Hacking - Sabotage

Version PDF

Qu'est ce que c'est le Hacking / Sabotage ?

Hacking :

C'est l'intrusion non autorisée dans un système informatique. L'intrusion implique généralement une intention malveillante, mais le fait d'établir involontairement une connexion et de la maintenir volontairement est également considéré comme un piratage. Même le piratage d'un système informatique peu ou pas sécurisé est punissable.

Sabotage de données et/ ou d'ordinateurs :

Le sabotage informatique peut être défini comme du vandalisme dans un environnement informatique.
La différence du sabotage informatique est que cette démarche n'entraîne pas nécessairement un enrichissement. La modification de données sans autorisation est en soi un délit.

Le développement et la distribution d'outils de sabotage de données sont également punissables.

De quoi avez-vous besoin pour déposer plainte ?

- Recueillir des informations sur l'appareil piraté
    - Marque et modèle, numéro de série, système d'exploitation, programme anti-virus, ...
    - Qui a accès (physique et à distance) à l'appareil ?

    - Quand l'appareil a-t-il fonctionné correctement et quand le problème a-t-il été détecté, comment et par qui ?
    - Ce qui s'est passé juste avant que le problème ne survienne (clic sur un lien, réception d'un message sur l'écran, ...)
    - Si vous avez demandé l'aide d'un expert: demandez-leur d'imprimer ou de télécharger autant de preuves que possible afin que vous puissiez nous les remettre. Par exemple, les fichiers log.
- Collectez des informations concernant toute communication avec l'auteur des faits.
    - Numéros de téléphone, adresses e-mail, noms (pseudos), adresses IP, comptes de médias sociaux utilisés, etc.
    - faites des captures d'écran
- Collectez des informations concernant les paiements
    - numéros de compte, transactions, adresses de bitcoins, ...
    - faites des captures d'écran

Que pouvez-vous encore faire ?

- Changez vos mots de passe pour tous vos comptes.
- Activez la vérification en deux étapes (2FA) pour **tous les comptes qui le permettent**.
    - Cela empêche les pirates d'accéder à votre compte, même s'ils disposent de votre identifiant et de votre mot de passe. Après tout, une "deuxième étape" doit être franchie. Cela peut se faire par SMS ou par une application sur votre smartphone.
- Vérifiez l'absence de virus et de logiciels espions sur votre ordinateur ou votre appareil en effectuant une analyse approfondie. En cas de doute, contactez un expert.
- Limitez les dégâts en déconnectant tous vos appareils d'Internet (pensez aussi aux connexions Wifi).

Comment éviter d'être à nouveau victime ?

- Utilisez des mots de passe sûrs (longs, avec des chiffres, des symboles, des minuscules et des majuscules, il peut aussi s'agir d'une phrase).
- Utilisez l'authentification à deux facteurs chaque fois que possible. Il s'agit d'une sécurité supplémentaire via, par exemple, votre téléphone portable.
- Utilisez un mot de passe unique pour chaque compte important, ne le partagez pas et ne mentionnez pas les mots de passe dans vos e-mails,

votre smartphone ou votre ordinateur.

- Sécurisez vos systèmes informatiques en installant un logiciel anti-virus, un pare-feu et un anti-spyware et effectuez des analyses régulières.
- Installez régulièrement les mises à jour de votre ordinateur et de vos programmes. Vous pouvez paramétrer cette opération pour qu'elle se produise automatiquement dès que la mise à jour est disponible.
- Restez critique à l'égard des courriels provenant d'expéditeurs inconnus. Ne les ouvrez pas, n'y répondez pas et ne les transmettez pas.
- Ne téléchargez pas de logiciel ou autre chose à partir de sources inconnues.
- Si vous êtes connecté à un site web pour faire des achats, écrire un commentaire ou autre, pensez à vous déconnecter avant de quitter la page.
- En cas de doute, demandez conseil !

Où pouvez-vous trouver plus d'informations ?

https://www.safeonweb.be/fr/mon-compte-est-pirate