul grado di rischio.*

Rischi di natura fisica						
Rischio di area	n/b/m/a	n/b/m/a	n/b/m/a	n/b/m/a	n/b/m/a	n/b/m/a
Rischio dei locali	n/b/m/a	n/b/m/a	n/b/m/a	n/b/m/a	n/b/m/a	n/b/m/a
Rischi di natura logica						
Malfunzionamento	n/b/m/a	n/b/m/a	n/b/m/a	n/b/m/a	n/b/m/a	n/b/m/a
Accesso abusivo agli strumenti	n/b/m/a	n/b/m/a	n/b/m/a	n/b/m/a	n/b/m/a	n/b/m/a
Accesso abusivo ai dati	n/b/m/a	n/b/m/a	n/b/m/a	n/b/m/a	n/b/m/a	n/b/m/a
Perdita dei dati per virus e attacchi	n/b/m/a	n/b/m/a	n/b/m/a	n/b/m/a	n/b/m/a	n/b/m/a
Intercettazione dei dati	n/b/m/a	n/b/m/a	n/b/m/a	n/b/m/a	n/b/m/a	n/b/m/a
Giudizio conclusivo	**n / b / m / a**	**n / b / m / a**	**n / b / m / a**	**n / b / m / a**	**n / b / m / a**	**n / b / m / a**
	A	**B**	**C**	**D**	**E**	**F**

STRUMENTI UTILIZZATI PER IL TRATTAMENTO

Presentare il quadro di sintesi del grado di rischio, che grava sui singoli trattamenti, incrociando quello che si riferisce alla natura dei dati ed il giudizio conclusivo, sul rischio cui sono sottoposti gli strumenti.

RISCHIO - DATI

Banca di dati 1	***b / m / a / e***						
Banca di dati 2	***b / m / a / e*** *o*						
Banca di dati 3	***b / m / a / e***						
Banca di dati 4	***b / m / a / e***						
Banca di dati 5	***b / m / a / e***						
Banca di dati 6	***b / m / a / e***						
Banca di dati 7	***b / m / a / e***						
		n / b / m / a	**n / b / m / a**	**n / b / m / a**	**n / b / m / a**	**n / b / m / a**	**n / b / m / a**
		A	**B**	**C**	**D**	**E**	**F**

RISCHIO - STRUMENTI

15.3.4 Misure da adottare per garantire l'integrità e la disponibilità dei dati

(punto 19.4 del disciplinare tecnico)

Si devono descrivere:

- *sia le misure che risultano già adottate dalla società, nel momento in cui viene redatto il documento*
- *che quelle ulteriori, finalizzate ad incrementare la sicurezza, la cui adozione è prevista entro un periodo di tempo ragionevole (indicativamente: un anno). Per quanto non sia obbligatorio, è opportuno che si accenni ai preventivi di spesa.*

Distinguere le misure atte a garantire:

- *la protezione delle aree e dei locali*
- *la corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali*
- *la sicurezza logica, nell'ambito dell'utilizzo degli strumenti elettronici*

La protezione delle aree e dei locali

Riferimento: Paragrafo 6.5.1 del manuale

- ***vigilanza della sede***
- ***ingresso controllato nei locali ove ha luogo il trattamento***
- ***sistemi di allarme e/o di sorveglianza antintrusione***
- ***registrazione degli accessi***
- ***autenticazione degli accessi***
- ***dispositivi antincendio***
- ***continuità dell'alimentazione elettrica***

L'archiviazione e custodia di atti, documenti e supporti

Riferimento: quinto capitolo del manuale

- ***custodia in classificatori o armadi non accessibili***
- ***custodia in armadi blindati e/o ignifughi o deposito in cassaforte***
- ***custodia dei supporti in contenitori sigillati***
- ***predisposizione dell'archivio ad accesso controllato, per i dati sensibili e giudiziari***

Le misure logiche di sicurezza

Riferimento: sesto capitolo del manuale

Alcune delle possibili misure sono:

- ***autenticazione dell'incaricato (paragrafo 6.1)***
- ***adozione di un sistema di autorizzazione (paragrafo 6.2)***
- ***controllo degli accessi (paragrafo 6.3.1)***
- ***registrazione degli accessi***
- ***controlli aggiornati antivirus (paragrafo 6.3.1)***
- ***sottoscrizione elettronica***
- ***cifratura dei dati memorizzati (paragrafo 6.6)***
- ***cifratura dei dati trasmessi (paragrafo 6.5.3)***
- ***annotazione della fonte dei dati***
- ***annotazione del responsabile dell'operazione***
- ***rilevazione di intercettazioni***

- ***monitoraggio continuo delle sessioni di lavoro***
- ***sospensione automatica delle sessioni di lavoro***
- ***verifiche periodiche su dati o trattamenti non consentiti o non corretti***
- ***verifiche automatizzate dei requisiti dei dati***
- ***controllo sull'operato degli addetti alla manutenzione***
- ***controllo dei supporti consegnati in manutenzione***
- ***controllo sull'operato degli addetti alla manutenzione***
- ***verifica della leggibilità dei supporti.***

15.3.5 Criteri e modalità di ripristino dei dati, in seguito a distruzione o danneggiamento

(punto 19.5 del disciplinare tecnico)

Riferimento: paragrafo 6.3.2 del manuale
- *salvataggio regolare dei dati*
- *procedure di Back – up*
- *piano di continuità operativa*
- *piano di disaster recovery.*

15.3.6 Analisi del mansionario privacy e degli interventi formativi degli incaricati

(punti 19.2 e 19.6 del disciplinare tecnico)

- *riportare gli elementi salienti del mansionario privacy*
- *descrivere le misure di sicurezza di carattere organizzativo*
- *descrivere i piani di formazione del personale*

Il mansionario privacy
Riferimento: secondo capitolo del manuale
Descrivere:
- *l'articolazione dei responsabili (paragrafo 2.2), con i loro compiti essenziali*
- *specificare se esiste un responsabile per la sicurezza (paragrafo 2.2.2) e chi riveste la qualifica di amministratore del sistema informativo (paragrafo 2.2.3)*
- *indicare quali siano le unità, per le quali sia stato individuato per iscritto l'ambito di trattamento, precisando quale esso sia (paragrafo 2.3)*

Le misure di sicurezza di carattere organizzativo
Riferimento: Secondo capitolo del manuale e Paragrafo 3.1.1
- *descrivere le modalità di incarico del personale (paragrafo 2.3)*
- *confermare di avere impartito le prescrizioni in termini di sicurezza (paragrafo 2.3.2)*
- *confermare di avere adottato le procedure per la classificazione dei dati (paragrafo 3.1.1)*
- *prescrizione di linee – guida di sicurezza e altre istruzioni interne*

I piani di formazione del personale
Riferimento: Paragrafo 6.5.2 del manuale

15.3.7 L'affidamento di dati personali all'esterno

(punto 19.7 del disciplinare tecnico)

Riferimento: Settimo capitolo del manuale

Per i casi in cui il trattamento di dati sensibili e/o giudiziari venga affidato a soggetti esterni, si provvede alla nomina degli stessi come responsabili del trattamento di dati personali.
Nelle ipotesi in cui tali soggetti utilizzino strumenti elettronici per il trattamento, per avere la garanzia che essi adottino le misure minime di sicurezza, previste dalla normativa:

- *si esige da loro una dichiarazione di avere redatto il documento programmatico sulla sicurezza, nel quale abbiano attestato di avere adottato le misure minime previste dal disciplinare tecnico*
- *si esige da loro una copia del documento programmatico di sicurezza da essi redatto / del certificato di conformità rilasciato da chi ha curato la progettazione e l'attuazione delle misure minime di sicurezza*
- *si convengono con essi clausole contrattuali, che disciplinano gli aspetti legati alla gestione dei dati personali. Se i soggetti sono residenti in Paesi extra-Ue, che non sono considerati sicuri per il trattamento di dati personali, tali clausole sono conformi a quanto previsto dalla Decisione della Commissione CE 2002/16/CE del 27 dicembre 2002.*

15.3.8 Controllo generale periodico sullo stato della sicurezza

Riferimento: Paragrafo 6.3.2.1 del manuale

Descrivere:

- *le procedure per il monitoraggio dello stato della sicurezza*
- *le caratteristiche degli eventuali interventi di audit della sicurezza programmati.*

16 La mappa delle misure minime di sicurezza

Nel presente capitolo si *tirano le somme*, avendo riguardo a due aspetti:

- l'evoluzione della mappa delle misure minime di sicurezza: l'analisi di *cosa cambia*, in ogni caso opportuna, si rende necessaria per comprendere se l'organizzazione è già in grado di adottare le nuove misure, sulla base degli strumenti elettronici posseduti al 31 dicembre 2003, ovvero se esistono obiettive ragioni di carattere tecnico che impediscono l'immediata adozione di tali misure. In questo secondo caso, è possibile redigere un documento avente data certa, al fine di differire il termine ultimo, entro cui adottare le nuove misure, a marzo 2005, invece della generale scadenza del 31 dicembre 2004
- il rapporto tra le diverse *classi di misure di sicurezza* richieste, con il fine di organizzare le modalità di trattamento dei dati personali in modo tale, da minimizzare gli adempimenti imposti per la sicurezza.

16.1 L'evoluzione della mappa delle misure minime di sicurezza

Nella seguente tabella si riassume la mappa delle misure minime di sicurezza, confrontando le nuove misure, previste dal codice privacy e dal relativo disciplinare tecnico, con quanto prevedeva il precedente Dpr 318/1999.

Nell'**intestazione delle colonne**, viene mantenuta innanzitutto la distinzione, commentata nei paragrafi 3.2 e 3.2.1 del terzo capitolo, tra trattamenti effettuati con:

- strumenti diversi da quelli elettronici (**MAN**)
- strumenti elettronici che non sono in rete, né dispongono di accesso ad Internet (**ALONE**)
- strumenti elettronici che sono in rete privata (**PRIV**)
- strumenti elettronici che sono in rete pubblica e/o dispongono di accesso ad Internet (**PUBB**).

In ognuna di tali circostanze, si distingue il caso di trattamento di dati di natura comune (**C**), da quello di trattamento di dati sensibili o giudiziari (**P**).

Sulle righe si riporta la descrizione delle misure di sicurezza che devono essere adottate, aggiungendo il codice che identifica il paragrafo del manuale, nel quale è trattato l'argomento. Si noti che:

- la "scrittura in carattere normale" indica che la riga si riferisce alle nuove regole, introdotte dal codice privacy
- la "*scrittura in carattere corsivo*" indica che la riga si riferisce alle vecchie regole, previste dall'abrogando Dpr 318/1999.

Nelle **caselle di intersezione** si indica se, per il trattamento preso in esame nella colonne, si devono adottare le misure minime di sicurezza indicate nella riga, come segue:

- indicando la lettera N se vi è l'obbligo di adottare la misura, ai sensi del nuovo codice
- indicando le lettera *v* se l'obbligo di adottare la misura è previsto dal Dpr 318/1999.

