Cybersécurité: les ennuis commencent déjà à l'installation

System hardening

En cybersécurité, les ennuis commencent bien souvent à l'installation du système d'exploitation. Il est tellement facile de charger un cd dans l'ordinateur et de cliquer next-next-next! L'installation réussit et l'ordinateur démarre, qu'attendiez-vous d'autre? Mais on peut se poser la question si tout ceci garantit effectivement la fiabilité du système. La plupart des fabricants de systèmes d'exploitation ouvrent les portes toutes grandes, pour des raisons que l'on peut comprendre. Ce que l'utilisateur veut, en effet, c'est pouvoir installer son logiciel sans anicroches. Mais les cybercriminels exploiteront habilement ce point faible en implantant des maliciels dans votre ordinateur si facilement installé, à l'aide d'un virus ou d'un courrier 'hameçon' par exemple.

Si l'on veut installer un système d'exploitation de façon rigoureusement correcte, il faut prévoir un 'hardening' ou durcissement lors du processus d'installation. Le durcissement permet de sécuriser systèmes et/ou réseaux en paramétrant les différentes configurations (techniques). Un bon durcissement porte sur les serveurs, les composants de réseau actifs tels que parois coupe-feu et commutateurs, les ordinateurs portables et autres ainsi que l'appareillage mobile. Bref, toute la chaîne réseaux-systèmes d'automatisation. Le processus de durcissement désactive et/ou retire les fonctionnalités superflues des systèmes d'exploitation, des logiciels et du matériel. En attribuant des valeurs très spécifiques à certains paramètres, on réduit les risques de compromission d'un système, on améliore sa sécurité générale et on se défend efficacement contre les attaques de maliciels. Un bon exemple de l'utilité d'un durcissement est l'installation de Windows sur un ordinateur: ce faisant, on installe automatiquement des fonctionnalités telles que les accessoires de bureau ou Windows Mediaplayer, bien souvent superflues. Mais, une fois installées, elles augmentent les risques en matière de sécurisation du système. D'autre part, la désactivation de la fonction Autorun, l'introduction d'une politique de mots de passe sur le système, la limitation des infos disponibles sur les ports ouverts et autres mesures contribuent aussi à la cybersécurité. Et Windows n'est pas le seul système concerné; dans le cas d'Unix, on peut penser à la désactivation ou à la suppression de certains services superflus, tels qu'X11 ou Telnet daemon. Mais on peut également supprimer des comptes d'utilisateur superflus ou non employés, ou modifier des mots de passe standard présents sur certains systèmes. Tout ceci contribue indiscutablement à une meilleure sécurisation.

CIS Security Benchmarks

Reste à savoir ce qu'il faut exactement désactiver et/ou retirer. A ce sujet, des organisations comme le Center for Internet Security (CIS) publient régulièrement des Benchmarks, ainsi nommés. Les CIS Security Benchmarks sont des documents très utiles pour le paramétrage de systèmes et

applications dans le cadre d'un processus de durcissement. En plus du CIS, certains pouvoirs publics, banques ou autres grands employeurs d'ICT émettent leurs propres directives de durcissement. Nombreux sont aussi les fabricants de systèmes d'exploitation et de logiciels/matériels qui produisent des documents expliquant comment durcir leur produits.

Un sacré boulot

Le durcissement d'un système d'exploitation et de ses applications prend pas mal de temps. Il faut en effet examiner, régler et vérifier les paramètres un par un, et il y a souvent des centaines de ces paramètres. Mais le durcissement n'est aussi qu'un 'instantané' du système: l'installation ou la désinstallation d'un logiciel applicatif, par exemple, peut perturber complètement un système d'exploitation qui vient d'être durci. C'est surtout lors de la désinstallation qu'on court le risque de ne pas rétablir certains paramètres par oubli, ce qui met à nouveau le système en danger. On conseille donc de contrôler périodiquement le durcissement d'un système. Mais comme mentionné ci-dessus, le processus prend beaucoup de temps et la qualité de l'exécution dépend fortement du sérieux et de l'application de la personne en charge.

Il vaut donc mieux établir périodiquement un état automatisé du durcissement de vos systèmes. Des fabricants comme Easy2Audit, Lumension et Siemens proposent à cet effet des scanneurs automatisés qui scrutent les systèmes mais sans installer des logiciels, par exemple. Les résultats de ces interrogations/scrutations sont rassemblés dans un fichier et, ensuite, incorporés dans un compte-rendu d'état. Ces scanneurs disposent souvent de capacités de compte-rendu très étendues ce qui permet à leurs utilisateurs de démontrer aux auditeurs et organismes de surveillance qu'ils sont effectivement 'in control'.

Conclusion

Le durcissement est un processus important pour l'installation/configuration d'un ordinateur, ce qu'on a tendance à oublier. Un durcissement manuel prend peut-être beaucoup de temps mais peut vous éviter pas mal d'ennuis en matière de cybersécurité. Incorporez donc systématiquement cette technique dans vos processus d'installation et finissez-en avec cette habitude néfaste de cliquer next-next-next pour s'exclamer ensuite 'Chic, ça marche!'.

(Par Ronald Eygendaal)

Sources:

- **http://www.cisecurity.org/resources-publications/**
- **http://www.easy2audit.com/**
- **https://www.lumension.com/kb/Home/Endpoint-Security/874.aspx**