2

Les dix règles de base pour sécuriser votre PC

CENTRE DE RECHERCHE
SUR L'INFORMATION
SCIENTIFIQUE ET TECHNIQUE
cerist

LES DIX RÈGLES DE BASE

1. Mettre à jour régulièrement le système d'exploitation et les logiciels installés : Maintenir votre système d'exploitation à jour est la première des règles de sécurité. La plupart des attaques tentent d'utiliser les failles d'un ordinateur (failles du système d'exploitation ou des logiciels). En général, les agresseurs recherchent les ordinateurs dont les logiciels n'ont pas été mis à jour afin d'utiliser la faille non corrigée et ainsi parviennent à s'y introduire. C'est pourquoi il est fondamental de mettre à jour tous ses logiciels afin de corriger leus failles.

2. Se protéger contre les intrusions en installant des logiciels de sécurité : Ces logiciels (antivirus, firewall, anti-spam.. etc.) permettent de vous protéger contre la plupart des attaques visant à corrompre votre ordinateur. Cependant, il ne faut pas oublier de les mettre à jour régulièrement. En général, une option de mise à jour automatique est disponible lors de la configuration de ces logiciels.

3. Effectuer des sauvegardes régulières : Un des premiers principes de défense est de conserver une copie de ses données (sur des supports amovibles : CD/DVD, disque dur externe…) afin de pouvoir réagir à une attaque ou un dysfonctionnement. La sauvegarde de vos données est une condition de la continuité de votre activité.

4. Utiliser des mots de passe de qualité : Par définition, un mot de passe désigne une séquence de caractères utilisée par un usager pour valider son accès à des ressources personnelles. Plus la séquence est aléatoire, plus le mot de passe est sûr. Pour ce faire, une combinaison de majuscules, minuscules, chiffres et caractères spéciaux avec une taille du mot de passe dépassant les dix caractères est recommandée pour éviter qu'il soit cassé par des outils automatisés.

5. Ne pas ouvrir des pièces jointes provenant de sources suspectes ou inconnues : Une des méthodes les plus efficaces pour diffuser des codes malveillants est d'utiliser des fichiers joints aux courriels. Pour se protéger, ne jamais ouvrir les pièces jointes dont les extensions sont les suivantes : .pif (comme par exemple une pièce jointe appelée «photos.pif), .com, .bat, .exe, .vbs et .lnk .

6. Eviter de cliquer rapidement sur des liens suspects : Une des attaques classiques visant à tromper l'internaute pour lui voler des informations personnelles, consiste à l'inciter à cliquer sur un lien placé dans un message. Ce lien peut-être trompeur et malveillant. Plutôt que de cliquer sur celui-ci, il vaut mieux saisir soi-même l'adresse du site dans la barre d'adresse du navigateur, de nombreux problèmes seront ainsi évités.

POUR SÉCURISER VOTRE PC

7. Désactiver par défaut les composants ActiveX et JavaScript : Les composants ActiveX ou JavaScript permettent des fonctionnalités intéressantes, mais ils présentent aussi des risques de sécurité pouvant aller jusqu'à la prise de contrôle par un intrus d'une machine vulnérable. En dépit de la gêne que cela peut occasionner, il est conseillé de désactiver leur interprétation par défaut et de choisir de ne les activer que lorsque cela est nécessaire et si l'on estime être sur un site de confiance.

8. Eviter de divulguer des informations personnelles : Les informations personnelles diffusées sur internet (nom, prénom, numéro de tél… etc.) peuvent faciliter la tâche à un utilisateur malveillant préparant une attaque de type « social engineering ». Il faut éviter aussi de saisir des informations sensibles (comme des coordonnées bancaires) sur des sites qui n'offrent pas toutes les garanties requises.

9. Eviter d'installer des logiciels de partage (P2P) : Le Peer-to-Peer (P2P) est un moyen de téléchargement devenu très populaire. Cependant, les auteurs de malwares ont investi ce réseau afin d'y déposer des fichiers piégés dans le but de propager leurs infections.

10. Ne pas surfer sur Internet tout en étant en mode Administrateur : Vous ne devez ni surfer sur le Web, ni consulter vos e-mails, ni accéder sous quelque forme que ce soit (messagerie instantanée, P2P etc. ...) à l'Internet lorsque vous êtes en mode Administrateur. Ceci peut être dangereux vu que les droits dits d'Administrateur donnent tous les privilèges à un attaquant si celui-ci a pu compromettre votre PC.