	MAN		ALONE		PRIV		PUBB		
	C	P	C	P	C	P	C	P	NOTE
Adempimenti nella attribuzione di ruoli e compiti									
Usare la forma scritta e fornire istruzioni dettagliate (2.3)	N	N	N	N	N	N	N	N	
Usare la forma scritta e fornire istruzioni dettagliate	*v*	*v*	*v*	*v*	*v*	*v*	*v*	*v*	
Predisporre ed aggiornare il mansionario privacy (2.4)	N	N	N	N	N	N	N	N	1
Predisporre ed aggiornare il mansionario privacy									
Prevedere procedure per la classificazione dei dati trattati (3.1.1)	N	N	N	N	N	N	N	N	
Prevedere procedure per la classificazione dei dati trattati	*v*	*v*	*v*	*v*	*v*	*v*	*v*	*v*	

	MAN		ALONE		PRIV		PUBB		
	C	P	C	P	C	P	C	P	NOTE
Creazione e gestione di archivi fisici									
Controllo e custodia di atti, documenti e supporti (5.1)	N	N	N	N	N	N	N	N	2
Controllo e custodia di atti, documenti e supporti	*v*	*v*	*v*	*v*	*v*	*v*	*v*	*v*	
Archivio ad accesso selezionato – per i dati comuni (5.2)									
Archivio ad accesso selezionato – per i dati comuni	*v*		*v*		*v*		*v*		
Archivio ad accesso controllato – per i dati particolari (5.2)		N		N		N		N	
Archivio ad accesso controllato – per i dati particolari		*v*		*v*		*v*		*v*	

	MAN		ALONE		PRIV		PUBB		
	C	P	C	P	C	P	C	P	NOTE
Autenticazione per accedere agli strumenti elettronici									3, 4
Adozione di un sistema di autenticazione informatica (6.1)			N	N	N	N	N	N	

Adozione di un sistema di autenticazione informatica					*v*	*v*	*v*	*v*	
Semplice attribuzione di parole chiave			*v*	*v*					
Misure logiche di autorizzazione per accedere ai dati									5, 6, 7
Adozione di un sistema di autorizzazione (6.2)			N	N	N	N	N	N	
Autorizzazione all'accesso di dati particolari						*v*		*v*	
Adozione di misure di protezione e ripristino dei dati									
Software antivirus ed analoghi (6.3.1)			N	N	N	N	N	N	
Software antivirus ed analoghi					*v*	*v*	*v*	*v*	
Strumenti anti – intrusione (6.3.1)						N		N	
Strumenti anti – intrusione									
Programmi finalizzati alla manutenzione logica degli strumenti (6.3.1)			N	N	N	N	N	N	
Programmi finalizzati alla manutenzione logica degli strumenti									
Salvataggio almeno settimanale dei dati (6.3.2)			N	N	N	N	N	N	
Salvataggio almeno settimanale dei dati									
Procedure per il ripristino dei dati entro sette giorni (6.3.2)				N		N		N	
Procedure per il ripristino dei dati entro sette giorni									
Procedure di controllo dei supporti di memorizzazione (6.4)				N		N		N	
Procedure di controllo dei supporti di memorizzazione						*v*		*v*	
	MAN		**ALONE**		**PRIV**		**PUBB**		
	C	**P**	**C**	**P**	**C**	**P**	**C**	**P**	**NOTE**
Documento programmatico sulla sicurezza									
Redazione e revisione del Documento programmatico sulla sicurezza (6.5)				N		N		N	
Redazione e revisione del Documento programmatico sulla sicurezza								*v*	
Ulteriori adempimenti, per chi redige il documento programmatico									
Analisi dei rischi (capitolo 4)				N		N		N	
Analisi dei rischi								*v*	
Protezione di aree e locali interessati dalle misure di sicurezza (6.5.1)				N		N		N	
Protezione di aree e locali interessati dalle misure di sicurezza								*v*	
Autorizzazione all'accesso delle persone ai locali e controllo									8

Autorizzazione all'accesso delle persone ai locali e controllo								*v*
Assicurare la sicurezza nella trasmissione dei dati (6.5.3)						N		N
Assicurare la sicurezza nella trasmissione dei dati								*v*
Piano di formazione degli incaricati del trattamento (6.5.2)				N		N		N
Piano di formazione degli incaricati del trattamento								*v*
Controllo generale periodico sullo stato della sicurezza (6.3.1.2)				N		N		N
Controllo generale periodico sullo stato della sicurezza								*v*

9

NOTE

1) Anche in vigenza del Dpr 318/1999, si rendeva opportuna la redazione del mansionario. La novità consiste nel fatto che, con il nuovo codice, l'aggiornamento periodico dell'individuazione dell'ambito di trattamento consentito agli incaricati diviene esplicitamente una misura minima di sicurezza.

2) Nel caso in cui atti, documenti o supporti contengano dati sensibili o giudiziari, la custodia deve avvenire mediante cassetti chiudibili a chiave, o strumenti equivalenti.

3) Procedura non richiesta nei casi in cui vengano trattati esclusivamente dati personali di cui è consentita la diffusione

4) Si osserva che, anche agli elaboratori che non sono in rete, vengono estese le più severe procedure, che in vigenza del Dpr 318/1999 dovevano essere seguito solo per gli elaboratori in rete.

5) Procedura non richiesta nei casi in cui vengano trattati esclusivamente dati personali di cui è consentita la diffusione.

6) In casi limitati, il nuovo codice consente di prescindere dalla adozione di un sistema di autorizzazione.

7) Per il trattamento di dati relativi all'identità genetica, da parte degli organismi sanitari e degli esercenti le professioni sanitarie, è inoltre prescritto che si debbano adottare sistemi tali, da permettere "il trattamento disgiunto dei dati relativi all'identità genetica dagli altri dati personali che permettono di identificare direttamente gli interessati" (*paragrafo 6.6 del manuale*).

8) Per il trattamento di dati relativi all'identità genetica, da parte degli organismi sanitari e degli esercenti le professioni sanitarie, è prescritto che essi "sono trattati esclusivamente all'interno di locali protetti, accessibili ai soli incaricati dei trattamenti ed ai soggetti specificamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali, riservati al loro trattamento, deve avvenire in contenitori muniti di serratura o dispositivi equipollenti" (*paragrafo 6.6 del manuale*).

9) Per il trattamento di dati relativi all'identità genetica, da parte degli organismi sanitari e degli esercenti le professioni sanitarie, è prescritto che "il trasferimento dei file in formato elettronico è cifrato" (*paragrafo 6.6 del manuale*).

Si osserva che, con il nuovo codice, viene in generale prevista l'adozione di misure minime di sicurezza più impegnative, per i casi in cui si utilizzino

strumenti elettronici per il trattamento: a tale riguardo, perde sostanzialmente rilievo la circostanza che tali strumenti siano o meno in rete, con la conseguenza di doversi adeguare alle procedure che, in vigenza del Dpr 318/1999, erano imposte per i soli elaboratori in rete.

In particolare, si rende necessario:

- adottare un sistema di autenticazione informatica, non essendo più sufficiente ricorrere alla semplice attribuzione delle parole chiave, neppure nei casi in cui l'elaboratore non sia in rete
- adottare un sistema di autorizzazione, che permetta l'accesso alle banche dati, di qualsiasi natura essi siano, anche nei casi in cui il trattamento avviene con elaboratori non in rete
- dotare anche gli elaboratori non in rete di software antivirus
- dotare tutti gli strumenti elettronici di programmi finalizzati al controllo del loro corretto funzionamento
- procedere in tutti casi ai salvataggi, con frequenza almeno settimanale.

Nei casi in cui si trattino con strumenti elettronici *dati sensibili o giudiziari*, si ha una vera e propria rivoluzione: in questa ipotesi viene infatti generalizzato l'obbligo di redigere, ed aggiornare con cadenza annuale, il documento programmatico sulla sicurezza, che in vigenza del Dpr 318/1999 era limitato ai casi di trattamento con strumenti elettronici in rete pubblica.
E' previsto inoltre l'obbligo, in caso di trattamento con strumenti in rete, di dotarsi di dispositivi anti – intrusione.

16.2 Il rapporto tra le diverse *classi di sicurezza*

Il quadro delle misure di sicurezza, come è stato presentato nei precedenti capitoli, prescinde dal fatto che nella medesima organizzazione vengono generalmente posti in essere trattamenti che richiedono l'adozione di misure di sicurezza differenti, in relazione alle diverse tipologie di dati trattati ed ai diversi strumenti utilizzati.

Sotto il primo profilo, si osserva che praticamente tutte le organizzazioni trattano dati comuni (si pensi ai semplici dati anagrafici di clienti e fornitori), mentre in molti casi il trattamento di dati sensibili ha natura residuale, spesso limitandosi alla rilevazione dello stato di salute dei dipendenti.
Dal punto di vista degli strumenti utilizzati per il trattamento, in un'unica azienda frequentemente coesistono trattamenti effettuati senza l'ausilio di elaboratori e trattamenti effettuati con gli stessi.

E' quindi probabile che una organizzazione rientri in più di una delle ***classi di sicurezza***, presentate nella tabella del precedente paragrafo 9.1, e non è raro che possa rientrare in tutte le otto classi.
In tali casi è necessario, al fine di disegnare la mappa delle misure minime di sicurezza obbligatorie, comprendere quali relazioni esistano tra le diverse classi di sicurezza, e che riflessi abbia il fatto di appartenere ad una determinata classe, sulla organizzazione nel suo complesso.

Ad esempio, il fatto di ***trattare dati sensibili con l'utilizzo di strumenti elettronici***, lungi dal limitare i propri effetti alle modalità di accesso agli strumenti stessi ed ai dati sensibili in essi contenuti, implica per l'intera organizzazione l'obbligo di ottemperare agli adempimenti previsti dal Documento programmatico di sicurezza: tale fatto è stato ribadito dalla relazione di accompagnamento al Dpr 318/1999, laddove è scritto che "si noti che, nei casi in cui vengano trattati sia dati comuni che dati sensibili o giudiziari, sarà necessario osservare le misure di sicurezza previste per la categoria *più elevata*, a nulla rilevando che le diverse categorie di dati eventualmente si trovino all'interno di diversi archivi".

Analizzando la mappa elaborata nel paragrafo 9.1, si osserva innanzitutto che, per quanto riguarda la misura di sicurezza **Creazione e gestione di archivi fisici**, la differenza sostanziale consiste nel fatto che, per i documenti e gli atti contenenti dati sensibili o giudiziari, si deve predisporre un *archivio ad accesso controllato*, la cui organizzazione è più complessa ed impegnativa, rispetto alla normale diligenza richiesta per l'archiviazione di atti e documenti contenenti solo dati comuni.

Un'organizzazione, che dovesse trattare in modo limitato e residuale dati sensibili o giudiziari, con strumenti diversi dal quelli elettronici, potrebbe quindi trovare conveniente archiviare questi ultimi in luoghi diversi, dagli archivi dove tiene i dati comuni, per potere beneficiare di una maggiore flessibilità, nelle procedure di archiviazione dei dati comuni *di tutti i giorni*: a tale fine, potrebbe ad esempio decidere di tenere i dati sensibili, relativi al personale, nell'armadio-cassaforte situato nell'ufficio del Presidente, riservando i locali del vero e proprio archivio ai soli dati comuni. Poco saggio sarebbe invece archiviare insieme in quest'ultimo dati comuni e particolari, perché ai primi si estenderebbero automaticamente i più impegnativi accorgimenti, richiesti per i secondi, a tutela della sicurezza.

Proseguendo con l'analisi delle classi di sicurezza, si nota che vi è una differenza di fondo, nell'ipotesi in cui i dati **sensibili e/o giudiziari** vengano trattati esclusivamente con strumenti diversi da quelli elettronici, rispetto a quella in cui il trattamento avvenga anche mediante tali strumenti. In questa seconda ipotesi, ci si troverebbe nell'ipotesi più impegnativa, che coinvolge l'intera organizzazione, in relazione ai complessi adempimenti legati all'impianto, al rispetto ed all'aggiornamento delle misure previste nel Documento programmatico di sicurezza.

Sarebbe quindi illogico che la nota Brambilla Sas, che di mestiere produce articoli di alto artigianato, non fa la casa di cura, trattasse i dati sensibili o giudiziari relativi ai cinque dipendenti con strumenti elettronici, con ciò venendo a configurarsi come organizzazione che tratta i dati sensibili (malattie e, in generale, dati idonei a rivelare lo stato di salute dei dipendenti) con strumenti elettronici.

Il semplice accorgimento di togliere i dati sensibili, relativi ai dipendenti, da tali strumenti, per annotarli manualmente in un quaderno, permetterebbe alla Brambilla Sas di rientrare nelle seguenti classi:

- *trattamento di soli dati comuni con strumenti elettronici*, per cui non è necessario redigere ed aggiornare il documento programmatico sulla sicurezza
- *trattamento di dati sensibili con strumenti diversi da quelli elettronici*, per effettuare il quale tutto ciò che viene richiesto è di adottare alcuni accorgimenti, nella custodia ed archiviazione del quaderno contenente i dati sensibili.

17 Il periodo transitorio

Il nuovo codice privacy entra in vigore il 1° gennaio 2004.
In relazione al fatto che una scadenza così ravvicinata, entro cui adottare le ***nuove misure minime***, avrebbe potuto creare problemi di ordine tecnico ed organizzativo, il legislatore ha differito, con l'articolo 180, il termine ultimo entro il quale è possibile adeguarsi a quanto previsto dal disciplinare tecnico, nei seguenti termini:

- **in generale**, il comma 1 dell'articolo 180 stabilisce il termine ultimo del **30 giugno 2004**, per adottare le ***nuove*** misure minime
- nei particolari casi, in cui i soggetti che trattano i dati possiedano **strumenti elettronici tecnicamente inadeguati**, i commi 2 e 3 dell'articolo 180 differiscono ulteriormente al **1° gennaio 2005** il termine ultimo, entro cui si devono adottare le ***nuove*** misure minime.

17.1 Il differimento del termine generale

NUOVO CODICE PRIVACY
180[1] Le misure minime di sicurezza di cui agli articoli da 33 a 35 e all'allegato B) che non erano previste dal decreto del Presidente della Repubblica 28 luglio 1999, n. 318, sono adottate entro il 30 giugno 2004(oggi prorogato al 31 dicembre).

