Print Reset

Notfallplan bei einem Cyber-Ereignis

Füllen Sie den Notfallplan am besten mit Ihrer IT-Spezialistin bzw. Ihrem IT-Spezialisten aus

Unternehmung:	
Ersteller/in:	
Funktion der Erstellerin / des Erstellers:	
Datum der Erstellung oder Überarbeitung:	
Version:	
Cyber-Versicherungspolice:	AXA Versicherungen AG, Police Nr.

Wer ist bei einem Cyber-Ereignis der/die Hauptansprechpartner/-in (Name / Vorname / Tel.-Nr. / E-Mail usw.)?

Hauptverantwortung:	
Stellvertreter/-in:	

Informationen der wichtigsten IT-Partner/-innen

Funktion	Unternehmen	Ansprechperson Telefon-Nr. E-Mail-Adresse
IT-Dienstleister/-in:		
Web-Hoster:		
Telekommunikations-Provider:		
Cloud-Service-Provider:		
Datenschutzbeauftragte/-r:		
Cyber-Versicherin:	AXA Versicherungen	+41 58 218 11 33 schaden@axa.ch
Cyber-Security-Expertin/-Experte:		

17907DE – 2022-05 D

Inhaltsverzeichnis

1 Grundlagen zum Cyber-Ereignis

Unter einem Cyber-Vorfall kann z. B. ein Befall durch Viren oder andere bösartige Software auf PC, Notebooks und Servern verstanden werden. Cyber-Vorfälle können z. B. zu Datenverlust in deiner Firma oder zu gestohlenen Kundendaten führen. Im Extremfall können wichtige Teile oder die ganze IT über eine längere Periode ausfallen. Das Ziel des Cyber-Notfallplans ist die Vorbereitung auf einen Cyber-Vorfall, um so rasch wie möglich die Wiederherstellung des Normalzustands im Betrieb sicherzustellen.

Typische Beispiele eines Cyber-Vorfalls:

- Crypto Locker / Ransomware / Malware / Viren: importiert via E-Mail, Webseite, USB-Stick.
- Distributed Denial of Service DDoS, der zu einem Ausfall der Website Service führt.

Welche Massnahmen kann ich treffen?
Präventivmassnahmen zur Vorbereitung (nicht abschliessend):

- Regelmässige Datensicherung, regelmässige Prüfung der erfolgreichen Wiederherstellung der Daten.
- Antivirus-/Anti-Malware- Schutz auf PC, Notebooks, Telefonen und Servern.
- Regelmässiges Aufspielen der aktuellen Software für
  - Betriebssysteme (PC/Laptops und Server),
  - IT-Anwendungen,
  - Smartphones,
  - Kommunikationsgeräte (Switches, Firewalls).
- Benutzerschulung: Bewusstsein für Cyberbedrohungen und Cybersicherheit schaffen.

Wiederherstellungsmassnahmen:

- Erstellung eines Cyber-Notfallplans.
- Testen der Pläne.
- Dokumentation der kritischen IT-Applikationen und der Infrastruktur.

2 Typischer Verlauf und Vorgehen bei einem Cyber-Ereignis

a) Mitarbeitende oder IT-Verantwortliche stellen IT-Problem fest. Systeme reagieren nicht wie gewohnt oder sind gar nicht mehr verfügbar.
b) Mitarbeitende/-r informiert den/die interne/-n IT-Verantwortliche/-n und schildert den Sachverhalt.
c) IT-Verantwortliche/-r konsultiert externe/-n IT-Dienstleister/-in (falls nicht intern gelöst)
d) Optional: Meldung an die AXA zur Schadenregulierung

Mögliche Anzeichen für ein Cyber-Ereignis:

- Crypto Locker: Meldung, dass die Daten verschlüsselt wurden. Zur Entschlüsselung soll Geld überwiesen werden.
- DDoS: Meine Website ist nicht mehr verfügbar.

3 Gliederung der IT-Landschaft und der IT-Verantwortlichkeiten

Zeigen Sie die Gliederung der IT-Landschaft und der IT-Verantwortlichkeiten auf:

(Applikationsliste und Applikationsverantwortliche/-r)
App. 1
App. 2

(Serverliste und
Server-/Infrastrukturverantwortliche, z. B. auch externe Partner/-innen)
Serv.1
Serv.2

(Netzwerkplan und Netzwerkverantwortliche/-r)

4 Informationen zu den Präventivmassnahmen

Back-up

a) Wer ist für das Back-up verantwortlich?
(Kontaktdaten inkl. Tel.-Nr. und Stv.)

b) Wovon wird ein Back-up erstellt?
☐ Applikationen ☐ Server
☐ PC/Laptops ☐ Datenbanken

c) Wie oft werden die Back-ups erstellt?
☐ täglich ☐ mehrmals wöchentlich
☐ wöchentlich ☐ weniger oft

Bemerkungen:

d) Wann wurden die Back-ups zuletzt erfolgreich auf getestet? (z. B. durch Wiederherstellung von Daten und Servern)

Datum:

Wie oft werden die Back-ups getestet?

