Print Reset

Plan d'urgence en cas de cyberévénement

Merci de remplir le plan d'urgence de préférence avec votre spécialiste informatique.

Entreprise:	
Auteur:	
Fonction de l'auteur:	
Date d'établissement ou de modification:	
Version:	
Police Assurance Cyber:	AXA Assurances SA, police n°

Qui est l'interlocuteur principal en cas de cyberévénement dans l'entreprise (nom / prénom / n° de tél. / e-mail, etc.)?

Responsable principal:	
Suppléant:	

Informations sur les principaux partenaires informatiques

Fonction	Entreprise	Interlocuteur N° de téléphone Adresse e-mail
Prestataire de services informatiques:		
Hébergeur web:		
Prestataire de télécommunication:		
Prestataire de service de cloud:		
Délégué/déléguée à la protection des données:		
Assureur cyber:	AXA Assurances	+41 58 218 11 33 sinistre@axa.ch
Expert en cybersécurité:		

17907FR – 2022-05 D

Table des matières

1 Informations générales sur les cyberévénements

On entend par cyberévénement p. ex. une attaque de virus ou d'autres logiciels malveillants dirigée contre des ordinateurs, des ordinateurs portables et des serveurs. Les cyberévénements peuvent entraîner p. ex. une perte de données dans une entreprise ou le vol de données de clients. Dans les cas extrêmes, des parties importantes du système informatique, voire l'ensemble du système, peuvent être indisponibles pendant une période prolongée.
L'objectif du plan d'urgence en cas de cyberévénement est de se préparer à une telle éventualité afin de garantir le rétablissement du système le plus rapidement possible.

Exemples typiques de cyberévénements:
- CryptoLocker (crypto-verrouilleur) / rançongiciel / logiciel malveillant / virus: importés par e mail, par un site web, par une clé USB.
- Distributed Denial of Service (DDoS, attaque par déni de service distribué) entraînant une défaillance du service sur le site web.

Quelles sont les mesures que je peux prendre?
Mesures préventives (liste non exhaustive):
- Sauvegarde régulière des données, contrôle régulier de la procédure de reconstitution des données.
- Protection antivirus / antimalware sur les ordinateurs, les ordinateurs portables, les téléphones et les serveurs.
- Téléchargement régulier des mises à jour pour:
  - Systèmes d'exploitation (ordinateurs / ordinateurs portables et serveurs)
  - Applications informatiques
  - Smartphones
  - Dispositifs de communication (commutateurs réseau, pare-feux)
- Formation des utilisateurs: sensibilisation aux cybermenaces et à la cybersécurité.

Mesures de rétablissement:
- Établissement d'un plan d'urgence en cas de cyberévénement
- Test des plans
- Documentation des applications informatiques et infrastructures critiques.

2 Déroulement typique et procédure en cas de cyberévénement

a) Les collaborateurs ou les responsables informatiques constatent des problèmes informatiques. Les systèmes ne réagissent pas normalement, voire sont totalement indisponibles.
b) Le ou les responsables informatiques consultent un prestataire informatique externe (si le problème ne peut être réglé en interne).
c) Le ou les responsables informatiques consultent un prestataire informatique externe (si le problème ne peut être réglé en interne).
d) Éventuellement: annonce à AXA pour le règlement du sinistre

Signes possibles d'un cyberévénement:
- Crypto-verrouilleur: message annonçant que les données ont été cryptées. Une somme d'argent doit être versée pour décrypter les données.
- DDoS: mon site Internet n'est plus disponible.

3 Structure du paysage informatique et des responsabilités informatiques

Décrivez la structure du paysage informatique et des responsabilités informatiques:

(liste des applications et de leurs responsables)
Appli 1
Appli 2

(Liste des serveurs et des responsables de serveurs / d'infrastructures, y compris partenaires externes)
Serveur 1
Serveur 2

(plan du réseau et responsable du réseau)

4 Informations sur les mesures préventives

Sauvegardes
a) Qui est responsable des sauvegardes? (Coordonnées, avec n° de tél. et suppléance)

b) Qu'est-ce qui fait l'objet d'une sauvegarde?
☐ Applications ☐ Serveurs
☐ Ordinateurs / ordinateurs portables ☐ Bases de données

c) À quelle fréquence les sauvegardes sont-elles effectuées?
☐ Quotidiennement ☐ Plusieurs fois par semaine
☐ Une fois par semaine ☐ Moins souvent

Remarques:

d) Quand le dernier test des sauvegardes, avec résultat positif, a-t-il été mené? (p. ex. reconstitution des données et des serveurs)

Date:

À quelle fréquence les sauvegardes sont-elles testées?