Alla generalità dei soggetti, che trattano dati personali, viene data la facoltà di adottare **entro marzo 2005**, invece che entro il 31 dicembre 2003, le ***nuove*** misure minime di sicurezza: con tale termine si intendono quelle, introdotte dagli articoli da 33 a 35 del nuovo codice, che non erano previste dall'abrogando Dpr 318/1999.
Si precisa che la norma non intendere concedere una proroga al 31 dicembre 2004, per l'adozione di ***tutte*** le misure minime di sicurezza, ma solo per l'adeguamento alle ***nuove***: sino a tale scadenza, rimane quindi fermo l'obbligo di essere adeguati, alle prescrizioni del *vecchio* Dpr 318/1999, senza alcuna eccezione.
Il termine ***nuove misure minime*** di sicurezza va inteso, per i fini in esame, nella duplice accezione di:

- **novità oggettiva**, conseguente cioè al fatto che il nuovo codice introduce una misura che non era prevista dal Dpr 318/1999: ad esempio, i più *severi* requisiti previsti per l'autenticazione informatica, descritti nel paragrafo 6.1 del sesto capitolo, rispetto a quelli sinora richiesti
- **novità soggettiva**, derivante cioè dal fatto che, alla luce delle nuove regole, possa aumentare la portata degli adempimenti cui è tenuto un determinato soggetto, rispetto a quanto avveniva alla luce della previgente normativa. Tipico esempio è quello di chi, trattando dati sensibili o giudiziari con l'uso di strumenti elettronici che non sono in rete pubblica, deve ora redigere il documento programmatico sulla sicurezza, adempimento al quale non era in precedenza tenuto.

17.2 Il particolare differimento a Marzo 2005

NUOVO CODICE PRIVACY
180[2] Il titolare che alla data di entrata in vigore del presente codice dispone di strumenti elettronici che, per obiettive ragioni tecniche, non consentono in tutto o in parte l'immediata applicazione delle misure minime di cui all'articolo 34 e delle corrispondenti modalità tecniche di cui all'allegato B), descrive le medesime ragioni in un documento a data certa da conservare presso la propria struttura. **180[3]** Nel caso di cui al comma 2, il titolare adotta ogni possibile misura di sicurezza in relazione agli strumenti elettronici detenuti in modo da evitare, anche sulla base di idonee misure organizzative, logistiche o procedurali, un incremento dei rischi di cui all'articolo 31, adeguando i medesimi strumenti al più tardi entro un anno dall'entrata in vigore del codice.

Il termine ultimo per adeguarsi alle nuove misure minime può essere **ulteriormente differito a marzo 2005**, solo nell'ipotesi in cui, alla data del 31 dicembre 2004, si fossero posseduti ***strumenti elettronici inadeguati***: con tale termine si intendono gli *strumenti elettronici che, per obiettive ragioni tecniche, non consentono in tutto o in parte l'immediata applicazione delle nuove misure minime di sicurezza*. Un esempio relativamente frequente potrebbe essere quello degli elaboratori che non consentono di adottare il più *sofisticato* sistema di autenticazione informatica, previsto dal nuovo codice (si veda il paragrafo 6.1 del sesto capitolo capitolo).
La circostanza di disporre di strumenti elettronici che, per obiettive ragioni tecniche, non consentono in tutto o in parte l'immediata applicazione delle nuove misure minime, deve essere verificata in data 31 dicembre 2004: chi si trovasse in questa situazione può quindi beneficiare del maggiore termine, anche nell'ipotesi in cui gli strumenti elettronici venissero modificati, o sostituiti con strumenti adeguati, prima del 30 giugno 2004(oggi prorogato al 31 dicembre).
Durante il processo di adeguamento, il titolare deve comunque adottare ogni possibile misura, in relazione agli strumenti elettronici detenuti, in modo da evitare un incremento dei rischi per la sicurezza.

17.2.1 Entro il 31 dicembre 2004: redazione del documento avente data certa

Per potersi avvalere del maggiore termine di marzo 2005, il titolare deve *descrivere le obiettive ragioni tecniche che non consentono in tutto o in parte l'immediata applicazione delle nuove misure minime in un documento:*

- *a data certa*
- *da conservare presso la propria struttura*.

Il contenuto del documento

Nel documento in esame si deve:

- *descrivere le obiettive ragioni tecniche che non consentono in tutto o in parte l'immediata applicazione delle nuove misure minime*: sul punto non ci si può limitare a fornire a generiche giustificazioni, ma si devono analizzare le caratteristiche tecniche degli strumenti elettronici, specificando per quale obiettiva ragione non sia possibile procedere al loro adeguamento entro il 31 dicembre 2004
- *esporre sinteticamente gli accorgimenti da adottare, o già adottati, per evitare un incremento dei rischi per la sicurezza, sino al 31 dicembre 2004*
- *esporre gli elementi che caratterizzano il piano di adeguamento, che deve concludersi entro il 31 dicembre 2004, nonché le singole fasi in cui esso è eventualmente ripartito*: a tale fine si potrà fare utile riferimento all'elencazione delle misure di sicurezza necessarie, caso per caso, illustrate nei capitoli precedenti. Per ciascuna misura si devono riportare le previsioni, sul momento in cui essa verrà compiutamente posta in essere, con un accenno al piano di spesa.

La data certa

Il documento deve essere redatto e sottoscritto dal titolare entro **il 31 dicembre 2004**, termine che deve essere attestato attribuendo al documento la ***data certa***.

Per ottenere il requisito della data certa, non è necessario recarsi da un notaio o all'Ufficio del registro, ma è ad esempio sufficiente inviare a sé stessi il documento, mediante piego raccomandato con ricevuta di ritorno, poiché la data apposta dall'Ufficio Postale attribuisce certezza. Al riguardo, la Cassazione (sentenze 8692/1990 e 186/1983) ha riconosciuto che il timbro postale, apposto sul foglio contenente le informazioni richieste, può comprovare in modo sicuro l'anteriorità della formazione del documento.

In occasione della redazione di un documento avente finalità analoghe, allorché entrò in vigore il Dpr 318/1999, il Garante per la protezione dei dati personali ha indicato ***alcuni strumenti idonei***, per conferire ad un documento la data certa:

- ricorso alla cosiddetta ***autoprestazione, presso gli uffici postali***, con apposizione del timbro direttamente sul documento, anziché sull'involucro che lo contiene
- adozione, per le amministrazioni pubbliche, di una ***delibera*** di cui sia certa la data, in base alla concreta disciplina della formazione, numerazione e pubblicazione dell'atto

- apposizione della cosiddetta ***marca temporale*** sui documenti informatici
- apposizione di autentica, deposito del documento o vidimazione di un verbale ***presso un notaio***
- registrazione o produzione del documento presso un ***ufficio pubblico***.

La tenuta del documento
Il documento, cui è stata attribuita data certa, deve essere ***custodito presso la struttura del titolare***, per esibirlo in sede di eventuali controlli: esso **non va quindi inviato al Garante**.

17.2.2 Il rapporto con il Documento programmatico sulla sicurezza

Con il provvedimento del 22 marzo 2004 il Garante ha chiarito che, nei casi in cui si è tenuti alla redazione o all'aggiornamento del Documento programmatico per la sicurezza, il termine ultimo per porre in essere tale adempimento è il 31 dicembre 2004, anche nell'ipotesi in cui il soggetto attestasse di possedere strumenti tecnicamente inadeguati, potendo di conseguenza differire a marzo 2005 l'adozione delle nuove misure minime di sicurezza.
In questi casi, potrebbe essere opportuno **accorpare in un unico documento** il DPSS, redatto per il 2004, ed il documento con il quale si attesta di possedere strumenti tecnicamente inadeguati, per cui si necessita del più lungo temine di marzo 2005 per adottare le nuove misure di sicurezza introdotte dal codice privacy.
Nella norma non vi è alcun ostacolo, per agire in tale senso: l'unico avvertimento da tenere presente è che, in questi casi, si rende obbligatorio attribuire data certa al *documento unitario* in esame.

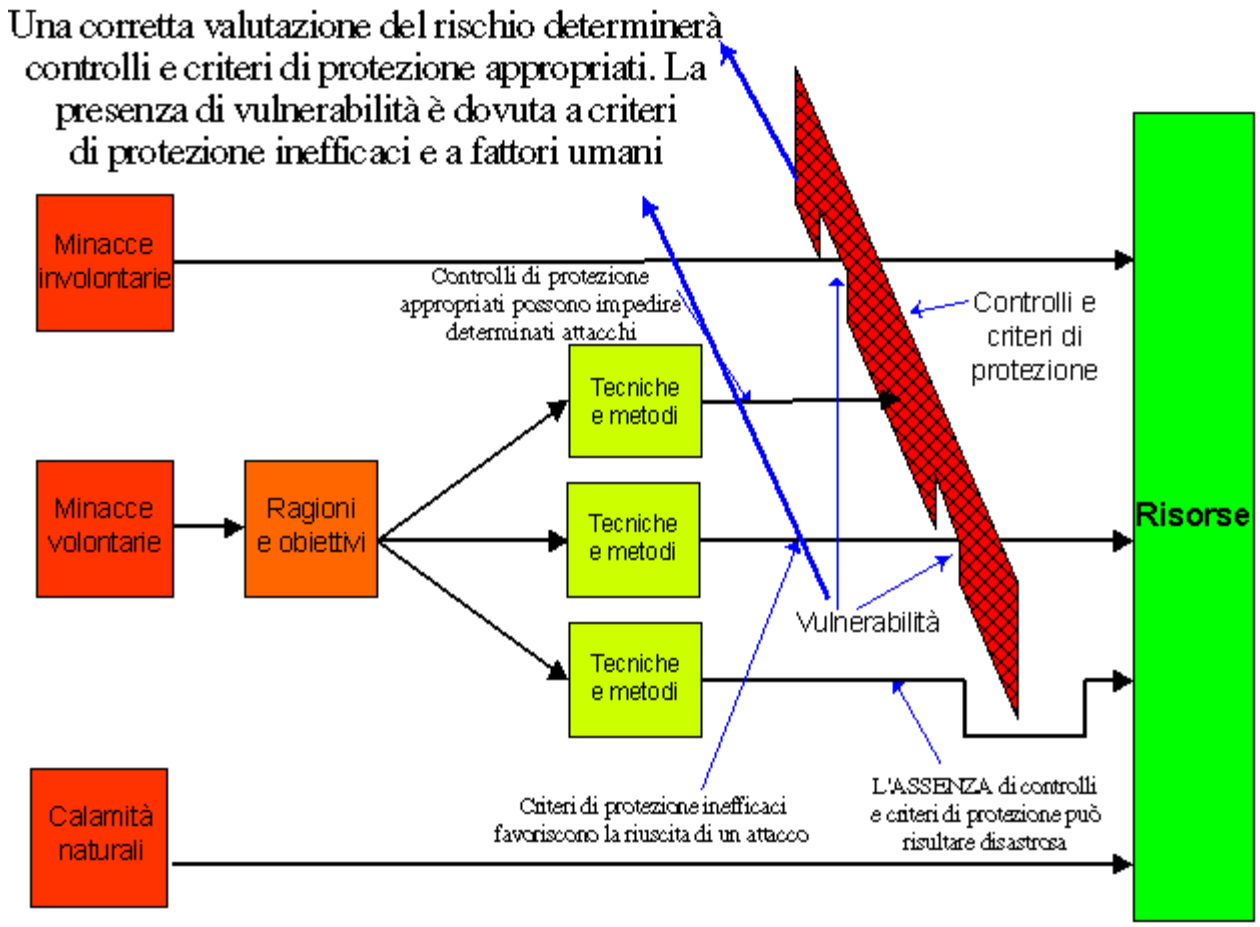
18 Pianificazione della sicurezza Proattiva

18.1 Introduzione

Dopo la valutazione del rischio, il passaggio successivo è la pianificazione proattiva. La pianificazione proattiva riguarda lo sviluppo di controlli e criteri di protezione e l'implementazione di strumenti e tecniche che contribuiscono alla protezione del sistema.
Così come per le strategie di protezione, è necessario predisporre un piano per la protezione proattiva e reattiva. Il piano proattivo viene sviluppato per proteggere le
risorse da attacchi ed errori dei dipendenti. Il piano reattivo è un piano di emergenza da implementare quando i piani proattivi falliscono.

18.2 Sviluppo di controlli e criteri di protezione

Il piano di protezione di una società è costituito da criteri di protezione. Essi forniscono istruzioni per specifiche aree di responsabilità e consistono di passaggi da seguire e regole cui attenersi.
I criteri devono stabilire le risorse da considerare importanti e specificare i passaggi da seguire per proteggerle. Possono essere redatti in molti modi. Un esempio è costituito da un criterio generale composto da poche pagine che prevede la maggior parte delle eventualità. Un altro esempio è rappresentato da criteri redatti per insiemi di risorse differenti, tra cui, ad esempio, la posta elettronica, le password, l'accesso a Internet e l'accesso remoto.



