Méfiez-vous des supports mobiles

Virus. Une clé USB ou un CD-Rom qui traîne avec l'inscription «confidentiel». La tentation est forte de les brancher sur son ordinateur. Et d'ouvrir ainsi la voie au piratage.

À NOTER

Techniquement parlant, ces types de programmes malicieux peuvent prendre le contrôle d'un système d'exploitation mal protégé pour cause de négligence.

Ces programmes trafiqués peuvent modifier les droits de sortie, c'est-à-dire qu'un utilisateur pourrait être amené à envoyer des informations confidentielles à son insu.

PHILIPPE D. MONNIER

Comme le met en avant Claude Krähenbühl, directeur général de Navixia, jeune société vaudoise spécialisée dans la sécurité de l'information, «ouvrir un tunnel entre un hacker et une société cible est parfois un jeu d'enfants». Jacques Medina, security architect dans la même société, ajoute: «Il suffit de laisser traîner aux abords d'une entreprise choisie une clé USB ou un CD-Rom, si possible munis de l'inscription «confidentiel», pour attiser la curiosité.» Il y aura bien un employé imprudent qui ne résistera pas à la tentation d'insérer ses supports mobiles dans son ordinateur. Et comme ils contiennent des programmes malicieux s'exécutant automatiquement, le pirate s'est ouvert l'accès aux données de l'entreprise cible.
Une autre tactique pernicieuse est d'attirer un utilisateur sur un site Web dont le but est d'aspirer illicitement des données confidentielles.

Photomontage MA

PORTE. *Une simple clé USB peut servir de cheval de Troie.*

IMPRUDENCE. Les programmes malicieux subrepticement installés sur des supports mobiles sont comparables aux courriels munis de virus informatiques dissimulés dans les pièces jointes. En d'autres termes, la stratégie d'attaque est basée sur l'imprudence d'une petite minorité d'utilisateurs.
Il est toujours possible de renforcer la sécurité de manière drastique. Par exemple, un navigateur Web peut être configuré pour maximiser son niveau de sécurité. Le problème est que, en général, plus le niveau de sécurité est élevé, moins l'utilisation des outils informatiques est pratique pour les utilisateurs. Il faut donc trouver un compromis entre le niveau de sécurité et le confort d'utilisation.
Claude Krähenbühl souligne: «Il est souvent plus adéquat de sensibiliser les utilisateurs quant aux risques de sécurité que de rajouter une couche de logiciel.» Cela est d'autant plus vrai qu'une des méthodes préférées des hackers reste encore le recours à toutes sortes de subterfuges pour obtenir un mot de passe de la bouche même d'un utilisateur.
«Il importe de mettre en place un système de sécurité qui prenne en considération les besoins spécifiques des différents utilisateurs, explique encore Jacques Medina. Par exemple, une secrétaire n'aura pas forcément besoin d'utiliser de clé USB. Par conséquent, on réduira les risques en s'assurant que son ordinateur ne soit pas équipé de lecteur pour clé USB.»

ENCRYPTAGE. Mettre en place et gérer la sécurité de l'information n'est pas une sinécure, ce d'autant plus que l'utilisation de supports mobiles est en forte croissance. Selon Gartner Group, 47% des données corporate résident aujourd'hui sur des supports mobiles du type PDA, laptop, smartphone ou clé USB. Pour se protéger au mieux, il est conseillé d'utiliser des mots de passe temporaires, en plus de l'encryptage des données confidentielles et un accès réservé aux utilisateurs autorisés.
Techniquement, les supports mobiles apportent leur lot de complication. Les données se trouvent souvent sur des SD RAM au lieu d'être stockées sur les disques durs. En outre, il est difficile de prévoir quand et avec quel type de connexion l'utilisateur va se connecter au réseau de l'entreprise. Ce qui exige des solutions spécifiques, notamment pour la gestion des back-up.
Côté positif on note que, grâce aux connexions à distance, il est possible d'effacer automatiquement des données au cas où un support mobile aurait été dérobé. ■