Comportement en cas de cyberattaque

Cyberrisques et mesures de protection

Les enquêtes révèlent qu'une PME suisse sur trois a déjà subi une cyberattaque réussie. Toute entreprise, aussi petite soit-elle, devrait être consciente de ce qu'une cyberattaque peut déclencher. Qu'il s'agisse simplement d'un accès temporairement refusé à des applications informatiques ou d'une perte d'image suite à un vol de données rendu public ou même des conséquences juridiques en raison d'éventuelles violations du devoir de diligence. Il est donc particulièrement important de mettre en place des mesures de prévention pour se protéger efficacement de ces attaques. Il s'agit tout d'abord de configurer son propre système ou de l'équiper en fonction, de définir des processus internes de telle manière qu'ils ne peuvent être influencés depuis l'extérieur et sensibiliser les collaborateurs. Cette fiche technique sert de rappel à l'ordre à tous les responsables.

Contenu :

28.11.2023 Comportement en cas de cyberattaque
Publication publique

Bahnhofstrasse 94, 5000 Aarau
T +41 44 388 53 00
info@jardinsuisse.ch | jardinsuisse.ch

JardinSuisse
Association suisse des entreprises horticoles
Nous cultivons l'avenir.

1. Mesures pour une protection efficace contre les cyberattaques

- Assumer des tâches de gestion et partager les responsabilités
- Sauvegarder régulièrement les données par le biais de back-ups externes (protection contre le vol de données). Périodicité : tant que les activités peuvent se poursuivre sans applications informatiques
- Actualiser régulièrement les logiciels
- Protéger l'accès à Internet avec un pare-feu
- Actualiser le programme antivirus
- Définir des mots de passe sûrs (au moins 12 signes, comprenant des majuscules et des minuscules, des chiffres, des signes de ponctuation), combinés à un coffre-fort de mots de passe et utiliser l'authentification à deux facteurs
- Communiquer les directives d'utilisation informatique à tous les collaborateurs
- Classifier les données et contrôler les droits d'accès
- Contrôler les adaptations des systèmes de production grâce à la gestion des changements (processus de panification, mise en œuvre et contrôle des changements apportés aux systèmes informatiques, afin d'assurer une transition sans faille)
- Protéger l'environnement informatique (par ex. les contrôles d'accès, protection contre les effractions)

2. Identifier une cyberattaque

Les hackers sont comme des cambrioleurs. Ils essaient d'éveiller le moins possible les soupçons et de dissimuler leurs traces. Souvent, on ne voit pas tout de suite si un cybercriminel est déjà entré dans le système. Des semaines ou mêmes des mois peuvent s'écouler avant que le maliciel soit activé.

Signes d'une cyberattaque en cours :

- Un système lent
- Les données ne sont pas disponibles
- Les mots de passe ne fonctionnent plus
- Un écran clignotant
- L'ordinateur semble effectuer des actions de manière autonome
- Les programmes ne démarrent pas ou réagissent de manière inattendue
- L'ordinateur produit de nombreux messages d'erreur
- Une demande de rançon apparaît sur l'écran

Agissez rapidement lorsque vous identifiez de tels signes. Cette liste n'est pas exhaustive.

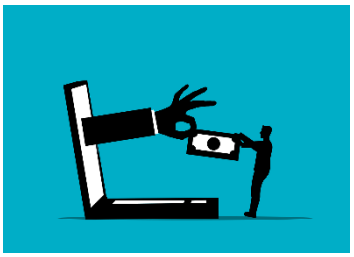
3. Comment bien réagir à une cyberattaque

1. Déconnecter immédiatement tous les systèmes du réseau et éteindre le Wi-Fi
2. Informer la personne responsable de la sécurité informatique
3. Informer les collaborateurs
4. Analyser le problème et les dommages (évtl. avec des experts)
5. Si vous disposez d'une cyberassurance, informez-la :
   L'assurance a des entreprises partenaires spécialisées qui peuvent apporter leur aide. Dans le meilleur des cas, elle prend en charge les coûts pour le nettoyage des systèmes informatiques, la restauration des données et indemnise l'interruption d'exploitation.

En cas d'attaque de grande ampleur, on attend que la police ait sécurisé des indices avant de nettoyer et de restaurer les systèmes. Même en l'absence de dommage, il est préconisé d'informer de l'incident la police ainsi que le Centre national pour la cybersécurité NCSC (www.report.ncsc.admin.ch/fr/). Les auteurs sont rarement arrêtés, mais les signalements peuvent contribuer à la prévention et à la sensibilisation d'autres victimes potentielles.

Important : ne payez pas de rançon ! En effet, qui paie une fois devient une victime vraiment intéressante pour les hackers.

3.1. Les cinq erreurs majeures en cas de cyberattaque



- Laisser le système informatique connecté au réseau, ne pas éteindre le Wi-Fi
- Ne rien faire et laisser passer l'attaque
- Payer une rançon
- N'informer personne pour éviter les dommages de réputation
- Penser que cela n'arrive qu'aux autres et ne prendre aucune mesure pour la cybersécurité

4. Formation de sensibilisation aux cyberrisques pour les collaborateurs

Tout va très vite : Un collaborateur ouvre un e-mail sans réfléchir et toute l'entreprise est soudainement immobilisée. Il est donc important d'informer et de sensibiliser les collaborateurs à l'utilisation d'Internet et du courrier électronique. Différents prestataires et certaines assurances proposent des cyberformations pour les entreprises. En envoyant des e-mails d'hameçonnage simulés, le prestataire de cours peut rendre compte à l'entreprise des réactions des employés. Vous voyez ainsi si d'autres mesures de sensibilisation sont nécessaires.

5. Liens

Le Centre national pour la cybersécurité NCSC de la Confédération fournit des renseignements supplémentaires sur les mesures organisationnelles et techniques (www.ncsc.admin.ch/ncsc/fr/home.html).

Sources : dergartenbau numéro 20/2023, www.mobiliar.ch