# Un guide pour sécuriser les postes de travail Linux

La Linux Foundation, consortium chargé de veiller à l'unité de l'OS libre, a décidé d'apporter conseils et recommandations pour mieux sécuriser les postes de travail sous Linux dans les entreprises. Ces indications sont issues du travail effectué pour sécuriser les postes des administrateurs systèmes de l'organisation, qui s'assurent de la sécurité des contributeurs travaillant à distance. Comme l'ont montré les documents exfiltrés par Edward Snowden dévoilant les pratiques de la NSA américaine ou encore des piratages récents, les sysadmin sont une cible de choix pour les hackers, en raison des privilèges élevés dont ils bénéficient sur les systèmes. Logique donc de voir les pirates cibler ses profils dans leur campagne mélangeant ingénierie sociale et recours à des malwares.

Publié sur Git Hub, le vade-mecum de la Linux Foundation vise à adopter des bonnes pratiques en fonction du niveau de sécurité souhaité. Le guide comprend plusieurs niveaux, allant de bas à modéré en passant par critique. On notera la présence d'un mode 'Paranoid' pour les utilisateurs qui souhaitent travailler en mode complétement fermé, si sécurisé qu'il demandera des efforts d'adaptation aux administrateurs.

## Check-list hardware et logiciel

En fonction du niveau de criticité choisi, la Linux Foundation dresse une check-list aussi bien sur le hardware (support du SecureBoot, absence de ports Firewire, Thunderbolt ou ExpressCard, présence d'une puce de chiffrement TMP) que sur l'aspect logiciel. Y figurent notamment différents éléments sur le choix de la distribution (publication de correctifs, chiffrement natif des disques) ou la politique de backup....

Le guide donne aussi ses préférences pour les navigateurs avec différents scénarios. Dans l'idéal, l'utilisateur jonglera avec deux navigateurs. Firefox est recommandé pour le travail avec l'ajout de certains modules complémentaires comme NoScript, Privacy Badger, HTTPS Everywhere et Certificate Patrol. Chrome sera privilégié pour tout le reste. Un autre scénario privilégie l'usage d'un des deux navigateurs au sein d'une VM, principalement Chrome. Enfin, une dernière option s'appuie sur la virtualisation complète pour isoler les différents environnements de travail.

Pour les paranoïaques, le verrouillage est le maître mot avec l'installation d'un système de détection d'intrusion (IDS) et d'un gestionnaire de mots de passe des comptes non web. Sur la partie chiffrement, la Linux Foundation recommande la mise en place de solutions comme SSH et PGP quel que soit le niveau de sécurité visé.

**A lire aussi :**

Linux 4.2 : une édition centrée sur le hardware

Solus OS : un système Linux qui démarre en 1,2 seconde

Sysadmin : un métier plus ou moins condamné ?

**Code Linux Crédit Photo@isaak55-Shutterstock**