Due problemi comuni per i criteri dell'organizzazione sono:

1. Il criterio di protezione non è significativo, non specifica scelte e non fornisce indicazioni.
2. Il criterio di protezione non viene realmente usato dall'organizzazione. Si tratta invece di un pezzo di carta da mostrare ai revisori, agli avvocati, ad altri componenti dell'organizzazione o ai clienti, ma non influenza il funzionamento.

Una valutazione appropriata del rischio permette di determinare se sono stati implementati controlli e criteri di protezione efficaci. La presenza di vulnerabilità e debolezze può essere dovuta a criteri di protezione insufficienti e al fattore umano, come mostrato nel diagramma che segue. I criteri di protezione troppo rigorosi vengono spesso ignorati perché gli utenti si stancano di rispettarli (fattore umano).

Il sistema diventa quindi vulnerabile ad attacchi e violazioni di protezione.
Ad esempio, specificando un criterio di protezione restrittivo relativo al blocco degli account aumenta la possibilità di attacchi di negazione del servizio. Un altro esempio è rappresentato dall'implementazione di un tastierino di protezione sulla porta della stanza del server. Gli amministratori potrebbero stancarsi di immettere il PIN di protezione e impedire la chiusura della porta usando un libro o una scopa, evitando in tal modo il controllo di protezione. Anche specificando criteri restrittivi per le password potrebbe diminuire la protezione della rete.

Se si pretende che vengano utilizzate password più lunghe di sette caratteri, infatti, molti utenti avranno difficoltà a ricordarle. Potrebbero quindi scrivere le password e lasciarle dove un intruso può trovarle.
Il diagramma seguente mostra la relazione tra una valutazione del rischio appropriata e i controlli e i criteri di protezione.

Per essere efficace, il criterio richiede visibilità. La visibilità consente infatti l'implementazione del criterio in quanto ne assicura la diffusione all'interno di tutta l'organizzazione. Questa viene realizzata tramite il piano di ciascun criterio, costituito da un insieme di passaggi e regole scritte. Il piano definisce quando, come e da chi questi vengono implementati.
L'organizzazione di presentazioni, video, comitati di esperti, relatori esterni, forum di domande/risposte e notiziari contribuisce ad aumentare la visibilità. Se l'organizzazione aumenta la consapevolezza e la preparazione in tema di sicurezza del sistema, sarà possibile avvisare gli utenti di nuovi criteri e far conoscere ai nuovi dipendenti i criteri dell'organizzazione.

I criteri per la sicurezza dei computer devono essere introdotti in modo tale che risulti chiaro il sostegno incondizionato da parte della direzione dell'azienda, specialmente in ambienti in cui i dipendenti sono inondati di criteri, indicazioni, istruzioni e procedure. I criteri dell'organizzazione consentono di promuovere l'impegno della direzione nella sicurezza dei computer e nella definizione della condotta, degli obblighi e delle responsabilità dei dipendenti.

18.3 Tipi di criteri di protezione

Possono essere definiti criteri per qualsiasi area di protezione. Spetta al responsabile della sicurezza e al responsabile IT classificare i criteri da definire e decidere chi deve prepararli. I criteri possono riguardare l'intera società o solo alcune sezioni. I diversi tipi di criteri che possono essere inclusi sono:

- Criteri per le password
- Responsabilità amministrative
- Responsabilità degli utenti
- Criteri per la posta elettronica
- Criteri per Internet
- Criteri per il backup e il ripristino

18.4 Criteri per le password

La protezione fornita da un sistema di password dipende dalla capacità di mantenere riservate le password. Una password è vulnerabile ogni volta che viene usata, memorizzata o persino conosciuta. In un meccanismo di autenticazione basato su password implementato in un sistema, le password sono vulnerabili a causa di cinque aspetti peculiari:

- Una password deve essere assegnata inizialmente a un utente al momento della creazione.
- La password di un utente deve essere cambiata periodicamente.
- Il sistema deve gestire un "database di password".
- Gli utenti devono ricordare le password.
- Gli utenti devono immettere le password nel sistema al momento dell'autenticazione.
- I dipendenti non devono rivelare le password a nessuno. Nemmeno agli amministratori o ai responsabili IT.

È possibile configurare i criteri per le password in base alle esigenze dell'organizzazione. Ad esempio, è possibile specificare una lunghezza minima, non usare password vuote e assegnare alle password una validità minima e massima. È inoltre possibile impedirne la riutilizzazione e assicurarsi che gli utenti usino caratteri specifici per renderle più difficili da identificare. A tale scopo, è possibile usare i criteri di account di Windows 2000, illustrati più avanti in questo stesso white paper.

18.5 Responsabilità amministrative

Molti sistemi vengono forniti con alcuni accessi utente standard già predefiniti. Si consiglia di cambiare le password per tutti gli utenti standard configurati prima di consentire l'accesso al sistema da parte di tutti gli utenti. Ad esempio, cambiare la password dell'amministratore quando si installa il sistema.
L'amministratore è responsabile della generazione e dell'assegnazione della password iniziale per ciascun utente. È quindi necessario comunicare questa password all'utente. In alcuni casi può essere necessario impedire che l'amministratore possa visualizzare le password. In altri casi, l'utente può impedire facilmente questa visibilità. Per impedire la visibilità di una password, è possibile utilizzare un sistema di smart card in congiunzione al nome e alla password dell'utente.
Anche se l'amministratore conosce la password, non potrà usarla senza smart card. Quando la password iniziale di un utente è visibile all'amministratore, si può procedere facendo in modo che l'utente cambi immediatamente la password seguendo la procedura normale.
A volte può accadere che un utente dimentichi la password o che l'amministratore determini che la password di un utente è compromessa. Per poter risolvere questi problemi, si consiglia di consentire all'amministratore di cambiare la password di qualsiasi utente generandone una nuova. Per effettuare questa operazione, non occorre che l'amministratore conosca la password dell'utente. È sufficiente che per la distribuzione della password segua le stesse regole valide per l'assegnazione della password iniziale. Per la sostituzione di una password dimenticata è richiesta l'identificazione positiva dell'utente da parte dell'amministratore.

18.6 Responsabilità degli utenti

Gli utenti devono assumersi la responsabilità di mantenere riservate le password e di segnalare modifiche al proprio stato di utente, sospetti di violazioni della sicurezza e così via. Per assicurarsi della consapevolezza degli utenti in tema di protezione, si consiglia di far firmare a ciascun utente una dichiarazione in cui conferma di essere a conoscenza di questa responsabilità.

Il modo più semplice per risolvere i problemi di compromissione delle password consiste nel cambiarle. Per evitare che esistano password compromesse di cui non si conosce l'esistenza, è necessario che le password siano cambiate periodicamente. La modifica delle password deve avvenire abbastanza frequentemente, in modo che la probabilità di compromissione durante la durata di vita di una password sia sufficientemente bassa. Per evitare la visibilità inutile delle password all'amministratore, gli utenti devono essere in grado di cambiarle da soli.

18.7 Criteri per la posta elettronica

La posta elettronica riveste un'importanza sempre crescente per la normale conduzione del lavoro. Le organizzazioni devono predisporre criteri per la posta elettronica per consentire ai dipendenti di utilizzarla in modo appropriato, per ridurre il rischio di cattivo uso intenzionale o involontario e per assicurare che le registrazioni ufficiali trasferite tramite posta elettronica siano gestite correttamente. Così come esistono criteri per l'uso appropriato del telefono, le organizzazioni devono quindi definire anche criteri per l'uso corretto della posta elettronica. I criteri dell'organizzazione sono necessari per stabilire un controllo generale nelle aree seguenti:

- Uso della posta elettronica per svolgere attività ufficiali
- Uso della posta elettronica a scopo privato
- Controllo dell'accesso e protezione della riservatezza dei messaggi
- Gestione e archiviazione dei messaggi di posta elettronica

È facile avere problemi con la posta elettronica. Le cartelle della posta possono infatti crescere fino a bloccare il sistema di posta. La configurazione errata del software per i forum di discussione può causare l'invio di messaggi ai gruppi sbagliati. Errori nelle liste di distribuzione possono sommergere gli utenti con centinaia di messaggi di errore. A volte i messaggi di errore possono rimbalzare da un server di posta elettronica all'altro. Alcuni metodi per impedire che si verifichino tali problemi sono:

- Addestrare gli utenti ad affrontare e risolvere i problemi che si possono verificare e a utilizzare gli strumenti in modo corretto.
- Configurare i programmi di posta elettronica in modo che la modalità di funzionamento predefinita sia anche quella più sicura.
- Utilizzare programmi che rispettano rigorosamente le convenzioni e i protocolli Internet di posta elettronica. Ogni volta che un servizio in linea collega tramite un gateway un sistema di posta elettronica proprietario a Internet, si verificano proteste a causa del flusso di messaggi di errore generati dal malfunzionamento dei server di posta elettronica.

Utilizzando algoritmi di crittografia per firmare digitalmente i messaggi di posta elettronica si può evitare che vengano assunte delle identità fittizie. Crittografando il contenuto del messaggio o il canale su cui viene trasmesso si può evitare di essere spiati.

Gli utenti che usano luoghi pubblici come i cybercafé e le chat per accedere alla posta elettronica possono lasciare informazioni importanti memorizzate nella cache o scaricate sul computer. In questi casi è quindi necessario pulire il computer dopo averlo utilizzato, in modo da non lasciarvi alcun documento importante. Questo è spesso un problema in luoghi quali le sale d'aspetto degli aeroporti.

18.8 Criteri per Internet

Il Web è formato da componenti software e da un insieme di protocolli e convenzioni che consentono di spostarsi e trovare informazioni su Internet. Mediante tecniche ipertestuali e multimediali, chiunque è in grado di esplorare e contribuire al Web con semplicità.
I client Web, noti anche come browser Web, forniscono un'interfaccia utente che consente di spostarsi tra le informazioni posizionando il puntatore e facendo clic. I browser introducono vulnerabilità in un'organizzazione, anche se generalmente meno gravi delle minacce poste dai server.

I server Web possono essere attaccati direttamente o utilizzati come punto di partenza per attaccare le reti all'interno di un'organizzazione. Sono molte le aree dei server Web da proteggere: il sistema operativo sottostante, il software del server Web, gli script del server, software di altro tipo e così via. I firewall, una configurazione appropriata dei router e il protocollo IP possono contribuire a respingere gli attacchi di negazione del servizio.

18.9 Criteri per il backup e il ripristino

Le operazioni di backup sono importanti soprattutto quando le informazioni memorizzate nel sistema sono fondamentali e preziose. I backup sono importanti per molti motivi:

- *Errori hardware*. Alcuni componenti hardware quali dischi rigidi o sistemi RAID potrebbero non funzionare.
- *Errori software*. Alcune applicazioni potrebbero avere difetti a causa dei quali le informazioni vengono interpretate o memorizzate in modo non corretto.
- *Errori dell'utente.* Gli utenti spesso modificano o eliminano i file accidentalmente. Predisponendo backup regolari si possono ripristinare i file modificati o eliminati.
- *Errori dell'amministratore.* A volte anche gli amministratori commettono degli errori, come l'eliminazione fortuita di account utente attivi.
- *Azioni di hacker e atti vandalici.* Gli hacker a volte alterano o eliminano i dati.
- *Furto.* I computer sono costosi e in genere facili da vendere. A volte il furto si limita ai componenti hardware presenti all'interno del computer, quali i dischi rigidi, le schede video e le schede audio.
- *Calamità naturali.* Inondazioni, terremoti, incendi e tempeste possono avere conseguenze disastrose sui sistemi di computer. L'edificio può subire danni o venire distrutto.
- *Altre calamità.* Altri danni possono essere provocati da eventi imprevedibili quali cadute di aerei su edifici o esplosioni causate da fuoriuscite di gas.

Quando si effettuano aggiornamenti del software o aggiornamenti dell'hardware:

- Non effettuare mai gli aggiornamenti senza eseguire il backup dei file di dati indispensabili.
- Assicurarsi di eseguire il backup delle informazioni di sistema quali i registri e i record di avvio principali e del settore di avvio della partizione.

.

Le informazioni di cui è necessario eseguire il backup comprendono:

- Informazioni importanti riservate all'organizzazione e indispensabili per la continuità di funzionamento. Sono inclusi database, server della posta e qualsiasi file degli utenti.
- Database di sistema, quali database di account utente e registri.

18.10 Archiviazione dei backup in sede e fuori sede

Archiviazione in sede: archiviare i backup in un luogo sicuro a prova di incendio. I backup non devono essere archiviati nel cassetto del tavolo su cui si trova il computer. L'archiviazione sicura protegge dalle calamità naturali, dal furto e dal sabotaggio dei dati fondamentali. Anche tutti i componenti software, inclusi sistemi operativi, service pack e altre applicazioni critiche, dovrebbero essere archiviati in un posto sicuro.

