Print Reset

Piano di emergenza per cyber-evento

Si consiglia di compilare il piano di emergenza insieme al proprio specialista IT

Impresa:	
Autore:	
Funzione autore:	
Data stesura o rielaborazione:	
Versione:	
Polizza di assicurazione Cyber:	AXA Assicurazioni SA, polizza n.

Chi è il referente principale in caso di cyber-evento (cognome, nome, n. tel., e-mail, ecc.)?

Responsabile principale:	
Sostituto:	

Informazioni sui principali partner IT

Funzione	Impresa	Referente N. di telefono Indirizzo e-mail
Fornitore servizi informatici:		
Web host:		
Provider di telecomunicazione:		
Provider servizi in cloud:		
Incaricato protezione dati:		
Assicuratore Cyber:	AXA Assicurazioni	+41 58 218 11 33 schaden@axa.ch
Esperto di cyber security:		

17907IT – 2022-05 D

Indice

1 Nozioni fondamentali sui cyber-eventi

Un cyber-evento consiste ad esempio in un attacco provocato da virus o da altri software malevoli a computer, notebook e server. Tra le possibili conseguenze rientrano la perdita di dati aziendali oppure il furto di dati dei clienti. In casi estremi l'intera infrastruttura IT o parte di essa risulta inutilizzabili per un periodo prolungato. L'obiettivo del piano di emergenza è essere pronti a un cyber-evento, così da garantire il ripristino delle condizioni di normalità in azienda nel più breve tempo possibile.

Tipici esempi di cyber-evento:

- Cryptolocker / ransomware / malware / virus: importati tramite e-mail, siti Internet, chiavette USB.
- DDoS (Distributed Denial of Service): determina un'interruzione di servizio del sito Internet.

Che misure posso adottare?

Misure preventive di preparazione (elenco non esaustivo)

- Backup periodico dei dati, regolare verifica del ripristino ottimale dei dati.
- Protezione antivirus/antimalware su computer, notebook, telefoni e server.
- Regolare installazione del software più aggiornato per
  - sistemi operativi (PC/laptop e server)
  - applicazioni IT
  - smartphone
  - dispositivi di comunicazione (switch, firewall)
- Formazione utenti: creare consapevolezza su minacce cibernetiche e cybersicurezza.

Misure di ripristino

- Elaborazione di un piano di emergenza cibernetico.
- Verifica dei piani.
- Documentazione delle applicazioni IT critiche e dell'infrastruttura.

2 Sviluppo tipico e procedura in caso di cyber-evento

a) Rilevazione del problema informatico da parte degli addetti o dei responsabili IT. I sistemi non reagiscono come di consueto o addirittura non sono più disponibili.
b) Il collaboratore informa il responsabile interno IT e descrive la situazione.
c) Il responsabile IT consulta il fornitore esterno di servizi IT (se non è stato possibile risolvere internamente).
d) Opzione: notifica ad AXA per la liquidazione del danno

Possibili segnali di un cyber-evento

- Cryptolocker: segnalazione che i dati sono stati criptati. Per la decriptazione viene richiesto un riscatto in denaro.
- DDoS: il sito Internet non è più disponibile.

3 Struttura architettura e responsabilità IT

Illustrare la struttura dell'architettura e delle responsabilità IT:

(Elenco applicazioni e relativi responsabili)
App. 1
App. 2

(Elenco server e responsabili server/infrastruttura, ad es. anche partner esterni)
Serv. 1
Serv. 2

(Piano e responsabile/i di rete)

4 Informazioni sulle misure preventive

Backup

a) Chi è responsabile per il backup?
(dati di contatto incl. n. di tel. e sostituto)

b) Qual è l'oggetto del backup?
☐ Applicazioni ☐ Server
☐ PC/laptop ☐ Banche dati

c) Con quale frequenza vengono effettuati i backup?
☐ Quotidiana ☐ Più volte la settimana
☐ Settimanale ☐ Meno spesso

Osservazioni:

d) Quando sono stati positivamente testati per l'ultima volta i backup (ad es. con ripristino di dati e server)?

