**Esercitazione Information Security**

Il modello sviluppato dovrà fare riferimento a quanto previsto dallo standard ISO/IEC 27001 e prevedere quanto segue:

1. Dovrà essere identificata un’azienda di riferimento (sia essa reale o di fantasia) determinandone il contesto interno ed esterno che può influenzare la sicurezza delle informazioni (cfr slide pag 72) OK
2. Dovranno essere identificati le informazioni che possono essere critiche per la realtà aziendale identificata al punto precedente.
3. Dovrà essere condotta un’analisi del rischio relativa alle informazioni aziendali identificate determinando le scale di valutazione degli impatti e delle probabilità (cfr slide pag 76,77) e un elenco di minacce applicabili al contesto identificato
4. Dovranno essere determinati quali controlli relativi all’annex A l’organizzazione tiene in considerazione per proteggere le informazioni (cfr slide pag 85- 105)
5. Dovrà essere sviluppato un piano di trattamento del rischio atto a mitigare alcuni rischi identificati all’interno della realtà aziendale prescelta

*Il progetto dovrà essere sviluppato da gruppi formati da un massimo di 4 persone*

*a)*

*WebSoft: azienda informatica per lo sviluppo e assistenza di applicazioni web-based con offerta di servizi di data center e web hosting.*

Contesto interno:

* server dedicati per i servizi di hosting e data center
* dipendenti dell’azienda e loro relative conoscenze
* computer *per lo sviluppo software*

*Dipendenti:*

* *1 Project Manager (anche programmatore)*
* *1 impiegato amministrativo*
* *4 programmatori*

Contesto esterno:

* *Clienti*
* *Fornitori*

*b)*

*- Dati dei clienti*

*- Codice sorgente da salvaguardare*

*- Server di hosting da proteggere*

*- Errori di programmazione lato sicurezza*

*- Possibile infezione malware dei computer dei dipendenti*

*c)*

*Minacce:*

* *Esfiltrazione/manomissione dei dati dei clienti*
* *Esfiltrazione/manomissione del codice sorgente*
* *Manomissione dei computer dei dipendenti*
* *Attacchi hacker verso i server aziendali (non intromissione)*
* *Intromissione di un terzo all’interno di un dispositivo utilizzato in azienda o per telelavoro*
* *Spionaggio industriale (assunzione personale con intenzioni fraudolente)*
* *Scarsa formazione del personale*
* *Intrusione da parte di terzi all’interno di un’area ad accesso privilegiato*
* *Furto di identità da parte di terzi (compromissione di chiavi crittografiche relative a uno o più domini di hosting)*
* *Accesso non autorizzato ad un’area protetta non esposta alla rete Internet*
* *Furto o manipolazione di dati sensibili o informazioni presenti su dispositivi dismessi o riutilizzati*
* *Accesso non autorizzato* a dispositivi lasciati incustoditi degli utenti
* *Perdita o corruzione di dati causata da software non aggiornato*
* *Perdita dei dati dei clienti/dei codici sorgenti per mancato backup preventivo*
* Infezione da malware
* *Navigazione su siti malevoli*

Criterio di valutazione della probabilità

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | *Molto Raro* | *Raro* | *Improbabile* | *Possibile* | *Frequente* | *Quasi certo* |
| *Livello* | *1* | *2* | *3* | *4* | *5* | *6* |
| *Probabilità* | *Ogni 10 anni* | *Ogni 5 anni* | *Ogni 2 anni* | *Ogni 6 mesi* | *Ogni mese* | *Ogni settimana* |

*Probabilità*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| *Molto-Raro* | *Raro* | *Improbabile* | *Possibile* | *Frequente* | *Quasi certo* |

Criterio di valutazione degli impatti

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | *Molto Basso* | *Basso* | *Medio* | *Alto* | *Molto Alto* |
| *Livello* | *1* | *2* | *3* | *4* | *5* |
| *Impatto* | *Fino a 5k euro* | *Tra 5k a 20k euro* | *Tra 20k a 35k euro* | *Tra 35k e 50k euro* | *Più di 50k euro* |

