EXPERT suisse
Wirtschaftsprüfung
Steuern
Treuhand

Liste de contrôle en cas de cyberattaque

Mesures préventives

1. Sensibiliser et former les collaborateurs, notamment à l'aide de tests de hameçonnage et de formations en cybersécurité.
2. Vérifier constamment la protection de l'infrastructure IT. Installer les correctifs et les mises à jour en continu.
3. Effectuer des sauvegardes régulières et contrôler le pare-feu.
4. Utiliser des logiciels anti-malware.
5. Limiter les autorisations d'installation de logiciels.
6. Utiliser des mots de passe forts et sécurisés. Changer les mots de passe régulièrement.
7. Activer l'authentification multifactorielle *(multi-factor authentication ou MFA)* à chaque fois que possible.
8. Être **prudent** sur les médias sociaux.
9. Toujours utiliser une **connexion Internet sécurisée** (VPN), ainsi que généralement le cryptage.

Liste de contrôle en cas de cyberattaque

1. D'abord, **garder son calme** et agir de manière réfléchie. Ne répondez **jamais** aux demandes des criminels. Autrement, l'entreprise sera considérée comme une cible lucrative et d'autres attaques pourront suivre. Attention: il est important de **documenter** chaque étape pour être en mesure de réitérer la procédure ultérieurement.
2. Déconnecter immédiatement les systèmes infectés du réseau. Pour ce faire, débrancher le câble réseau de l'ordinateur et, le cas échéant, les adaptateurs Wi-Fi existants. Introduire des mesures pour empêcher la propagation de la potentielle attaque (redirection du trafic réseau, filtrage ou blocage du trafic des données et isolement de tout ou partie du réseau éventuellement compromis).
3. Informer son **supérieur hiérarchique** et le **service informatique** par téléphone.
4. Vérifier s'il s'agit effectivement d'une cyberattaque ou d'une erreur technique. En attendant, éviter toute communication possible vers l'extérieur. S'il s'agit d'une cyberattaque, informer la police et faire appel à des spécialistes.
5. Identifier les systèmes qui ont été atteints pour comprendre la manière dont l'attaque s'est déroulée. En outre, il s'agit de déterminer si des **données** ont été **volées** et lesquelles, et quels réseaux sont concernés. Déterminer quels nœuds ont été compromis, quels services ont été interrompus et évaluer l'étendue et la nature des dommages causés aux systèmes.
6. Le **Préposé fédéral à la protection des données et à la transparence (PFPDT)** doit impérativement être informé en cas de vol de données sensibles présentant un risque important pour la personnalité ou les droits fondamentaux des personnes concernées.
7. Combler toutes les failles de sécurité utilisées par le ou les pirates.
8. Informez les **collaborateurs** et les **clients** concernés.
9. Ne jamais négocier avec les criminels **sans l'aide de la police!**
10. Prendre des mesures pour essayer de restaurer les données et les systèmes.
11. **Analyse:** Comment l'attaque aurait-elle pu être évitée? Quelles mesures devront désormais être mises en œuvre?

Date de création: 20 mai 2022