Data:

Con quale frequenza vengono testati i backup?

☐ Mensile ☐ Annuale
☐ Ad hoc ☐ Meno spesso

e) Dove vengono salvati i dati di backup?
☐ Su server locale ☐ Su server esterno
☐ In cloud ☐ Presso un operatore IT

Osservazioni:

f) I backup vengono effettuati automaticamente o con procedura manuale?
☐ Automaticamente ☐ Manualmente

Osservazioni:

Protezione antivirus
I server e i PC/laptop sono protetti da un programma antivirus aggiornato?

Server	☐ Si	☐ No
PC/laptop	☐ Si	☐ No

Aggiornamenti
Server e laptop vengono regolarmente sottoposti ad aggiornamenti (di sicurezza)?

Server	☐ Si	☐ No
PC/laptop	☐ Si	☐ No

Formazioni
I collaboratori dell'azienda vengono regolarmente formati in materia di rischio cibernetico?

Management	☐ Si	☐ No
Personale	☐ Si	☐ No

5 Ripristino della funzionalità

Quali applicazioni e sistemi IT hanno la priorità in caso di cyber-evento?

Priorità	Applicazione / sistema IT	Necessario per	Tempo di fermo max. accettabile
1	(App. 1/Serv.)	(Ordine merci)	(0,5 giorni lavorativi
2			
3			
4			

Dove si trovano le istruzioni sulle applicazioni / sui sistemi IT?

Dove si trovano i dati di accesso per le applicazioni / i sistemi IT?

6 Comunicazione in caso di cyber-evento

In caso di cyber-evento informare per tempo i principali stakeholder.
Attenzione: una volta effettuata la comunicazione tenere costantemente aggiornati i vari uffici.

a) Comunicazione interna

Accertare che …

- internamente tutto il personale sia informato dell'evento
- siano elaborate regole di comportamento obbligatorie per tutto il personale, ad es.
  - non fornire alcuna dichiarazione ai media, a soggetti o istituzioni esterni
  - evitare supposizioni e speculazioni
  - sapere di cosa tenere conto in questo caso particolare
- tutte le richieste di informazioni siano inoltrate a un soggetto predeterminato

b) Comunicazione esterna

Inserire nella tabella gli stakeholder esterni importanti (clienti ed eventualmente autorità):

Contatto (cognome/nome)	N. di telefono	Indirizzo e-mail

- Se necessario informare anche i clienti in modo da evitare il propagarsi del cyber-evento. **Un elenco di contatti dei clienti è reperibile in:**

c) Chi è responsabile della comunicazione?

Comunicazione interna:	
Responsabile principale:	
Sostituto:	
Comunicazione esterna	
Responsabile principale:	
Sostituto:	

7 Lista di controllo

☐ Sono noti tutti i contatti necessari in caso di cyber-evento?

☐ I responsabili IT sono chiaramente elencati?

☐ Abbiamo designato un coordinatore e relativo sostituto per i casi di emergenza?

☐ Sono state fornite le risposte alle domande sul backup?

☐ Si è proceduto a definire le applicazioni e i sistemi IT più importanti per la prosecuzione dell'attività dell'azienda?

☐ I dati di accesso e le istruzioni per le applicazioni / i sistemi IT sono accessibili e sappiamo dove trovarli?

☐ Sono noti i soggetti esterni che devono essere informati in caso di cyber-evento?

☐ Sono stati definiti un responsabile e un sostituto per la comunicazione interna ed esterna?

☐ Sono disponibili dispositivi sostitutivi (apparecchiature «pulite» da usare in sostituzione)?

☐ Esercitazione IT di emergenza: i nostri responsabili IT, i collaboratori e i fornitori di servizi coinvolti conoscono la procedura esatta in caso di attacco cibernetico?

☐ Abbiamo preparato testi informativi per i nostri canali social media (informazioni su avarie, limitazioni di servizio ecc.)?

Jetzt Security-Check machen – schnell & einfach online!

AXA
General-Guisan-Strasse 40
Casella postale 357
8401 Winterthur
AXA Assicurazioni SA

AXA.ch
myAXA.ch (portale clienti)