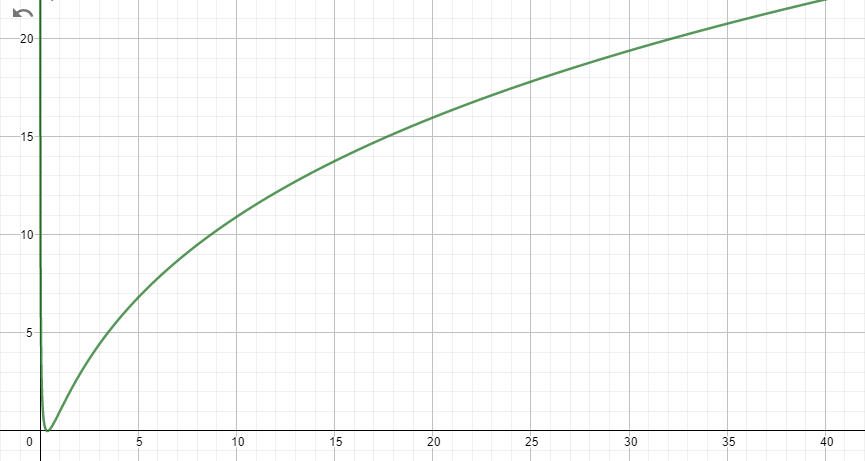
*Impatto*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Molto-Basso* | *Basso* | *Medio* | *Alto* | *Molto-Alto* |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | *Molto Raro* | *Raro* | *Improbabile* | *Possibile* | *Frequente* | *Quasi certo* |
| *Molto Alto* | *7* | *11* | *14* | *16* | *18* | *20* |
| *Alto* | *6* | *9* | *12* | *14* | *16* | *17* |
| *Medio* | *4* | *8* | *10* | *12* | *14* | *15* |
| *Basso* | *3* | *6* | *8* | *9* | *11* | *12* |
| *Molto Basso* | *1* | *3* | *4* | *6* | *7* | *9* |

*Rischio Residuo*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Basso* | *Medio-Basso* | *Moderato* | *Medio-Alto* | *Alto* |

**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | ***Probabilità*** | ***Impatto*** | ***Rischio Residuo*** | ***Da trattare*** |
| *Esfiltrazione/manomissione*  *dei dati dei clienti* | *Possibile* | *Molto-Alto* | *Alto* | *X* |
| *Esfiltrazione/manomissione del codice sorgente* | *Possibile* | *Alto* | *Medio-Alto* | *X* |
| *Manomissione dei computer dei dipendenti* | *Improbabile* | *Molto-Alto* | *Medio-Alto* | *X* |
| *Attacchi hacker verso i server aziendali (non intromissione)* | *Possibile* | *Alto* | *Media-Alto* | *X* |
| *Intromissione di un terzo all’interno di un dispositivo utilizzato in azienda o per telelavoro* | *Raro* | *Molto-Alto* | *Medio-Alto* | *X* |
| *Spionaggio industriale (assunzione personale con intenzioni fraudolente)* | *Molto-Raro* | *Alto* | *Medio-Basso* |  |
| *Scarsa formazione del personale* | *Improbabile* | *Alto* | *Medio-Alto* | *X* |
| *Intrusione da parte di terzi all’interno di un’area ad accesso privilegiato* | *Raro* | *Molto-Alto* | *Medio-Alto* | *X* |
| *Furto di identità da parte di terzi (compromissione di chiavi crittografiche relative a uno o più domini di hosting)* | *Molto-Raro* | *Molto-Alto* | *Moderato* |  |
| *Accesso non autorizzato ad un’area protetta non esposta alla rete Internet* | *Improbabile* | *Molto-Alto* | *Medio-Alto* | *X* |
| *Furto o manipolazione di dati sensibili o informazioni presenti su dispositivi dismessi o riutilizzati* | *Improbabile* | *Alto* | *Medio-Alto* | *X* |
| *Accesso non autorizzato* a dispositivi lasciati incustoditi dagli utenti | *Frequente* | *Alto* | *Alto* | *X* |
| *Perdita o corruzione di dati causata da software non aggiornato* | *Molto-Raro* | *Medio* | *Basso* |  |
| *Perdita dei dati dei clienti/dei codici sorgenti per mancato backup preventivo* | *Raro* | *Molto-Alto* | *Medio-Alto* | *X* |
| *Infezione da malware* | *Possibile* | *Molto-Alto* | *Alto* | *X* |
| *Navigazione su siti malevoli o in generale non consentiti* | *Quasi certo* | *Alto* | *Alto* | *X* |