Archiviazione fuori sede: i dati importanti dovrebbero essere archiviati anche fuori sede. Alcune società sono specializzate nell'archiviazione dei dati. Una soluzione alternativa consiste nell'utilizzare una cassetta di deposito di una banca.

19 Risposta agli incidenti

Per qualsiasi azienda è di fondamentale importanza che il reparto IT sia in grado di gestire eventuali incidenti relativi alla protezione. Numerose organizzazioni, infatti, si preparano a rispondere a tali incidenti solo dopo aver subito un attacco, ma a questo punto le conseguenze possono essere decisamente più gravi del necessario. La capacità di rispondere in modo adeguato a un incidente deve costituire parte integrante della strategia globale di un'azienda ai fini della protezione e della riduzione dei rischi.

Tale capacità può offrire considerevoli vantaggi diretti, ma anche benefici indiretti di ordine finanziario. Ad esempio, è possibile che le compagnie di assicurazioni pratichino sconti particolari se l'azienda dimostra di essere in grado di gestire eventuali attacchi in modo rapido e conveniente. Un piano di risposta agli incidenti consolidato inoltre, può consentire ai provider di servizi di ampliare la propria base di clienti, poiché dimostra l'interesse a fornire un processo di protezione delle informazioni efficiente.

L'elenco di controllo riportato di seguito descrive le procedure a cui attenersi per rispondere in modo efficace agli incidenti. L'esatto ordine dei passaggi da eseguire dipende dal tipo di organizzazione e dalla natura dell'incidente.

Indicazioni generali per la risposta agli incidenti	
Documentare tutte le informazioni, annotando eventuali commenti. Riportare le operazioni eseguite, il momento e il motivo della loro esecuzione.	
Mantenere la calma, evitando di farsi prendere dal panico. Attenersi attentamente ai criteri di sicurezza.	
Utilizzare strumenti di comunicazione non in linea, come voce, telefono e fax, dato che l'autore dell'attacco potrebbe essere in grado di rilevare i dati trasmessi in rete.	
Restare costantemente in comunicazione con tutti i team e con qualsiasi altra persona interessata.	
Non riavviare computer o eseguire accessi e disconnessioni, perché queste operazioni possono avviare codice dannoso.	
Obiettivo 1 - Valutazione iniziale	
1.1	Contattare il personale tecnico per verificare che l'incidente non sia un falso positivo.
1.2	Esaminare i log di controllo per verificare la presenza di attività insolite, la mancanza di log o l'assenza di informazioni all'interno dei log.
1.3	Cercare di identificare gli strumenti utilizzati dall'autore dell'attacco (strumenti di intercettazione delle password, cavalli di Troia e così via).
1.4	Verificare che non siano presenti applicazioni non autorizzate configurate per l'avvio automatico.
1.5	Esaminare gli account per controllare che non siano stati acquisiti impropriamente privilegi o appartenenze a gruppi.
1.6	Verificare che non siano in esecuzione processi non autorizzati.
1.7	Decidere se esistono prove che è opportuno conservare.
1.8	Confrontare le prestazioni dei sistemi compromessi con i parametri di riferimento.

1.9	Definire un livello di priorità iniziale e un responsabile dell'incidente.
Obiettivo 2 - Segnalazione dell'incidente	
2.1	Comunicare l'incidente a tutti gli interessati e i membri del CSIRT (Computer Security Incident Response Team).
Obiettivo 3 - Contenimento dei danni e riduzione dei rischi	
3.1	In base alla gravità dell'incidente e ai criteri di sicurezza adottati, isolare i sistemi colpiti disconnettendoli.
3.2	Modificare le password dei sistemi colpiti.
3.3	Eseguire il backup dei sistemi per il ripristino dei dati e, se necessario, per raccogliere prove.
Obiettivo 4 - Identificazione della gravità e del tipo di violazione	
4.1	Determinare il tipo di attacco.
4.2	Determinare lo scopo dell'attacco (automatico, rivolto specificamente contro l'organizzazione o per raccolta di informazioni)
4.3	Individuare tutti i sistemi coinvolti nell'attacco. Se vengono identificati nuovi sistemi, ripetere i passaggi relativi al contenimento dei danni.
4.4	Ripetere la valutazione e se necessario riassegnare il livello di priorità dell'evento.

Obiettivo 5 - Protezione delle prove	
5.1	Non appena consentito dai processi di risposta e ripristino, eseguire il backup dei sistemi su supporti mai utilizzati in precedenza.
5.2	Se possibile, eseguire backup completi, inclusi i log e lo stato dei sistemi.
5.3	Definire le responsabilità per la custodia delle prove raccolte.
5.4	Proteggere le prove e documentare nonché i dati relativi a quando, come e da chi sono state raccolte, oltre alle persone che hanno avuto accesso alle prove.
Obiettivo 6 – Notifica a organismi esterni	
6.1	Con il supporto di un consulente legale, segnalare l'incidente alle autorità appropriate.
6.2	Informare dell'incidente i responsabili delle relazioni pubbliche del CSIRT e fornire la necessaria assistenza.
6.3	Segnalare l'incidente a eventuali organismi di competenza, come il CERT Coordination Center della Carnegie Mellon University (http://www.cert.org), che potrebbero fornire informazioni utili per il ripristino.
Obiettivo 7 - Ripristino dei sistemi	
7.1	Individuare e convalidare i più recenti backup non compromessi.
7.2	Ripristinare il sistema.
7.3	Verificare le funzionalità dei sistemi e confrontarne le prestazioni con i parametri di riferimento.
7.4	Controllare eventuali ripetizioni degli attacchi o errori di configurazione dovuti alle procedure di contenimento dei danni.
Obiettivo 8 - Preparazione e organizzazione della documentazione relativa all'incidente	
8.1	Raccogliere e organizzare tutte le annotazioni e le registrazioni relative all'incidente.
8.2	Distribuire la documentazione a tutti gli interessati affinché venga rivista e approvata (inclusa la valutazione dell'idoneità delle prove dal punto di vista legale).
8.3	Analizzare la causa della violazione e migliorare la strategia di difesa allo scopo di prevenire attacchi analoghi in futuro.
8.4	Assistere il reparto amministrativo nella valutazione dei costi derivanti dall'attacco.
8.5	Preparare un report per illustrare ai dirigenti e a tutti gli interessati la dinamica dell'incidente, il relativo impatto economico e le contromisure adottate per evitare nuovi attacchi.

19.1 Case study

Gestione degli incidenti presso un'azienda Americana -Northwind Traders

Per dimostrare come i vari passaggi della risposta a un incidente consentano di affrontare un attacco, è stato elaborato un case study che illustra la risposta del team CSIRT di Northwind Traders alla diffusione del virus Code Red II. Sebbene questo case study sia fittizio, le contromisure attuate riflettono fedelmente quelle adottate da organizzazioni reali in caso di attacco.

Tabella : Case study Northwind Traders

Fase della risposta all'incidente	Contromisura attuata
Elaborazione di una valutazione iniziale	Samantha Smith, membro del team CSIRT, riceve una breve descrizione di un evento registrato dal sistema di rilevamento delle intrusioni di Northwind Traders. Il sistema indica un possibile attacco causato da Code Red II nel server Web WEB2. Samantha cerca la stringa della firma nel file di log IIS di WEB2 e verifica l'esistenza di root.exe in c:\inetpub\scripts. I risultati di questa indagine suggeriscono che non si tratta di un falso positivo.
Segnalazione dell'incidente	Samantha comunica telefonicamente i primi risultati al CSIRT e si accorda per notificare eventuali dettagli aggiuntivi non appena saranno disponibili.
Limitazione dei danni e riduzione dei rischi	Poiché la strategia di risposta agli incidenti adottata da Northwind Traders prevede che, quando si rileva la presenza di un virus, il sistema sia rimosso dalla rete, Samantha disconnette il cavo di rete. Fortunatamente, WEB2 appartiene a un insieme di server con carico bilanciato, quindi i clienti non rileveranno tempi di inattività causati dalla disconnessione.
Determinazione della gravità dell'intrusione	Samantha analizza i file di log degli altri server per determinare se il virus si è diffuso e scopre che questo non è accaduto.
Segnalazione dell'incidente	Samantha comunica i risultati di questa ulteriore indagine al CSIRT tramite posta elettronica e contatta direttamente il responsabile del team CSIRT; quest'ultimo nomina Responsabile degli incidenti Mike Danseglio, un responsabile della protezione delle informazioni. Mike coordinerà tutte le attività e le comunicazioni provenienti e dirette al CSIRT principale. Mike notifica al Director of Technology e al team IT che il server Web è stato disconnesso dalla rete e che verrà ripulito dal virus prima di essere nuovamente connesso. Mike informa inoltre i dirigenti, il Responsabile delle pubbliche relazioni e il rappresentante legale, il quale

	suggerisce che, sebbene non sia possibile perseguire i colpevoli, è comunque consigliabile applicare le procedure per la raccolta delle prove.
Limitazione dei danni e riduzione dei rischi	Robert Brown, un altro membro del CSIRT, esegue Hfnetchk per stabilire se negli altri server è stata installata la patch relativa a Code Red II. Dopo aver individuato due sistemi non aggiornati, installa immediatamente la patch.
Determinazione della gravità dell'intrusione	Robert esegue un'ulteriore analisi dei file di log di tutti gli altri server IIS e rileva che, in quel momento, non esiste alcuna altra istanza del virus Code Red II.
Protezione delle prove	Tutti i risultati indicano che i danni sono circoscritti a WEB2. Poiché il danno è ragionevolmente limitato e il rappresentante legale ha suggerito di raccogliere le prove, Mike decide di effettuare questa operazione prima di sottoporre il sistema a un'analisi più approfondita, che potrebbe alterare o distruggere eventuali prove. Gli altri membri del team continuano a monitorare i log e i server Web per rilevare attività sospette. Un membro del CSIRT, specializzato nella raccolta di prove legali, crea due snapshot del sistema manomesso. Uno verrà accuratamente protetto ai fini di un'ulteriore accertamento legale, mentre l'altro potrà essere utilizzato nel processo di ripristino insieme ai backup eseguiti prima dell'incidente. I backup a fini legali vengono eseguiti su supporti WORM mai utilizzati prima, vengono accuratamente documentati, firmati e conservati in luoghi sicuri insieme ai dischi rigidi del server, come previsto dai criteri di protezione.

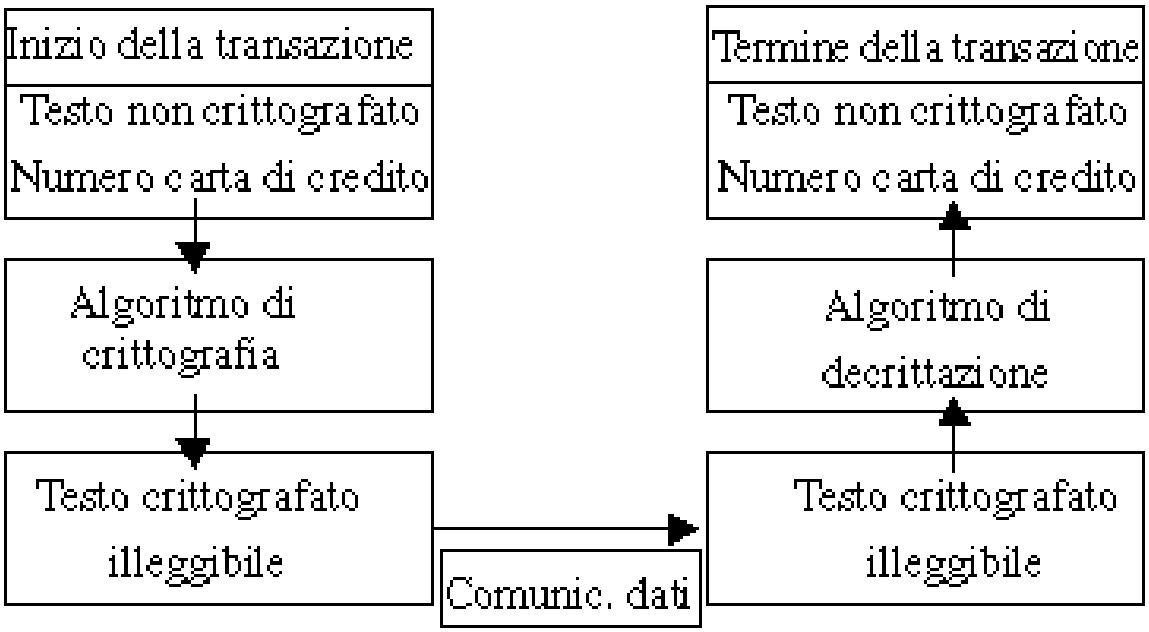
Fase della risposta all'incidente	Contromisura attuata
Identificazione del tipo e della gravità dell'intrusione	Il portatile in cui sono stati installati gli strumenti di protezione dell'organizzazione e che contiene vari strumenti legali viene utilizzato per controllare il backup di ripristino alla ricerca di ulteriori intrusioni. Nelle voci e nelle cartelle del Registro di sistema vengono cercate eventuali aggiunte alle aree che eseguono il software all'avvio, quali directory di profilo/avvio e chiavi Run e RunOnce del Registro di sistema. Il controllo delle modifiche viene eseguito anche negli account User e Groups nonché in Diritti utente e Criteri di protezione.
Notifica a organismi esterni	Mike comunica l'incidente al National Infrastructure Protection Center dell'FBI, poiché Northwind Traders partecipa a numerosi e importanti progetti del governo statunitense. Poiché il virus non ha influito né sulle informazioni dei clienti né sull'accesso ai sistemi, i clienti non vengono informati dell'accaduto.
Ripristino dei sistemi	Sebbene siano disponibili strumenti in grado di eliminare Code Red II da WEB2, il CSIRT e il team di supporto del server preferiscono reinstallare il sistema operativo su supporti nuovi. Questa operazione garantisce, infatti, che nel sistema non siano presenti file danneggiati o backdoor sfruttabili dai pirati informatici. Dopo aver reinstallato Windows 2000, il livello di protezione del sistema viene incrementato seguendo le istruzioni fornite nei precedenti capitoli di questa guida. Dopo aver individuato un backup non infetto, i dati vengono ripristinati con la massima cautela. Se i dati sono disponibili solo in backup infetti, questi vengono ripristinati in un sistema separato e non connesso e, quindi, reintrodotti in WEB2 dopo aver verificato che non costituiscano un pericolo. Il team CSIRT esegue una valutazione completa della vulnerabilità del sistema, documentando tutte le informazioni ricavate durante il processo. WEB2 viene nuovamente connesso e accuratamente monitorato.

