5 conseils pour améliorer la sécurité de votre PC Linux

je suis tombé sur une news qui pourrait intéresser les utilisateurs Linuxiens pour sécuriser leur PC.
Il y a beaucoup de serveurs Linux sur le net.
En conséquence, les cyberescrocs ont appris à pirater les serveurs Linux à l'échelle industrielle pour voler à la fois l'espace de stockage et la bande passante.
Avec ces serveurs piraté, ils poussent des logiciels malveillants, le spam, les escroqueries et les campagnes de phishing sur les utilisateurs à travers le monde.
Bien sûr, la grande majorité des victimes qui se font attaquer ou infectés via les serveurs corrompus sont sur un PC avec Windows.
Si vous exécutez un PC Linux, la vie peut être beaucoup plus calme, environ 2% des ordinateurs de bureau dans le monde entier.
Être dans une petite minorité signifie que vous n'avez pas encore attiré beaucoup l'attention des cybercriminels, qui font déjà d'énormes quantités d'argent de l'écosystème Windows.

Mais est-ce suffisant pour se considérer en sécurité ?

Nacked security propose 5 conseils pour sécuriser votre PC.

1. Choisissez Full Disk Encryption (FDE)

Peu importe le système d'exploitation que vous utilisez, ils recommandent de chiffrer l'ensemble de votre disque dur.

Si votre ordinateur portable est perdu ou volé, en utilisant un mot de passe de connexion simple pour protéger vos données: un voleur peut simplement démarrer Linux à partir d'une clé USB et lire toutes vos données hors connexion sans saisir de mot de passe.

En chiffrant votre disque dur, vous assurer que vos données restent sécurisées, parce que le voleur ne sera pas capable de lire vos données, sans le mot de passe FDE.

L'avantage de chiffrer votre répertoire Home et les fichiers qu'il contient est que vous ne devez plus vous soucier des fichiers temporaires, les fichiers SWAP ou d'autres répertoires où les fichiers importants pourraient finir sans vous en rendre compte.

Sur un ordinateur assez récent, vous avez peu de chances de remarquer, ou même d'être capable de mesurer, un ralentissement de l'utilisation au jour le jour.

Sur Ubuntu et Fedora, comme dans de nombreuses autres distributions Linux, le chiffrement de disque complet est disponible au moment de l'installation.

Vous pouvez facilement l'activer lors de l'installation en le sélectionnant, comme dans l'exemple ci-dessous (Ubuntu):

2. Garder vos logiciels à jour

Encore une fois, quel que soit le système d'exploitation que vous utilisez, vous devez toujours garder

à la fois votre système d'exploitation et vos applications, telles que les navigateurs Web, les lecteurs de PDF et de lecteurs vidéo, à jour.
La plupart des distributions Linux rendre cela facile.
Sur Ubuntu, par défaut, les mises à jour de sécurité sont installés automatiquement.
Vous pouvez double-vérifier cela à Paramètres système | Logiciels | Mises à jour et mises à jour.
Assurez-vous que l'option de mises à jour importantes de sécurité est activé:

3. apprendre à utiliser le Firewall dans Linux

Le noyau Linux inclue un Firewall appelé `iptables`, qui vous donne un moyen puissant pour gérer le trafic réseau et de vous protéger de nombreuses cyberattaque.
Sur Ubuntu une application appelée Uncomplicated Firewall (UFW), vous propose une interface graphique qui simplifie la mise en place de `iptables`.
Par défaut UFW est désactivé, mais vous pouvez l'activer à partir d'une invite de commande en faisant:

```
$sudo ufw enable
Password:

Firewall is active and enabled on system startup
$
```

Pour en savoir plus à propos de `iptables` et ce qu'il peut faire, vous pouvez également essayer un outil de configuration graphique tels que Gufw ou UFW Frontends.
Sur Fedora, vous trouverez FirewallD, une boîte à outils de gestion de pare-feu alternative qui est activée par défaut.
Une interface utilisateur graphique pour FirewallD, appelé firewall-config, est disponible, vous pouvez l'installer à partir d'un terminal avec :

```
$ yum install firewall-config
```

4. Renforcer la sécurité dans votre navigateur

Le navigateur est la manière pour de nombreuses cybermenaces actuelles, si vous utilisez Mozilla Firefox, Google Chrome, Opera ou un autre navigateur.
De nombreuses extensions sont disponibles gratuitement pour améliorer la sécurité de votre navigateur et votre vie privée ainsi. Parmi d'autres, vous voudrez peut-être envisager les mesures suivantes:

- HTTPS Everywhere-
- uBlock origin
- NoScript
- Disconnect
- RequestPolicy

5. utilisé un antivirus

Certaines personnes vous diront qu'il est inutile d'installer un logiciel anti-virus sur un système d'exploitation basé sur Linux.
L'argument principale est que la plupart des logiciels malveillants, que vous détectez sur un ordinateur Linux sera pour Windows.
Quelle question devrait-on se poser:
Alors, pourquoi devriez-vous être responsable de cela?
Que faire si vous passez un fichier infecté a quelqu'un?

L'autre argument est que les logiciels malveillants sur les ordinateurs de bureau Linux est assez rare et que vous pourriez tout aussi bien prétendre qu'il n'existe pas du tout.
Si vous vous sentez en sécurité seulement parce que vous pensez que le risque d'une violation est faible, alors les attaquants ont déjà gagné.**

Sophos Protection Linux

Ils ont regardé Sophos Antivirus, moi j'aime bien ClamAV.
Voici quelques articles que j'ai trouvés en lien :

- linuxfr.org
- ubuntu-fr.org
- wikipédia

Source: naked security et controle-tes-donnees.net