*Verranno trattati tutti i rischi il cui rischio residuo è >= 11)*

*d)*

* A.5.1.1 Politiche per la sicurezza delle informazioni

L’azienda sarà dotata di un sistema di gestione per la sicurezza delle informazioni attraverso la valutazione dei possibili fattori di rischio.

* A.6.1.4 Contatti con gruppi specialistici

L’azienda farà riferimento a specialisti nel settore per la gestione della sicurezza delle informazioni per la compilazione di un piano relativa a quest’ultima.

* A.6.1.5 Sicurezza delle informazioni nella gestione dei progetti

I progetti aziendali (così come i dati dei clienti) saranno protetti da una o più autenticazioni.

* A.6.2.1 Politica per i dispositivi portatili

I dispositivi portatili (così come quelli in sede) saranno protetti da una o più autenticazioni e da software integrato.

* A.6.2.2 Telelavoro

Il telelavoro sarà organizzato attraverso l’accesso e l’utilizzo di dispositivi sicuro.

* A.7.2.2 Consapevolezza, istruzione, formazione e addestramento sulla sicurezza delle informazioni

Il personale sarà scelto con accuratezza e nel caso istruito riguardo la sicurezza delle informazioni.

* A.9.2.1 Registrazione e de-registrazione degli utenti

Gli utenti saranno memorizzati in modo sicuro nel sistema con i rispettivi privilegi d’accesso e credenziali.

* A.9.2.3 Gestione dei diritti di accesso privilegiato

L’azienda suddividerà accuratamente i privilegi d’accesso fra i suoi dipendenti.

* A.9.2.4 Gestione delle informazioni segrete di autenticazione degli utenti

Le credenziali d’accesso al sistema dei clienti e dei dipendenti saranno mantenute segrete.

* A.9.2.6 Rimozione o adattamento dei diritti di accesso

Una volta che varia un ruolo di un qualche cliente/dipendente, si rivaluteranno i rispettivi diritti d’acceso.

* A.9.1.1 Politica di controllo accessi

L’azienda effettuerà un accurato controllo degli accessi (attraverso un log) per determinare gli accessi consentiti e verso quali aree.

* A.9.1.2 Accesso alle reti e ai servizi di rete

Ogni dispositivo aziendale e non sarà dotato di software per il controllo dell’accesso alle reti e ai servizi di rete.

* A.9.4.1 Limitazione dell’accesso alle informazioni

L’azienda limiterà l’accesso alle informazioni (progetti/dati dei clienti) attraverso un sistema di autenticazione e verifica delle credenziali.

* A.9.4.5 Controllo degli accessi al codice sorgente dei programmi

Il codice sorgente dei programmi dovrà essere accedibile solo dagli sviluppatori o da coloro che hanno accesso.

* A.11.2.7 Dismissione sicura o riutilizzo delle apparecchiature

Una volta deciso l’abbandono di un dispositivo, quest’ultimo dovrà essere ripulito e, nel caso di dismissione completa, distrutto adeguatamente.