Fase della risposta all'incidente	Contromisura attuata
Preparazione e organizzazione della documentazione relativa all'incidente	Mike e il CSIRT ricercano la causa della vulnerabilità e controllano se il sistema è stato reinstallato di recente senza applicare le necessarie patch, operazione contraria alla strategia chiaramente definita e già in uso. Vengono individuate le tre principali cause che hanno agevolato l'attacco: i membri del team di supporto non hanno reinstallato le patch, il reparto Information Security non ha controllato tempestivamente le patch installate e il gruppo Configuration Management non ha individuato la necessità di implementare le patch e di coinvolgere, quindi, Information Security nella verifica del sistema prima di ripristinare lo stato operativo. L'applicazione di tutte queste procedure avrebbe consentito di evitare l'intrusione. Per impedire che tali incidenti si verifichino nuovamente, il team decide di implementare una nuova procedura. Viene creato un elenco di controllo che deve essere completato da Change Management, Web Server Support e Information Security prima che quest'ultimo connetta o riconnetta qualsiasi sistema alla rete interna. La procedura basata sull'elenco di controllo deve essere completata prima che Information Security possa riconfigurare il firewall in modo da consentire l'accesso esterno al e dal sistema. Il reparto Audit deve inoltre verificare periodicamente che gli elenchi di controllo siano eseguiti in modo completo e accurato. Mike e il CSIRT preparano tutta la documentazione necessaria per determinare quali attività, specifiche per l'incidente, sono state completate, il momento in cui ciascuna di esse è stata eseguita e da chi. Queste informazioni vengono inviate al rappresentante finanziario, che calcola i costi in base ai principi GAAP (Generally Accepted Account Principles) relativi ai danni riportati dai computer. Il responsabile del team CSIRT deve comunicare agli addetti alla gestione il costo totale dell'attacco, quali sono i motivi che lo hanno determinato e come si intende prevenire tali incidenti in futuro. È importante che i responsabili della gestione comprendano le implicazioni derivate dal non aver rispettato le procedure e dalla mancanza di risorse adeguate, quale il CSIRT. La documentazione complessiva sull'incidente, l'esperienza maturata e le strategie seguite, o non seguite, vengono controllate dai membri del team. La documentazione e le procedure utilizzabili ai fini di un'azione legale vengono esaminate dal rappresentante legale, dal responsabile del team e dal responsabile degli incidenti CSIRT, oltre che dai dirigenti.

20 Sistemi Crittografici

20.1 Accesso protetto, dati protetti e codice protetto

Anche se gli utenti desiderano riservatezza e privacy, i malintenzionati possono spiare o sottrarre informazioni riservate per l'individuo o l'organizzazione. Se una società mette a punto un prodotto innovativo e ne memorizza le idee su un sistema di computer, esigerà protezione per i dati presenti su quel sistema e per il trasferimento dei dati da un sistema all'altro. Le reti e i canali di comunicazione dati spesso non sono protetti per cui i messaggi che li attraversano sono soggetti a minacce passive e attive. Si dice minaccia passiva quando un intruso intercetta i messaggi per visualizzarne i dati. Questo tipo di intrusione è anche noto come "eavesdropping". Si dice minaccia attiva quando un intruso modifica i messaggi intercettati. La crittografia è uno strumento efficace per proteggere i messaggi dalle minacce attive e passive durante le comunicazioni dati.
La crittografia consente di convertire il testo leggibile, o testo non crittografato, in un formato illeggibile, o testo crittografato e viceversa. Il processo di conversione consiste in una sequenza di calcoli matematici. I calcoli modificano l'aspetto dei dati senza alterarne il significato.
Per proteggere un messaggio, il creatore converte il testo normale del messaggio in testo crittografato. Questo processo, chiamato crittografia, è mostrato nel diagramma di flusso che segue. Il testo crittografato viene trasmesso attraverso una rete o un canale di comunicazione dati. Se il messaggio viene intercettato, l'intruso ha accesso solo al testo crittografato illeggibile. Alla ricezione, il destinatario del messaggio converte il testo crittografato nel formato testo normale originale. Questo processo è chiamato decrittazione.



Le operazioni matematiche usate per convertire il testo normale in testo crittografato e viceversa si chiamano algoritmi di crittografia. Gli algoritmi di crittografia richiedono almeno un valore che controlli il processo di conversione. Questo valore è chiamato chiave. Dato lo stesso testo e lo stesso algoritmo, chiavi differenti generano conversioni diverse.
La crittografia viene usata per fornire i servizi seguenti: autenticazione, integrità, non-ripudio e segretezza. Per un messaggio di posta elettronica, ad esempio, la crittografia fornisce:

- *Autenticazione.* Consente al destinatario di un messaggio di convalidarne l'origine. Impedisce a un impostore di assumere l'identità del mittente del messaggio.
- *Integrità.* Garantisce al destinatario che il messaggio non è stato modificato durante il percorso. Si noti che il servizio di integrità consente al destinatario di rilevare la modifica del messaggio, ma non di impedirla.
- *Non-ripudio.* Esistono due tipi di servizi di non-ripudio. Il servizio di non-ripudio con verifica di origine garantisce al destinatario l'identità del mittente. Il servizio di non-ripudio con verifica di recapito garantisce al mittente il recapito del messaggio.
- *Segretezza.* Nota anche come riservatezza, impedisce la rivelazione del messaggio agli utenti non autorizzati.

20.2 Infrastrutture a chiave pubblica

La crittografia a chiave pubblica può giocare un ruolo importante nella fornitura di servizi di protezione indispensabili tra cui la riservatezza, l'autenticazione, le firme digitali e l'integrità. La crittografia a chiave pubblica usa due chiavi elettroniche: una pubblica e una privata. Queste chiavi sono correlate matematicamente, ma la chiave privata non può essere determinata da quella pubblica. La chiave pubblica può essere conosciuta da tutti mentre il proprietario mantiene segreta quella privata.

Un'infrastruttura a chiave pubblica (PKI, Public Key Infrastructure) fornisce gli strumenti per associare le chiavi pubbliche ai rispettivi proprietari e consente la distribuzione di chiavi pubbliche affidabili all'interno di reti eterogenee di grandi dimensioni. Le chiavi pubbliche vengono associate ai rispettivi proprietari tramite certificati di chiave pubblica.

Questi certificati contengono informazioni quali il nome del proprietario e la chiave pubblica associata e sono rilasciate da un'autorità di certificazione (CA) attendibile. I certificati digitali, chiamati anche ID digitali, sono analoghi alle patenti di guida, ai passaporti o alle tessere di associazione. Un certificato digitale può essere presentato elettronicamente per dimostrare la propria identità o il diritto di accesso a informazioni o servizi in linea. I certificati digitali non sono usati solo per identificare gli utenti, ma anche per identificare i siti Web, funzione fondamentale per la protezione dell'e-business e del software che viene inviato sul Web. I certificati digitali forniscono attendibilità e protezione quando si comunica o si effettuano operazioni commerciali su Internet.

Una PKI è composta in genere da molte CA (autorità di certificazione) collegate tramite percorsi affidabili. Le CA possono essere collegate in molti modi. Possono essere disposte gerarchicamente sotto una "CA principale" che rilascia certificati a CA subordinate o in modo indipendente all'interno di una rete. Ciò costituisce l'architettura PKI.

20.3 Firme digitali

Le transazioni elettroniche sono sempre più importanti. Molte società che forniscono servizi in linea ed e-commerce vorrebbero disporre di meccanismi in grado di far aumentare la fiducia nelle transazioni elettroniche. Un acquirente che compra un prodotto passando al venditore un assegno bancario (cambiale) deve firmare l'assegno per assicurare la propria identità e convalidare la transazione.

La diffusione dell'uso della tecnologia PKI per il supporto delle firme digitali può contribuire ad aumentare la fiducia nelle transazioni elettroniche. Ad esempio, l'uso di una firma digitale consente a un venditore di dimostrare l'avvenuta richiesta di beni e servizi da parte di un acquirente e di esigerne quindi il pagamento. L'uso di una PKI consente a individui che non si conoscono di effettuare transazioni verificabili.

Ad esempio, un compratore interessato all'acquisto elettronico di beni dovrà ottenere un certificato di chiave pubblica da una CA. Il processo di ottenimento di un certificato da una CA consiste nel generare un coppia di chiavi pubblica-privata. L'acquirente invia una chiave pubblica con informazioni valide relative alla società a un'autorità di registrazione (RA, Registration Authority) e richiede un certificato. La RA verifica l'identità dell'acquirente in base alle informazioni fornite e risponde di ciò a una CA, che quindi rilascia il certificato.

Il nuovo acquirente certificato può ora firmare ordini di acquisto elettronici dei beni. Il fornitore che riceve l'ordine di acquisto può ottenere il certificato del compratore e l'elenco di revoca dei certificati (CRL, Certificate Revocation List) per la CA che ha rilasciato il certificato del compratore, controllare che il certificato non sia stato revocato e verificare la firma dell'acquirente. Verificando la validità del certificato, il fornitore conferma la ricezione di una chiave pubblica valida per il compratore. Verificando la firma sull'ordine di acquisto, il fornitore assicura che l'ordine non è stato modificato dopo che l'acquirente lo ha emesso.
Una volta stabilita la validità del certificato e della firma, il fornitore può spedire i beni richiesti al compratore essendo certo che sono stati effettivamente ordinati. Questa transazione può avvenire senza alcuna relazione preliminare tra l'acquirente e il venditore.

20.4 Secure Sockets Layer (SSL)

Il protocollo SSL protegge i dati che vengono trasmessi tra i browser e i server Web. Assicura inoltre che i dati provengano effettivamente dal sito Web di origine e che non siano stati alterati durante il percorso. Tutti gli indirizzi dei siti Web che iniziano con "https" sono stati abilitati all'utilizzo di SSL.
Il protocollo SSL fornisce un livello di protezione e riservatezza per chi desidera condurre transazioni protette su Internet. Il protocollo SSL protegge le trasmissioni HTTP su Internet aggiungendo un layer di crittografia che esclude la possibilità che le transazioni vengano intercettate da terzi.
Il protocollo SSL consente agli utenti del sito Web di comunicare in modo protetto tramite sessioni crittografate. L'uso di questo protocollo risulta fondamentale per le società che desiderino realizzare soluzioni di e-commerce, attività che prevede la ricezione di numeri di carta di credito o di altre informazioni riservate. Gli utenti del Web si accorgono di avere raggiunto un sito protetto da SSL grazie alla stringa "https" all'inizio dell'indirizzo della pagina Web. La "s" aggiunta al noto termine HTTP (HyperText Transfer Protocol) sta per sicuro.
Le società che desiderino condurre affari tramite Internet utilizzando le caratteristiche SSL devono rivolgersi a un'autorità di certificazione, ad esempio VeriSign Inc., che è un'organizzazione indipendente in grado di confermare l'identità di una società. La società potrà quindi configurare i relativi server Web per le connessioni SSL. Gli utenti non devono effettuare alcuna operazione per attivare una connessione SSL. La parte client dell'SSL è incorporata nel browser Web.

