talleri law

CYBERSECURITY GOVERNANCE

La visione aziendale in materia di Cybersecurity Governance attuata attraverso l'elemento centrale di ogni azienda; **il fattore umano**. Opportunità di intervento mediante regolamenti e contratti.

SOMMARIO

PERCHÉ È NECESSARIA?

OBBLIGHI LEGALI E RISCHI

Obblighi (e rischi) legali previsti ad esempio da:

- Legge federale sulla protezione dei dati, LPD, RS 235.1;
- Legge sul diritto d'autore, LDA, RS 231.1;
- Legge federale di complemento del Codice civile svizzero, CO, RS 220;
- Regolamento europeo in materia di protezione dei dati personali, GDPR, Reg.Ue 2016/679.

Rischi aziendali (danni d'immagine, valore ecc);

CONOSCERE L'AZIENDA

PREMESSA INDISPENSABILE PER ATTUARE LE MISURE NECESSARIE

Fra i vari metodi sviluppati per gestire e ridurre il rischio cyber, il National Institute for Standards and Technology (NIST) ha sviluppato un «Framework for Improving Critical Infrastructure Cybersecurity», che si basa su un insieme di categorie raggruppate secondo 5 *funzioni*:

1. IDENTIFY
2. PROTECT
3. DETECT
4. RESPOND
5. RECOVER

Partendo proprio dalla prima funzione, ovvero identify, si propone un metodo di analisi dei processi delle attività aziendali, i rischi connessi, l'asset e via dicendo.

«IDENTIFY»

IN PARTICOLAR MODO IN RELAZIONE ALL'ORGANIZZAZIONE

1. Conoscere la struttura, l'asset e l'attività dell'azienda;
2. Conoscere le normative applicabili all'attività aziendale e all'azienda;
3. Identificare i potenziali rischi, in particolare quelli inerenti l'IT e le attività critiche.

STRUTTURA

AZIENDALE

Nell'azienda:

1. sono note eventuali disposizioni legali e/o contrattuali applicabili in materia di trattamento dei dati?
2. sono rispettate?
3. l'accesso fisico all'infrastruttura IT è adeguamente protetto?
4. viene utilizzata la crittografia?
5. ci sono dei regolamenti specifici in ambito IT?
6. c'è un/a responsabile per la sicurezza IT? sono definite le responsabilità interne ed esterne?
7. esiste un regolamento specifico per il responsabile IT?
8. quali tipi di connessione esistono all'infrastruttura (eth, wlan, vpn, ecc.)?
9. è nota e mappata l'infrastruttura IT e inerente le telecomunicazioni aziendali e le relative risorse?
10. sono previste delle priorità a livello di attività, organizzazione e comunicazione?
11. sono noti le minacce e i rischi? e gli eventuali impatti?
12. esistono dei piani di intervento?

STRUTTURA

COLLABORATORI

I collaboratori dell'azienda:

1. conoscono e utilizzano in maniera adeguata l'infrastruttura?
2. accedono a tutti i dati dell'azienda indistintamente dalla loro funzione?
3. utilizzano dispositivi mobili?
4. accedono da remoto a sistemi IT dell'azienda?
5. sono operativi anche dall'estero? da quali Paesi?
6. sono debitamente formati per quanto attiene l'uso dell'IT?
7. vengono sensibilizzati regolarmente?
8. sanno come reagire in caso di una compromissione del sistema IT?
9. sanno come comportarsi nei confronti dei clienti, fornitori e terzi in relazione a eventuali obblighi in materia di protezione dei dati?

STRUTTURA

PARTNERS

I partners dell'azienda:

1. conoscono eventuali disposizioni legali e/o contrattuali applicabili in materia di trattamento dei dati?
2. le rispettano?
3. utilizzano dispositivi mobili?
4. accedono da remoto a sistemi IT dell'azienda?
5. anche dall'estero? da quali Paesi?
6. hanno un/a responsabile interno in ambito di sicurezza IT? dispongono dei suoi recapiti?
7. si sono vincolati a supportare l'azienda in relazione a eventuali suoi obblighi nei confronti di clienti, fornitori o autorità?
8. eseguono verifiche regolari di conformità?
9. sanno come reagire in caso di una compromissione dei loro sistemi IT?

STRUMENTI ORGANIZZATIVI

REGOLAMENTO AZIENDALE

Attraverso il regolamento aziendale è possibile definire, secondo le specifiche esigenze aziendali, le regole e i processi da adottare per limitare i rischi di un utilizzo dell'infrastruttura non conforme.

Ritengo che l'elaborazione di un regolamento aziendale in ambito di sicurezza IT competa in prima battuta, soprattutto nell'ambito delle PMI, al Management. Conoscere l'azienda è infatti presupposto indispensabile per definire le strategie necessarie per proteggerla contro i CYBER RISCHI. Si reputa altresì fondamentale l'aspetto formativo e culturale. L'essere umano è infatti – ancora oggi – l'elemento spesso più vulnerabile di ogni sistema di sicurezza cyber.

Un'adeguata istruzione, una pratica regolare e l'adozione di una corretta cultura CYBER sono e resteranno elementi cruciali per rendere efficace le altre misure di sicurezza.