☐ Une fois par mois ☐ Une fois par an
☐ Ad hoc ☐ Moins souvent

e) Où les données de sauvegarde sont-elles enregistrées?
☐ Localement sur un serveur ☐ En externe sur un serveur
☐ Dans un cloud ☐ Auprès d'un prestataire informatique

Remarques:

f) Les sauvegardes sont-elles automatisées ou s'agit-il d'un processus manuel?
☐ Automatique ☐ Manuel

Remarques:

Protection antivirus
Les serveurs et les ordinateurs / ordinateurs portables sont-ils protégés par un programme antivirus à jour?

Serveur	☐ Oui	☐ Non
Ordinateurs / ordinateurs portables	☐ Oui	☐ Non

Mises à jour
Les serveurs et les ordinateurs / ordinateurs portables sont-ils régulièrement mis à jour (notamment les dispositifs de sécurité)?

Serveur	☐ Oui	☐ Non
Ordinateurs / ordinateurs portables	☐ Oui	☐ Non

Formations
Les collaborateurs de l'entreprise sont-ils régulièrement formés aux cyberrisques?

Dirigeants	☐ Oui	☐ Non
Collaborateurs	☐ Oui	☐ Non

5 Rétablissement du fonctionnement

En cas de cyberévénement, quels sont les systèmes et les applications informatiques qui doivent être traités en priorité?

Priorité	Application / système	Nécessaire pour	Temps d'indisponibilité maximal acceptable
1	APP 1/SERV	(Commande des marchandises)	(0,5 jour ouvré)
2			
3			
4			

Où peut-on trouver les instructions sur ces applications et systèmes informatiques?

Où se trouvent les données d'accès pour ces applications et systèmes informatiques?

6 Communication en cas de cyberévénement

En cas de cyberévénement, informez rapidement les principales parties prenantes.
Important: après avoir signalé le cyberévénement, tenez régulièrement les différents services informés.

a) Communication interne

Veillez à ce que …

- tous les collaborateurs, etc. soient informés en interne de l'événement;
- les règles de conduite à respecter soient rappelées à tous les collaborateurs, p. ex.
  - ne communiquer aucune prise de position aux médias ou à des personnes ou institutions externes,
  - éviter les suppositions et les spéculations,
  - connaître les précautions à prendre face à cet événement,
- toutes les demandes de renseignements soient transmises à une personne désignée préalablement.

b) Communication externe

Indiquez dans ce tableau les principales parties prenantes externes (clients et év. autorités):

Identité (nom, prénom)	N° de téléphone	Adresse e-mail

- Au besoin, informez également vos clients pour éviter que le cyberévénement ne se propage. **Une liste des clients est disponible à l'adresse:**

c) Qui est responsable de la communication?

Communication interne:	
Responsable principal:	
Suppléant:	
Communication externe:	
Responsable principal:	
Suppléant:	

7 Check-list

- ☐ Tous les interlocuteurs importants en cas de cyberévénement sont-ils connus?
- ☐ Une liste claire des responsables informatiques est-elle disponible?
- ☐ Avons-nous désigné un responsable principal ainsi qu'un suppléant pour la coordination de la situation d'urgence?
- ☐ Avons-nous répondu aux questions concernant les sauvegardes?
- ☐ Les systèmes / applications informatiques indispensables au maintien de l'activité de l'entreprise ont-ils été définis?
- ☐ Les données d'accès ainsi que les instructions pour les systèmes / applications informatiques sont-elles accessibles, et savons-nous où les trouver?
- ☐ Les interlocuteurs externes à contacter en cas de cyberévénement sont-ils connus?
- ☐ Avons-nous désigné un responsable ainsi qu'un suppléant pour la communication interne et externe?
- ☐ Des appareils de remplacement sont-ils disponibles (appareils «propres» à utiliser en remplacement)?
- ☐ Exercice d'urgence informatique: nos responsables informatiques, les collaborateurs et les prestataires concernés connaissent-ils la procédure à suivre en cas de cyberattaque?
- ☐ Avons-nous préparé des informations textuelles pour nos canaux de médias sociaux (informations en cas d'indisponibilité, de restriction d'accès, etc.)?

AXA
General-Guisan-Strasse 40
Case postale 357
8401 Winterthur
AXA Assurances SA

AXA.ch
myAXA.ch (portail clients)