20.5 Protezione della posta elettronica

La posta elettronica standard di Internet viene in genere inviata sulla rete come testo normale. Gli intrusi possono quindi monitorare i server della posta e il traffico di rete per ottenere informazioni riservate.

Attualmente, i metodi proposti per fornire servizi per la protezione della posta elettronica sono due: Pretty Good Privacy (PGP) e Secure/Multipurpose Internet Mail Extensions (S/MIME). Questi servizi comprendono in genere l'autenticazione del creatore e la riservatezza dei dati. Possono anche fornire una ricevuta firmata dal destinatario.

Queste funzionalità si basano sull'uso della tecnologia a chiave pubblica e l'uso su vasta scala delle chiavi pubbliche richiede un metodo di certificazione che consenta di accertare che una determinata chiave appartiene a uno specifico utente.

PGP è uno schema crittografico di tipo militare disponibile per tutti gli utenti di computer. Si basa sull'uso di insiemi di coppie di chiavi. La chiave pubblica consente di codificare un messaggio che può essere decodificato solo con la chiave privata corrispondente.

Analogamente, l'autenticità della posta elettronica "firmata" con una chiave privata può essere verificata solo con la chiave pubblica corrispondente.
S/MIME è lo stesso metodo crittografico utilizzato per proteggere la posta elettronica, adottato da tutti i principali fornitori di posta elettronica. S/MIME usa la crittografia a chiave pubblica per firmare digitalmente e crittografare ciascun messaggio inviato tra partner commerciali. Questo assicura che il messaggio *non* venga letto, provenga solo dal mittente e non venga alterato durante il percorso.

20.6 Crittografia del file system

La crittografia dei dati è diventata sempre più importante nel lavoro di ogni giorno. Gli utenti cercano un metodo che consenta di proteggere i dati con la massima comodità e con requisiti aggiuntivi minimi. Desiderano usare un sistema di protezione in grado di proteggere tutti i file usati da una qualsiasi delle applicazioni, senza ricorrere a metodi di crittografia specifici di un'applicazione.
Con la tecnologia avanzata attualmente disponibile, gli affari si basano su registrazioni elettroniche. In precedenza, usare computer in rete o laptop remoti significava sacrificare la produttività o rischiare delle perdite. Viaggiare portando con sé copie di database di lavoro importanti era improponibile, ma ora non più.
Al giorno d'oggi, le informazioni aziendali critiche non risiedono più unicamente su mainframe o server centrali. Le informazioni riguardanti le strategie, la ricerca, lo sviluppo di prodotti, il marketing, i segreti aziendali e i dati di terze parti sono ora distribuite sui singoli computer all'interno dell'organizzazione. Le workstation, computer normali in posizioni fisse, singoli computer in uffici domestici e notebook, rappresentano i punti di accesso all'organizzazione più numerosi e più vulnerabili e sono tutti soggetti a intrusioni e furti.

Anche se un'organizzazione dispone di una protezione avanzata per l'accesso alla rete, una workstation non sorvegliata consente l'accesso immediato a file presenti sul disco rigido e persino sulla rete. Analogamente, un notebook rubato consente a concorrenti, dipendenti non autorizzati e altri utenti di accedere agevolmente a dati critici, la cui conoscenza può favorire guadagni a spese dell'organizzazione.
Per evitare che gli aggressori possano leggere file presenti sui dischi, è possibile usare l'EFS (Encrypting File System). L'EFS è una nuova funzionalità di Microsoft Windows 2000 che assicura la protezione e la riservatezza dei dati importanti tramite l'utilizzo della crittografia simmetrica delle chiavi insieme alla tecnologia della chiave pubblica.

Solo il proprietario del file protetto può aprirlo e leggerlo come un documento normale. La funzionalità EFS è integrata nel file system NT (NTFS). È possibile impostare l'attributo di crittografia per le cartelle e i file così come si fa per gli altri attributi.
L'EFS assicura la riservatezza agli utenti. Oltre all'utente che crittografa il file, solo un amministratore designato può decrittarlo in caso di ripristino di emergenza. L'EFS è un'operazione trasparente. L'utente non dovrà pertanto crittografare né decrittare il file.

20.7 Autenticazione

I sistemi di computer moderni forniscono servizi a più utenti e richiedono la capacità di identificare accuratamente l'utente che effettua la richiesta. Nei sistemi tradizionali, l'identità dell'utente viene verificata controllando una password digitata durante l'accesso. Il sistema registra l'identità e la usa per determinare le operazioni che possono essere effettuate. Il processo di verifica dell'identità dell'utente è chiamato autenticazione. L'uso dell'autenticazione basata su password non è appropriato per le reti di computer. Le password inviate in rete possono infatti essere intercettate e successivamente usate da impostori per assumere l'identità di altri utenti.

È importante verificare l'identità di qualcuno o qualcosa. Gli amministratori, non volendo permettere l'accesso a utenti non autorizzati o consentire a impostori di assumere l'identità di altri utenti, devono essere in grado di controllare chiunque accede al sistema e di verificarne l'identità. Microsoft Windows 2000 supporta due tipi di protocolli di autenticazione: Kerberos e NTLM. Il primo è il protocollo di autenticazione predefinito per i computer che eseguono Windows 2000. Il protocollo di autenticazione NTLM viene invece fornito per compatibilità con sistemi operativi Microsoft precedenti. In questa sezione verranno illustrate le varie caratteristiche di ciascun protocollo e le relative applicazioni.

20.8 Autenticazione Kerberos

Kerberos è stato sviluppato per fornire un'autenticazione avanzata per applicazioni client e server tramite crittografia con chiave segreta. Il protocollo Kerberos usa una crittografia avanzata in modo tale che un client possa dimostrare la sua identità a un server e viceversa attraverso una connessione di rete non protetta. Kerberos è un sistema di autenticazione di terze parti attendibile, il cui scopo principale è quello di consentire agli utenti e ai processi, chiamati principal, di dimostrare la propria identità in modo affidabile attraverso una rete non protetta. Invece di trasmettere le password segrete in chiaro, che sono soggette a intercettazione e lettura da parte di individui non autorizzati, i principal usano speciali tagliandi Kerberos, chiamati ticket di sessione, per autenticarsi reciprocamente. Un ticket è valido solo per la sessione durante la quale l'utente si è connesso.

L'autenticazione Kerberos richiede l'esistenza di un'entità di rete attendibile che svolga la funzione di server di autenticazione per i client e i server che richiedono informazioni di autenticazione. Questo server di autenticazione è chiamato Centro distribuzione chiavi (KDC, Key Distribution Center). Ha accesso a un database composto da un elenco di utenti e servizi client, dai relativi parametri di autenticazione predefiniti, dalle relative chiavi crittografiche e da altri dati. L'autenticazione è in genere un processo unidirezionale. È il processo tramite il quale un servizio autentica il client. Un vantaggio di Kerberos rispetto a NTLM consiste nella possibilità di autenticazione reciproca, che prevede anche l'autenticazione del servizio da parte del client.
L'autenticazione Kerberos viene realizzata attraverso lo scambio di messaggi speciali, i ticket di sessione, tra le applicazioni client, le applicazioni server e uno o più KDC. I processi client che agiscono per conto degli utenti si autenticano sui server per mezzo dei ticket di sessione. Il KDC genera i ticket, che vengono inviati ai processi client che li richiedono. Kerberos gestisce un insieme di chiavi segrete, una per ogni entità che deve essere autenticata all'interno di una determinata area di autenticazione o dominio. Un'area di autenticazione è l'equivalente per questo protocollo di un dominio di Windows 2000. Un client presenta un ticket al server come prova dell'identità del principal. Il ticket presentato al server "dimostra" che il client è stato autenticato da un KDC.
Kerberos, al contrario dell'NTLM, semplifica il processo di connessione e di accesso alle risorse. Nell'autenticazione Kerberos, il computer contatta prima il KDC per autenticarsi sulla rete. Quindi, quando l'utente è pronto ad accedere a una risorsa per la prima volta, contatta il KDC per ottenere un ticket di sessione per accedere alla risorsa. A ogni tentativo successivo, il computer potrà contattare direttamente la risorsa, usando lo stesso ticket, senza passare prima attraverso un domain controller. In questo modo viene eliminata la comunicazione inutile con il domain controller. Questo processo consente agli utenti di connettersi e accedere più velocemente alle risorse della rete.

20.9 Autenticazione NTLM

Nell'autenticazione NTLM, per evitare di rivelare le password direttamente su una rete considerata non attendibile, viene usato un sistema "challenge-response". In base a questo sistema, il server invia all'utente una specie di richiesta di verifica, in genere una stringa generata in modo casuale. L'utente elabora quindi una risposta, in genere una funzione basata sia sulla stringa di verifica che sulla password. In questo modo, un intruso che cattura una coppia verifica/risposta valida non potrà in ogni caso accedere al sistema dal momento che le stringhe di verifica future saranno probabilmente differenti e richiederanno risposte diverse.
In Microsoft Windows NT, il client contatta un Primary Domain Controller (PDC) o un Backup Domain Controller (BDC) per accedere al dominio. Quindi, quando è pronto a stabilire una sessione con una determinata risorsa, ad esempio una stampante condivisa, contatta il server che la gestisce. Il server, a propria volta, contatta il domain controller che gestisce la risorsa per fornirgli il token di accesso o le credenziali del client richieste. L'NTLM viene usato in Windows 2000 per compatibilità con prodotti Windows precedenti, ad esempio Windows NT e per evitare che gli utenti inviino le rispettive password non crittografate al servizio Telnet. Il servizio Telnet è implementato su Windows 2000 solo quando sono installati i Servizi per Unix.

20.10 Smart card

Le smart card sono carte simili a carte di credito che contengono una piccola quantità di memoria e a volte un microprocessore. Poiché le smart card contengono più memoria di una generica striscia magnetica e sono in grado di elaborare informazioni, vengono utilizzate in contesti di protezione dove queste caratteristiche sono indispensabili.

Consentono di memorizzare informazioni per l'accesso al sistema quali la chiave privata e altre informazioni personali dell'utente, inclusa la password. In un tipico ambiente di accesso con smart card, l'utente deve inserire la relativa smart card in una periferica di lettura connessa al computer. Il software usa quindi le informazioni memorizzate nella smart card per effettuare l'autenticazione. Il livello di protezione risulta maggiore se viene utilizzata insieme a una password e/o a un identificatore biometrico. Ad esempio, l'accesso risulta più sicuro se si deve sia inserire una smart card che immettere una password. Le utilità per la crittografia dei file che usano le smart card come chiavi della serratura elettronica rappresentano un altro utilizzo delle smart card a scopo di protezione.

20.11 Protezione del codice

La distribuzione elettronica del software su qualsiasi rete comporta potenziali problemi di protezione. Il software può infatti contenere programmi come virus e cavalli di troia. Per cercare di risolvere alcuni di questi problemi, è possibile associare ai file delle firme digitali. Un certificato digitale consente di stabilire l'identità tramite la crittografia a chiave pubblica. Il codice firmato con un certificato digitale verifica l'identità dell'autore e assicura che il codice non è stato alterato una volta firmato. La firma dei certificati e degli oggetti stabilisce l'identità e consente all'utente di prendere delle decisioni sulla validità dell'identità di una persona. Quando l'utente esegue il codice per la prima volta, viene visualizzata una finestra di dialogo. La finestra di dialogo contiene informazioni sul certificato e un collegamento all'autorità di certificazione.

Ad esempio, Microsoft ha sviluppato la tecnologia Authenticode, che consente agli sviluppatori e ai programmatori di firmare digitalmente il software. Prima che il software venga rilasciato pubblicamente o all'interno dell'organizzazione, gli sviluppatori possono firmarne digitalmente il codice. Se il codice viene modificato dopo essere stato firmato, la firma digitale diventa non valida. In Internet Explorer è possibile specificare impostazioni di protezione che impediscano agli utenti di scaricare o eseguire software non firmato da qualsiasi area di protezione. Internet Explorer può essere configurato per considerare automaticamente attendibili determinati fornitori di software e specifiche autorità, in modo tale che il codice e altre informazioni vengano accettate automaticamente.