REGOLAMENTO AZIENDALE

In base alle funzioni previste dal Framework del NIST, è possibile adottare, mediante dei regolamenti interni o mediante dei contratti, le misure che - caso per caso - saranno da ritenere opportune per tutelare («PROTECT») l'azienda.

Seguendo le funzioni previste dal Framework NIST, si adottano quindi le misure atte a proteggere l'azienda:

1. IDENTIFY
2. PROTECT
3. DETECT
4. RESPOND
5. RECOVER

Si tenga conto che la CYBERSECURITY richiede un approccio dinamico, che impone all'azienda di adattare continuamente i propri sistemi di protezione alle minacce e ai rischi. In questo senso anche i contratti e i regolamenti non possono essere considerati statici.

«PROTECT»

ELEMENTI DEL REGOLAMENTO

1. Premesse
2. Campi d'applicazione del Regolamento
3. Obbligo di formazione e sensibilizzazione
4. Obbligo di notifica e conoscenza procedure
5. Utilizzo sistemi informatici
    - Norme generali e crittografia
    - Credenziali e diritti d'accesso ("need-to-know")
    - Posta elettronica e sistemi di Messaging
    - Accesso remoto (ad esempio VPN)
    - Wireless LAN
    - Dispositivi mobili
    - Scanner, stampanti, fax e centralini telefonici
6. Accesso ai locali server

«PROTECT»

ELEMENTI DEL REGOLAMENTO

7. Categorie dei dati e rischi
8. Trattamento dei dati - supporti digitali e analogici
    - Archiviazione
    - Trasmissione
    - Sicurezza
    - Distruzione
    - Trasmissione a terzi dei dati
9. Disposizioni finali

«PROTECT»

CONTRATTUALISTICA

La singola azienda non può considerare adempiuti i propri obblighi in materia di sicurezza IT senza tenere conto dei propri partner.

Il GDPR, ad esempio, impone (cfr. Articolo 28 cpv. 3 GDPR) che fra il Titolare del trattamento e il Responsabile vi sia un «contratto o altro atto giuridico» che deve prevedere degli obblighi delle Parti in relazione al trattamento dei dati personali.

«PROTECT»

ALCUNI ELEMENTI DEL CONTRATTO EX ART 28 GDPR

1. *su istruzione documentata del titolare del trattamento (...)*
2. *garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;*
3. *adotti tutte le misure (...)*
4. *assista il titolare del trattamento con misure tecniche e organizzative adeguate, (...)*
5. *assista il titolare del trattamento nel garantire il rispetto degli obblighi (...)*
6. *su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi (...)*
7. *metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo (...)*

«PROTECT»

ELEMENTI GENERALI DEL CONTRATTO CON I PARTNERS AZIENDALI

1. campo di applicazione
2. definizione scopo e durata
3. obblighi in relazione al trattamento
4. obblighi in relazione alle misure tecniche organizzative
5. assistenza fra le parti
6. modalità di comunicazione e persone responsabili
7. obblighi al momento della fine del contratto
8. disposizioni in caso di fallimento di una parte
9. disposizioni in merito ai diritti di verifica del rispetto degli obblighi delle parti
10. clausola di salvaguardia
11. eventuale penale in caso di violazione del contratto
12. eventuali impegni di riservatezza
13. diritto applicabile
14. foro

CONCLUSIONI

1. conoscere l'azienda per poterla difendere;
2. da sole misure tecniche e organizzative non sono efficaci senza la consapevolezza delle persone che se ne avvalgono;
3. prevedere una sensibilizzazione e un aggiornamento costante di tutti i collaboratori, a prescindere dal ruolo e dalla funzione;
4. i partners commerciali devono garantire un adeguato livello di organizzazione, eventuali obblighi contrattuali devono anche essere fattivamente messi in pratica; prevedere sistemi di verifica e/o certificazione;
5. restare aggiornati, seguire gli sviluppi e conoscere le nuove minacce.

Domande?

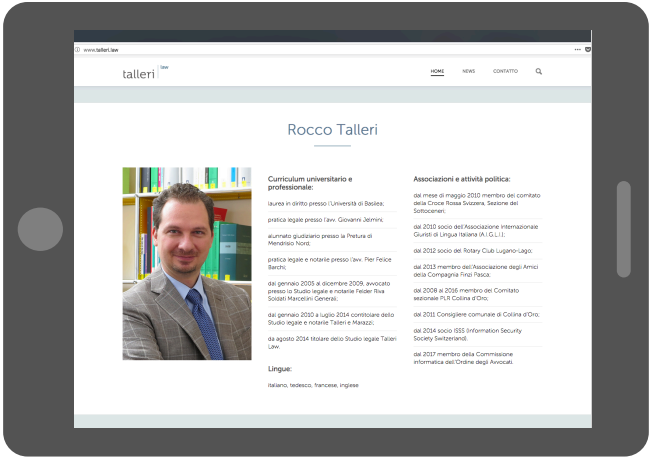
Grazie per l’attenzione!

avv. Rocco Talleri

rocco@talleri.ch

Talleri Law Studio legale

Via Cattedrale 4
CP 6544
CH -6901 Lugano
www.talleri.law



ATTENZIONE: il presente documento e il suo contenuto sono da intendersi ai soli fini informativo e divulgativo. Non costituisce un parere giuridico e non sostituisce in alcun modo una consulenza legale con un avvocato.