* A.11.2.8 Apparecchiature incustodite degli utenti

L’azienda adotterà delle tecniche atte a mitigare il furto di informazioni tratte da dispositivi lasciati incustoditi.

* A.12.2.1 Controlli contro il malware

Ciascun dispositivo aziendale sarà munito di software anti-malware aggiornato.

* A.12.3.1 Backup delle informazioni

Periodicamente verrà effettuato il backup dei dati dei clienti e dei codici sorgenti. Tale backup verrà mantenuto segreto.

* A.12.5.1 Installazione del software sui sistemi di produzione

Su ciascun dispositivo in sede e non, verrà installato e configurato tutto il software necessario per portare avanti la produzione.

* A.12.6.2 Limitazioni all’installazione del software

Su ciascun dispositivo in sede e non, verrà installato del software di controllo che limita, a sua volta, l’installazione di contenuti non consentiti.

* A.13.1.2 Sicurezza dei servizi di rete

L’azienda installerà un proprio firewall di rete per mitigare gli attacchi verso i server esposti alla rete Internet (Web Server e Server di hosting).

* A.13.2.1 Politiche e procedure per il trasferimento delle informazioni

Ciascun trasferimento di codice, o più in generale di informazioni, dovrà essere sicuro, facendo attenzione a non perdere o danneggiare alcun tipo di dato.

*e) Azioni che mitigano le minacce identificate:*

* ***Esfiltrazione/manomissione dei dati dei clienti****: Proteggere i dati dei clienti attraverso un sistema di autenticazione a due fattori (autenticazione basata su un segreto conosciuto dal personale amministrativo (es. password) e autenticazione fisica basata su un oggetto posseduto (es. token di autenticazione)). Limitazione di accesso a tali dati, esclusivamente ad un ristretto gruppo di persone.*
* ***Esfiltrazione/manomissione del codice sorgente****: Proteggere il codice sorgente attraverso un sistema di autenticazione basata su password (non si utilizza un’autenticazione a due fattori per velocizzare tale processo).*
* ***Manomissione dei computer dei dipendenti****: i computer dei dipendenti dovranno essere dotati di software che limitano l’accesso a risorse del sistema e che limitano l’installazione di applicativi non consentiti. I software di controllo non potranno essere rimossi dai dispositivi se non dal personale autorizzato.*
* ***Attacchi hacker verso i server aziendali (non intromissione):*** *i computer dei dipendenti dovranno essere protetti da firewall o packet filter e dovranno essere analizzate le possibili vulnerabilità causate da servizi che si interfacciano alla rete Internet.*
* ***Intromissione di un terzo all’interno di un dispositivo utilizzato in azienda o per telelavoro:*** *Proteggere l’accesso ai dispositivi in sede con un’autenticazione basata su password e proteggere l’accesso ai dispositivi da remoto attraverso riconoscimento IP e autenticazione basata su password.*
* ***Scarsa formazione del personale****: Verificare le competenze pregresse del dipendente ed istruirlo riguardo l’utilizzo e l’accesso ai dispositivi aziendali in sede e da remoto.*
* ***Intrusione da parte di terzi all’interno di un’area ad accesso privilegiato****: Circoscrivere le aree ad accesso privilegiato attraverso un sistema di autenticazione a due fattori (sempre basate su password e autenticazione fisica basata su token). Limitare il possedimento di tali credenziali ad un numero ristretto di persone, mitigando quindi la divulgazione di tali credenziali d’accesso a terzi.*
* ***Furto o manipolazione di dati sensibili o informazioni presenti su dispositivi dismessi o riutilizzati****: Ripulire sempre i dispositivi prima del loro riutilizzo o dismissione attraverso software di formattazione del disco rigido. Se tali dispositivi devono, per qualche motivo, essere dismessi, adottare tecniche specializzate di distruzione come ad esempio la punzonatura.*
* ***Accesso non autorizzato* a dispositivi lasciati incustoditi degli utenti**: Adottare o incrementare il controllo sui dispositivi lasciati incustoditi in sede. Esortare il personale a non lasciare incustodito il loro dispositivo durante il lavoro da remoto. Utilizzare delle tecniche di cifrature del disco quando il dispositivo non è in uso.
* ***Perdita dei dati dei clienti/dei codici sorgenti per mancato backup preventivo****: Effettuare periodicamente uno o più backup dei dati dei clienti/dei codici sorgenti. Proteggere fisicamente tali backup e cifrarne il contenuto per scongiurare copie non consentite.*
* ***Infezione da malware****: Installare sui dispositivi in sede o da remoto del software anti-malware aggiornato. Istruire il personale riguardo le possibili infezioni causate da software malevolo e sui possibili accorgimenti da adottare per evitare tali infezioni.*
* ***Navigazione su siti malevoli o in generale non consentiti****: Configurare i dispositivi in sede o da remoto in modo tale da evitare che il personale acceda a domini non consentiti (ad esempio utilizzando un proxy server che filtra le richieste HTTP). Tale configurazione non potrà essere modificata se non dal personale autorizzato.*