20.12 Tecnologie per proteggere la connettività della rete

Le aziende e altre organizzazioni utilizzano Internet perché fornisce servizi utili. L'organizzazione può scegliere di supportare o meno servizi basati su Internet in base a un business plan o a un piano strategico per l'impiego di tecnologie informatiche. In altri termini, le organizzazioni dovrebbero analizzare le proprie esigenze, identificare i metodi che potrebbero soddisfarle e considerare, oltre al costo e altri fattori, anche le implicazioni riguardanti la protezione.
La maggior parte delle organizzazioni usano servizi basati su Internet per potenziare le comunicazioni tra le divisioni interne, tra l'azienda e i relativi clienti o per disporre di strumenti economici per l'automazione dei processi aziendali. La protezione è un aspetto importante in quanto un singolo incidente potrebbe vanificare il risparmio e i vantaggi offerti dalla connettività Internet.
Alcuni metodi per proteggere l'organizzazione da intrusioni esterne prevedono l'uso di firewall e di reti virtuali private (VPN, Virtual Private Network).

20.13 Firewall

Molte organizzazioni hanno connesso o desiderano connettere le proprie LAN private a Internet per consentire agli utenti di accedere ai servizi offerti da Internet. Poiché Internet non è globalmente affidabile, i sistemi privati sono vulnerabili ad attacchi e a utilizzi errati. Un firewall consente di controllare l'accesso tra una rete affidabile e una che lo è meno. Un firewall non è un singolo componente. È invece una strategia per proteggere le risorse di un'organizzazione raggiungibili tramite Internet. Un firewall agisce come custode tra Internet, non affidabile, e le reti interne più affidabili.
La funzione principale di un firewall consiste nel centralizzare il controllo dell'accesso. Se gli utenti esterni o remoti possono accedere alle reti interne senza passare attraverso il firewall, l'efficacia di quest'ultimo risulta minore. Ad esempio, se un responsabile dispone di un modem collegato al computer dell'ufficio che può chiamare mentre viaggia e il computer fa parte di una rete interna protetta, un aggressore che si collega a quel computer può eludere il firewall. Anche un utente che dispone di un account per l'accesso remoto a Internet presso un ISP commerciale e che si connette a Internet dal computer dell'ufficio usando un modem stabilisce una connessione non protetta a Internet che elude il firewall. I firewall forniscono molti tipi di protezione:

- Possono bloccare il traffico indesiderato.
- Possono reindirizzare il traffico in ingresso a più sistemi interni attendibili.
- Nascondono i sistemi vulnerabili che non possono essere protetti con semplicità da Internet.
- Possono registrare il traffico diretto e proveniente dalla rete privata.
- Possono nascondere informazioni quali i nomi di sistema, la topologia di rete, i tipi di periferica di rete e gli ID utente interni da Internet.
- Possono fornire un'autenticazione migliore rispetto a quella che le applicazioni standard sono in grado di offrire.

Come per qualsiasi altra misura di salvaguardia, esiste un conflitto tra efficienza e protezione. La trasparenza è la visibilità che il firewall ha nei confronti degli utenti interni e di quelli esterni che lo attraversano. Un firewall è trasparente agli utenti se essi non lo notano o non vi vengono bloccati nel tentativo di accedere a una rete. I firewall sono in genere configurati in modo da essere trasparenti agli utenti della rete interna quando accedono all'esterno. D'altra parte, i firewall sono configurati in modo tale da non essere trasparenti per gli utenti della rete esterna che lo attraversano. Questo fornisce in genere il massimo livello di protezione senza appesantire eccessivamente gli utenti interni.
Esistono tipi di firewall che comprendono gateway per il filtro dei pacchetti, gateway per applicazioni e gateway ibridi o complessi.
Gateway per il filtro dei pacchetti

I firewall per il filtro dei pacchetti usano router con regole di filtraggio dei pacchetti per consentire o negare l'accesso in base all'indirizzo di origine, l'indirizzo di destinazione e la porta. Offrono una protezione minima, ma hanno un costo molto contenuto e possono rappresentare una scelta appropriata per ambienti a basso rischio. Sono veloci, flessibili e trasparenti. Le regole di filtraggio non sono facilmente gestibili su di un router, ma sono disponibili strumenti che semplificano le attività di creazione e gestione delle regole.
I gateway per il filtro sono soggetti a rischi, tra cui:

- Le porte e gli indirizzi di origine e destinazione contenuti nell'intestazione del pacchetto IP sono le uniche informazioni in base alle quali il router deve decidere se consentire o meno l'accesso del traffico a una rete interna.
- Non proteggono dallo spoofing degli indirizzi IP o DNS.
- Un aggressore avrà accesso diretto a qualsiasi host della rete interna una volta che l'accesso è stato concesso dal firewall.
- Con alcuni gateway per il filtro dei pacchetti non è disponibile un'autenticazione utente avanzata.
- Forniscono registrazioni ridotte o di scarsa utilità.

20.14 Strumenti per rilevare le intrusioni

Il rilevamento delle intrusioni è il processo che consiste nell'individuare l'utilizzo non autorizzato o l'attacco a un computer o una rete. I sistemi per il rilevamento delle intrusioni (IDS, Intrusion Detection System) sono sistemi software o hardware che scoprono questi utilizzi non autorizzati. Gli IDS possono rilevare i tentativi di compromettere la riservatezza, l'integrità e la disponibilità di un computer o di una rete. Gli attacchi vengono condotti da aggressori su Internet, da utenti interni autorizzati che fanno un cattivo uso dei privilegi assegnati e da personale interno non autorizzato che tenta di ottenere privilegi non consentiti.

La capacità di rilevare le intrusioni sta rapidamente diventando indispensabile per le infrastrutture di protezione di tutte le organizzazioni di grandi dimensioni. Il dubbio per i responsabili della protezione non deve riguardare l'uso o meno di sistemi del rilevamento delle intrusioni, ma la scelta delle funzionalità e delle caratteristiche appropriate. Tuttavia, si può dover ancora giustificare l'acquisto di un IDS. Ci sono almeno tre buone ragioni per acquistare un IDS: rilevare attacchi e altre violazioni della protezione che non possono essere evitate, impedire agli aggressori di esaminare una rete e documentare la minaccia di intrusione a un'organizzazione.

Sono attualmente disponibili molti tipi di IDS, caratterizzati da approcci di analisi e monitoraggio differenti. Ciascuno ha utilizzi, vantaggi e svantaggi distinti. Gli IDS possono monitorare gli eventi a tre livelli differenti: rete, host e applicazione. Questi eventi possono essere analizzati mediante due tecniche: il rilevamento della firma e il rilevamento delle anomalie. Alcuni IDS hanno anche la possibilità di rispondere automaticamente agli attacchi rilevati.

20.15 Antivirus

Gli antivirus eseguono tre funzioni di base. Consentono di rilevare, identificare e rimuovere i virus. Gli strumenti di rilevamento effettuano un rilevamento proattivo, attivo o reattivo. I virus vengono rilevati prima, durante o dopo l'esecuzione. Il funzionamento degli strumenti di identificazione e rimozione è più semplice. Nessuno dei due viene utilizzato prima del rilevamento di un virus.
Gli strumenti di rilevamento consentono di scoprire la presenza di un virus nel sistema. Il rilevamento viene effettuato in vari punti del sistema. Il virus può essere in esecuzione, risiedere in memoria o essere memorizzato nel codice eseguibile. Può essere rilevato prima, durante o dopo l'esecuzione e la replica. Sono disponibili tre categorie di strumenti di rilevamento e analisi:

- *Rilevamento statico.* Gli strumenti di rilevamento e analisi statici esaminano i file eseguibili senza eseguirli. Consentono di rilevare la presenza di un virus nel codice prima che si introduca nel sistema.
- *Rilevamento tramite intercettazione.* Per propagarsi, un virus deve passare ad altre applicazioni host. Alcuni strumenti di rilevamento hanno lo scopo di intercettare i tentativi di effettuare tale attività. Questi strumenti interrompono l'esecuzione dei programmi contenenti virus e i tentativi dei virus di replicarsi o diventare residenti.
- *Rilevamento di modifica.* Tutti i virus causano la modifica di eseguibili durante il relativo processo di replica. Di conseguenza, la presenza di virus può essere rilevata anche cercando modifiche impreviste degli eseguibili. Questo processo viene chiamato a volte controllo di integrità. Si noti che questo tipo di rilevamento funziona solo dopo che nel sistema sono presenti eseguibili contenenti virus e il virus si è replicato.

Gli strumenti di identificazione consentono di riconoscere il virus che si è introdotto in un determinato eseguibile. Ciò consente all'utente di ottenere informazioni aggiuntive sul virus. Si tratta di uno strumento utile in quanto può fornire indicazioni sui tipi di danno che il virus può causare e sulle procedure di pulitura appropriate.

Gli strumenti di rimozione tentano di ripristinare lo stato pulito del sistema in modo efficiente rimuovendo il codice del virus dall'eseguibile interessato. In molti casi, una volta individuato un virus, esso viene trovato su molti sistemi o in molti eseguibili di un singolo sistema. Il processo di ripristino dai dischetti originali o da copie di backup pulite può essere tedioso.
Sono molti i fornitori di terze parti che sviluppano gli strumenti citati in precedenza e rilasciano aggiornamenti sui virus. Scegliere il tipo appropriato di strumento in base alle necessità dell'azienda di rilevare e rimuovere i virus.

20.16 Controllo

Una volta stabiliti i meccanismi di protezione del sistema, sarà necessario monitorarli. Assicurarsi che funzionino effettivamente e notare qualsiasi indizio di malfunzionamento o di altri problemi. Il processo di monitoraggio del funzionamento del sistema è chiamato controllo.
Diversi sistemi operativi gestiscono alcuni file di registro che tengono traccia di ciò che si verifica sul computer. I file di registro sono un componente elementare importante di un sistema di protezione. Formano una cronologia registrata, o itinerario di controllo, degli eventi verificatisi sul computer, agevolando la scoperta di attacchi o problemi intermittenti. Mediante i file di registro è possibile raccogliere informazioni sufficienti per scoprire la causa di un bug, l'origine di una violazione e l'ambito del danno subito. Nei casi in cui non è possibile impedire il verificarsi di un danno, sarà almeno possibile registrarlo. Questi registri possono costituire esattamente ciò che serve per generare il sistema, condurre un'indagine, fornire una prova, farsi rimborsare dall'assicurazione o fare in modo che venga effettuato un accurato servizio sul campo.
I file di registro hanno anche una vulnerabilità fondamentale. Poiché vengono spesso salvati sul sistema, sono soggetti ad alterazione o eliminazione.

20.17 Eventi da controllare

È necessario scegliere gli eventi da controllare con molta attenzione. Il controllo potrebbe infatti causare un peggioramento delle prestazioni. Se su un sistema vengono controllati tutti gli eventi, le prestazioni del sistema peggioreranno notevolmente. Gli eventi da controllare devono quindi essere scelti con cura, in funzione di che cosa si desidera controllare. I sistemi operativi controllano molti eventi:

- Informazioni relative all'accesso e alla disconnessione
- Informazioni relative all'arresto e al riavvio del sistema
- Accesso ai file e alle cartelle
- Modifiche delle password
- Accesso agli oggetti
- Modifiche dei criteri di protezione

La maggior parte dei registri di controllo è in grado di memorizzare una cronologia o backlog di eventi. È possibile impostare i file di registro in vari modi, alcuni dei quali sono descritti di seguito:

- Impostazione di una determinata dimensione per il file di registro e sovrascrittura degli eventi quando il registro è pieno. Viene applicata la modalità FIFO (First In First Out).
- Impostazione del file di registro in modo che si riempia per un determinato numero di giorni.
- Impostazione di una determinata dimensione per il file di registro. Quando il file di registro è pieno, è necessario svuotarlo manualmente.

Conclusioni

“Fondamentalmente, la sicurezza informatica consiste di una serie di soluzioni tecniche a problemi non tecnici”. Il senso di questa fulminante definizione di Simson e Garfinkel va ricercato nel fatto che, come già detto in precedenza, la sicurezza informatica di un qualsiasi sistema non è un obiettivo realisticamente e totalmente raggiungibile, perché dipende da un insieme di fattori che non sono controllabili :

Hacker molto abili, dipendenti poco attenti o infedeli, calamità naturali, bug nel software. In definitiva, un’organizzazione che voglia affrontare il problema non deve inseguire l’utopistico obiettivo del raggiungimento della sicurezza totale e definitiva, ma deve decidere essenzialmente quanto è disposta a spendere, e come spenderlo, per realizzare un corretto piano di sicurezza aziendale.

Bibliografia

[1] S. Garfinkel, G. Spafford, Practical Unix and Internet Security, Sebastopol CA(Usa), O'Reilly, 1996

[2] V.Ahuja, Sicurezza in Internet e sulle reti, Milano, McGraw-Hill

[3] L. Klander, Hacker Proof- Sicurezza in rete, McGraw-Hill

[4] A.S. Tanenbaum, Reti di Computer, Jackson

[5] M. Terranova, Firma Digitale: tecnologie e standard, Aipa, Roma

[6] C. Paris, Crittografia, una necessità, Beta Online.

[7] J. Mc Donald, Biometric Authentication, Otago University, Dunedin, New Zealand