

Attaque informatique : les 7 gestes qui sauvent



Perspectives IT, 14 octobre 2016, 11:00SECURITÉ 3 1 108LOG PROPOSÉ PAR DELL EMCVotre PC est infecté. Mais repérer l'attaque n'est que la première étape. Il faut ensuite organiser la réponse à l'incident. Et les premiers gestes ont ici une importance capitale.

7 gestes de premiers secours à connaître face à une attaque informatique.

Votre poste de travail est infecté. La stratégie en place de détection des intrusions a fonctionné et une menace a été identifiée. Et ensuite ? Repérer l'attaque informatique n'est que la première étape. Encore faut-il savoir ensuite organiser la réponse à l'incident. Et les premiers gestes ont ici une importance capitale. Pour éviter que la situation ne s'aggrave tout d'abord, mais aussi pour permettre de récolter un maximum d'informations sur l'attaque. Les collaborateurs d'une entreprise n'étant pas censés être tous des experts en sécurité informatique, la formation et la sensibilisation sont des missions clés des RSSI. Pour les aider, le CERT-FR a dressé une liste des bons réflexes à adopter.

RÉAGIR EN CAS D'ATTAQUE INFORMATIQUE

- 1 Déconnecter le poste de travail**
Si votre ordinateur est infecté, déconnectez-le immédiatement de tous les réseaux (Wi-Fi, Ethernet, Bluetooth, etc.).
- 2 Ne pas aller sur d'autres ordinateurs**
La machine qui est infectée peut servir de relais pour infecter d'autres ordinateurs. Ne touchez pas d'autres ordinateurs, ni des clés USB.
- 3 Prévenir le responsable de votre service**
Informez votre responsable de l'incident. Il pourra vous aider à organiser la réponse à l'incident.
- 4 Appeler le CERT-FR**
Le CERT-FR est le centre national de réponse aux incidents de sécurité informatique. Il est composé de professionnels de la sécurité informatique et de la police. Vous pouvez les contacter par téléphone (01 20 39 61 32) ou par email (cert@cert.fr).
- 5 Effectuer une sauvegarde de l'état de l'ordinateur**
Effectuez une sauvegarde de l'état de l'ordinateur (système d'exploitation, fichiers, etc.) pour permettre l'analyse de l'incident.
- 6 Suivre les traces**
Conservez les données de l'ordinateur (logs, fichiers, etc.) pour permettre l'analyse de l'incident.
- 7 Ne pas effectuer de nouvelles opérations**
Ne faites pas de nouvelles opérations sur l'ordinateur infecté.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03841 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audit Sécurité (ISO 27001) ;
- Expertises techniques et judiciaires (avis techniques, technique de preuve, illégalités, diquesurs, e-mails, contenus, détournement de clientèle...)
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybersécurité ;
- Formation de CIL (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Réagissez à cet article

Source : *Attaque informatique : les 7 gestes qui sauvent – Silicon*