**PIANO TRATTAMENTO DEL RISCHIO**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Rischio** | **Danni all’azienda** | **Rischio residuo** | **Situazione attuale** | **Strategia di mitigazione** |
| Esfiltrazione/manomissione dei dati dei clienti | Furto e perdita di informazioni, cause legali da parte dei clienti (nel caso di perdita tali dati) | Alto | Dati dei clienti presenti in un file excel di un dispositivo collegato alla rete Internet | Spostare i dati dei clienti in una directory (es. LDAP) in un dispositivo non collegato alla rete Internet ed accedibile solo attraverso un’autenticazione a due fattori (password + token).  Limitazione di accesso a tali dati, esclusivamente ad un ristretto gruppo di persone |
| Esfiltrazione/manomissione del codice sorgente | Furto di codice sorgente, calo della produttività causata dal tempo di recupero del lavoro perso | *Medio-Alto* | Codici sorgenti memorizzati sui vari dispositivi aziendali | Predisporre un sistema di versioning del software (es. GIT) per poter centralizzare, sincronizzare e proteggere i vari codici sorgenti |
| Manomissione dei computer dei dipendenti | Furto e perdita di informazioni, cause legali da parte dei clienti (nel caso di perdita di tali dati), calo della produttività causata dal tempo di recupero del lavoro perso | *Medio-Alto* | Ciascun dipendente può modificare i file di sistema del proprio dispositivo aziendale | I computer dei dipendenti dovranno essere dotati di software che limitano l’accesso a risorse del sistema e l’installazione di applicativi non consentiti. Tali software di controllo non potranno essere rimossi dai dispositivi se non da personale autorizzato |
| Attacchi hacker verso i server aziendali (non intromissione) | Perdita di informazioni, disservizio nei confronti dei clienti, calo della produttività causata dal tempo di recupero del lavoro perso | *Media-Alto* | Rete locale non protetta da firewall o packet filter. Porte aperte verso alcuni dispositivi “critici”. | Installare un firewall sul gateway che si interfaccia alla rete Internet ed eventualmente anche nei dispositivi aziendali.  Chiudere determinate porte inutilizzate aperte del gateway per escludere eventuali vulnerabilità |
| Intromissione di un terzo all’interno di un dispositivo utilizzato in azienda o per telelavoro | Furto e perdita di informazioni, cause legali da parte dei clienti (nel caso di perdita di tali dati) | *Medio-Alto* | Dispositivi aziendali e non protetti da password deboli | Comunicare al personale la “debolezza” della password attuale incoraggiandolo ad utilizzarne una più sicura dal punto di vista della sicurezza.  Proteggere l’accesso ai dispositivi da remoto attraverso riconoscimento IP e autenticazione basata su password. |
| Scarsa formazione del personale | Perdita parziale dei dati relativi ai codici sorgenti (ad esempio per mancato salvataggio), autorizzazione inconsapevole di programmi malevoli all’interno del dispositivo | Medio-Alto | Personale scelto in solamente base in base alle competenze pregresse. | Verificare accuratamente le competenze pregresse del dipendente ed istruirlo riguardo l’utilizzo e l’accesso ai dispositivi aziendali in sede e da remoto |
