Sécurité informatique: Qualité logicielle

Cherchant un sujet sur le site web du CERN que j'analyserais, j'ai remarqué que le CERN accorde une grande attention à la sécurité informatique et qu'il y a beaucoup de texte lié à ce sujet. L'un des sujets que j'ai choisis est de savoir dans quelle mesure la qualité des logiciels affecte la sécurité et quelles sont les voies et recommandations pour une sécurité encore meilleure.

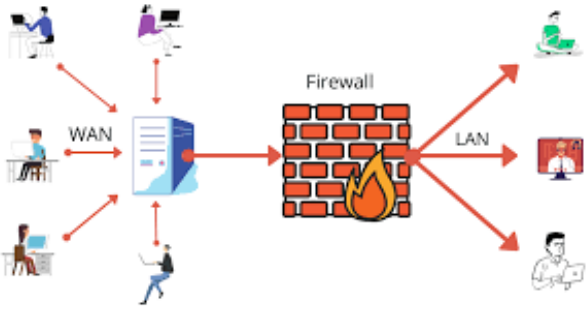
Un logiciel de qualité, programmé dans le respect des bonnes pratiques de sécurité, est plus difficile à exploiter.

Mises à jour régulières de l'appareil pour que les vulnérabilités et faiblesses connues ne puissent pas être exploitées par des personnes mal intentionnées fait partie des bonnes pratiques de base dans le domaine de la sécurité informatique. Le problème est que ces vulnérabilités et faiblesses ne sont justement pas toujours connues. Toutes ne sont pas signalées ou publiées immédiatement après leur découverte. Il existe généralement un délai de grâce d'environ trois mois accordé par les personnes pratiquant la “ divulgation responsible ” aux propriétaires de logiciels, pour que ces derniers puissent réparer les failles, avant qu'elles ne soient rendues publiques. Au moment de leur publication, les mesures prises sont documentées et appliquées grâce au mécanisme de mise à jour standard. Cependant, certaines personnes, organisations ou entreprises optent parfois pour une approche bien différente. Au lieu de pratiquer la divulgation responsable, elles collectent des données sur les vulnérabilités et faiblesses pour les vendre au plus offrant (souvent sur le marché noir), ou les utiliser à de mauvaises fins (espionnage, cyberattaques, etc.).

Une autre bonne pratique permet toutefois de limiter les risques en matière de sécurité informatique: la réduction de l'exposition aux attaques. Moins il y a de logiciels installés sur un appareil, mieux ils sont programmés ; moins un logiciel est répandu sur le marché, plus la surface d'attaque est limitée. Un logiciel qui n'est pas installé ou exécuté sur un appareil ne présente aucun risque pour ce dernier. Un logiciel de qualité, programmé dans le respect des bonnes pratiques de sécurité, est plus difficile à exploiter. Enfin, un logiciel utilisé par peu de personnes ne sera probablement pas pris pour cible par les pirates informatiques, puisque le détourner ne présente pas un intérêt financier suffisant.

Tous systèmes d'exploitation confondus (Windows, Mac et Linux), parmi les applications présentant le plus de failles signalées en 2017 figurent Microsoft Edge, Safari d'Apple, Adobe Acrobat et Acrobat Reader, et Java JDK et JRE d'Oracle.

Les types de programmes qui peuvent protéger un ordinateur contre les ”intrusions” d’autres ordinateurs sont les “pare-feu” (ang. Firewall). Un pare-feu est un périphérique de sécurité réseau qui autorise ou bloque les flux de trafic réseau qui ont lieu entre une zone non approuvée (comme Internet) et une zone sécurisée (approuvée) (comme un réseau privé ou d'entreprise). Le pare-feu doit empêcher le trafic indésirable, bloquer les “intrusions” dans le réseau local et protéger les ordinateurs qu'il contient.



En tant que “flic de la circulation” sur le réseau, le pare-feu surveille tout le trafic et active ou désactive le flux de certains trafics, c'est donc le meilleur emplacement pour l'application des politiques de sécurité.

Aussi, un programme informatique qui contribue au maintien de la sécurité est un antivirus. Un antivirus est un logiciel qui a pour but de détecter et d'éradiquer les virus présents dans micro, et de prendre des mesures pour les empêcher de nuire.

Les antivirus sont des programmes devenus de plus en plus indispensables au fil des années. Lorsqu’ils sont installés sur un ordinateur, il joue deux rôles différents : la première est de vous permettre de naviguer en toute protection sur le web et la seconde est la possibilité d’analyser les supports de stockage. Le rôle de l'antivirus consiste aussi à prévenir l'attaque virale, en analysant le comportement.

Sitographie:

- https://home.cern/fr/news/news/computing/computer-security-about-risks-and-threats
- https://home.cern/fr/news/news/computing/why-you-got-new-pdf-reader

Mots inconnus:

- la vulnérabilités , *f* – **ranjivost**
- la faiblesses, *f* – **slabost**
- le détourner, *m* – **otmica**
- la intrusion, *f* – **mesanje, upad**
- le pare-feu, *m* – **zaštitni zid**
- indésirable, *adj* – **nepoželjan**
- éradiquer, *v* – **iskoreniti, istrebiti**
- un délai de grâce, *m* – **grejs period**