☐ monatlich ☐ jährlich
☐ ad hoc ☐ weniger oft

e) Wo werden die Back-up-Daten gespeichert?
☐ lokal auf einem Server ☐ extern auf einem Server
☐ in einer Cloud ☐ bei einer/einem IT-Dienstleister/-in

Bemerkungen:

f) Erfolgen die Back-ups automatisch oder ist dies ein manueller Prozess?
☐ automatisch ☐ manuell

Bemerkungen:

Antivirenschutz
Werden die Server und PC/Laptops durch ein aktuelles Antivirusprogramm geschützt?

Server	☐ Ja	☐ Nein
PC/Laptops	☐ Ja	☐ Nein

Updates
Werden die Server und Laptops regelmässigen (Sicherheits-)Updates unterzogen?

Server	☐ Ja	☐ Nein
PC/Laptops	☐ Ja	☐ Nein

Schulungen
Werden die Mitarbeitenden der Unternehmung regelmässig bezüglich Cyberrisken geschult?

Management	☐ Ja	☐ Nein
Mitarbeitende	☐ Ja	☐ Nein

5 Wiederherstellung der Funktionalität

Welche IT-Anwendungen und IT-Systeme sind bei einem Cyber-Ereignis prioritär zu behandeln?

Priorität	IT-Anwendung / IT-System	Wird benötigt für	Max. akzeptable Ausfallzeit
1	(APP1/SERV)	(Warenbestellung)	(0.5 Arbeitstage)
2			
3			
4			

Wo sind Anleitungen zu den entsprechenden IT-Anwendungen bzw. IT-Systemen zu finden?

Wo liegen die Zugangsdaten für die IT-Anwendungen / IT-Systeme?

6 Kommunikation bei einem Cyber-Ereignis

Informieren Sie bei einem Cyber-Ereignis die wichtigsten Stakeholder frühzeitig.
Wichtig: Halten Sie die diversen Stellen nach erfolgter Kommunikation kontinuierlich auf dem Laufenden.

a) Interne Kommunikation

Stellen Sie sicher, dass …

- intern alle Mitarbeitenden usw. über den Vorfall informiert werden.
- Verhaltensregeln aufgestellt sind, die sämtliche Mitarbeitenden zu beachten haben, wie bspw.:
  - Es werden keine Stellungnahmen an Medien, externe Personen oder Institutionen abgegeben.
  - Mutmassungen und Spekulationen sind zu vermeiden.
  - Punkte, die bei diesem Zwischenfall speziell zu beachten sind.
- alle Anfragen zu Auskünften an eine vorher bestimmte Person weitergeleitet werden.

b) Externe Kommunikation

Ergänzen Sie die Tabelle mit wichtigen externen Stakeholdern (Kundinnen/Kunden und ggf. Behörden):

Kontakt (Vor-/Name)	Telefon-Nr.	E-Mail-Adresse

- Informieren Sie bei Bedarf auch Ihre Kundinnen und Kunden, damit sich das Cyber-Ereignis nicht weiterverbreitet. **Eine Kontaktliste der Kundinnen und Kunden ist zu finden unter:**

c) Wer ist für die Kommunikation verantwortlich?

Interne Kommunikation:	
Hauptverantwortung:	
Stellvertretung:	
Externe Kommunikation:	
Hauptverantwortung:	
Stellvertretung:	

7 Checkliste

- ☐ Sind im Falle eines Cyber-Ereignisses alle notwendigen Kontakte bekannt?
- ☐ Sind die IT-Verantwortlichkeiten klar aufgelistet?
- ☐ Haben wir einen Hauptverantwortlichen sowie eine/n Stellvertreter/in für die Koordination im Notfall definiert?
- ☐ Wurden die Fragen zum Back-up beantwortet?
- ☐ Sind die IT-Anwendungen / IT-Systeme, die für die Unternehmensfortführung am wichtigsten sind, definiert?
- ☐ Sind die Zugangsdaten sowie die Anleitungen für die IT-Anwendungen / IT-Systeme zugänglich und wissen wir, wo wir diese finden?
- ☐ Sind die externen Kontakte, die bei einem Cyber-Ereignis benachrichtigt werden sollten, bekannt?
- ☐ Sind verantwortliche sowie stellvertretende Personen für die interne und externe Kommunikation definiert?
- ☐ Stehen Ersatzgeräte zur Verfügung («saubere» Geräte, die als Ersatz dienen können)?
- ☐ IT-Notfallübung: Kennen unsere IT-Verantwortlichen, die Mitarbeitenden und die beteiligten Dienstleister/-innen den genauen Ablauf bei einem Cyberangriff?
- ☐ Haben wir Textinformationen für unsere Social-Media-Kanäle vorbereitet (Informationen über Ausfälle, Einschränkungen usw.)?

Jetzt Security-Check machen – schnell & einfach online!

AXA
General-Guisan-Strasse 40
Postfach 357
8401 Winterthur
AXA Versicherungen AG

AXA.ch
myAXA.ch (Kundenportal)