| Intrusione da parte di terzi all’interno di un’area ad accesso privilegiato | Furto e perdita di informazioni, cause legali da parte dei clienti (nel caso di perdita di tali dati) | Medio-Alto | Dispositivi appartenenti ad un’area ad accesso privilegiato (contenenti informazioni sensibili, quali ad esempio i dati dei clienti) protetti solamente da autenticazione basata su password | Circoscrivere le aree ad accesso privilegiato attraverso un sistema di autenticazione a due fattori (sempre basate su password e autenticazione fisica basata su token). Limitare il possedimento di tali credenziali ad un numero ristretto di persone, mitigando quindi la divulgazione di tali credenziali d’accesso a terzi |
| Furto o manipolazione di dati sensibili o informazioni presenti su dispositivi dismessi o riutilizzati | Diffusione delle credenziali e dei dati d’accesso e dei codici sorgenti dei progetti | Medio-Alto | Dismissione superficiale dei dispositivi aziendali.  Parziale cancellazione delle informazioni contenute in essi | Ripulire sempre i dispositivi prima del loro riutilizzo o dismissione attraverso software di formattazione del disco rigido. Se tali dispositivi devono, per qualche motivo, essere dismessi, adottare tecniche specializzate di distruzione come ad esempio la punzonatura |
| Accesso non autorizzato a dispositivi lasciati incustoditi dagli utenti | Furto e perdita di informazioni, cause legali da parte dei clienti (nel caso di perdita di tali dati) | Alto | Dispositivi lasciati completamente incustoditi durante il periodo nel quale il proprietario è assente | Adottare o incrementare il controllo sui dispositivi lasciati incustoditi in sede. Esortare il personale a non lasciare incustodito il loro dispositivo durante il lavoro da remoto. Utilizzare delle tecniche di cifrature del disco quando il dispositivo non è in uso |
| Perdita dei dati dei clienti/dei codici sorgenti per mancato backup preventivo | Cause legali da parte dei clienti, calo della produttività causata dal tempo di recupero del lavoro perso | Medio-Alto | Backup effettuati in intervalli di tempo eccessivamente lunghi. Supporti di backup facilmente accedibili e leggebili. | Effettuare periodicamente uno o più backup dei dati dei clienti/dei codici sorgenti. Proteggere fisicamente tali backup e cifrarne il contenuto per scongiurare copie non consentite |
| Infezione da malware | Furto e perdita di informazioni, cause legali da parte dei clienti (nel caso di perdita di tali dati), proporzionale calo della produttività causata dal tempo di ripristino del dispositivo | Alto | Dispositivi dotati di software anti-malware obsoleto o mancante. Personale poco istruito riguardo i possibili danni causati da software potenzialmente malevolo | Installare sui dispositivi in sede o da remoto del software anti-malware aggiornato. Istruire il personale riguardo le possibili infezioni causate da software malevolo e sui possibili accorgimenti da adottare per evitare tali infezioni |
| Navigazione su siti malevoli o in generale non consentiti | Calo della produttività del dipendente, problemi legali in generale, installazione di software non consentito | Alto | Ciascun dipendente può navigare in Internet senza limitazioni di alcun tipo | Configurare i dispositivi in sede o da remoto in modo tale da evitare che il personale acceda a domini non consentiti (ad esempio utilizzando un proxy server che filtri le richieste HTTP). Tale configurazione non potrà essere modificata se non da personale autorizzato |