

Contrôler les périphériques amovibles

La fuite des données

Les dispositifs de stockage amovibles ont désormais envahi l'entreprise sous de multiples formes : clés USB, disques durs externes, iPods, PDA, téléphones, appareils photos... La connectivité USB ou FireWire permet de transférer en quelques secondes des quantités massives d'information vers ces supports. Ces transferts sont furtifs, aucune trace ne permet aux responsables informatiques d'en rendre compte.

Les codes malveillants

Les dispositifs de stockage externes servent aujourd'hui de vecteur d'échanges de données – autorisés ou non - entre les postes de travail, aussi bien au sein de l'entreprise qu'à l'extérieur. Ces périphériques sont susceptibles de contenir des codes malveillants qui peuvent alors infecter tout poste sur lequel on les connecte. Malgré la robustesse des infrastructures de sécurité mises en place, seule une solution de sécurité embarquée au niveau du poste de travail permet de lutter efficacement contre cette menace.

Le détournement des infrastructures

Les capacités des dispositifs de stockage amovibles peuvent donner lieu à un détournement des infrastructures de communication. En utilisant l'accès très haut débit de l'entreprise, des employés indisciplinés téléchargent massivement de la musique ou des films piratés, puis les transfèrent à l'extérieur de l'organisation à l'aide de CD, DVD ou disques durs amovibles.

Contrôler les connectivités wireless

Les modes de connexion sans fil

Ces nouveaux modes de communication sur le réseau LAN (Wi-Fi) et PAN (Bluetooth) contribuent à l'essor du nomadisme en permettant aux utilisateurs de se connecter facilement au réseau en dehors de l'entreprise : à la maison, dans un hôtel ou un aéroport, chez un client ou un partenaire. Cette utilisation pose de multiples problèmes de sécurité : connexion à des bornes publiques et non cryptées, connexions simultanées au LAN de l'entreprise et à un réseau sans-fil voisin, utilisation du mode ad-hoc dans les connexions Wi-Fi, périphériques bluetooth détectables...

La maîtrise des points d'accès

Il est difficile de garantir que les bornes d'accès mises en place dans l'entreprise sont les seules auxquelles les collaborateurs ont accès. Les points d'accès non maîtrisés posent un problème de confidentialité pour le PC connecté à ce type de borne et un problème de sécurité globale : un PC connecté à la fois au LAN par le réseau Ethernet et au point d'accès par le réseau Wi-Fi peut servir de relais entre un attaquant externe et le réseau interne. La maîtrise des points d'accès à partir du poste de travail est l'un des éléments clé d'un réseau sans fil sécurisé.

La confidentialité des échanges

Il existe aujourd'hui plusieurs méthodes de cryptage et d'authentification sur les réseaux Wi-Fi. Si certains d'entre eux sont bien sécurisés (WPA, WPA2), d'autres ne le sont que très peu, voire pas du tout (WEP, Open). En laissant la possibilité à un collaborateur de se connecter sur des bornes extérieures, l'entreprise prend le risque de voir un poste se connecter à une borne qui ne sécurisera pas les échanges de données.

StormShield Device Control System est un module puissant et intelligent permettant de contrôler l'utilisation des périphériques de stockage de données amovibles. Grâce à sa technologie avancée, Stormshield DCS permet de distinguer finement et dynamiquement le type de media autorisé à fonctionner sur le poste de travail. StormShield Device Control System sécurise également vos PC en situation de mobilité, en contrôlant les connexions sans-fil. Connecté ou déconnecté de l'entreprise, vos informations sont protégées contre toute utilisation frauduleuse.

« Le contrôle des périphériques de stockage portables doit être appréhendé stratégiquement comme un canal de communication identique en terme d'impact aux services Internet »

Source : Gartner - Portable Storage Device Control Products, Worldwide, 2006

Fonctionnalités

- Contrôle des fonctionnalités de gravure de CD/DVD
- Contrôle des périphériques de stockage amovibles
- Gestion fine des droits d'accès aux périphériques de stockage amovibles
 - contrôle du périphérique en fonction du type, du modèle et du numéro de série
 - contrôle de l'accès, de la lecture et de l'écriture
 - surveillance du volume d'informations copiées
 - contrôle des droits en fonction des types de fichiers et par groupe de périphériques
 - Hot Plug Support
- Contrôle des classes de périphériques USB (stockage, scanners, souris...)
- Monitoring spécifique aux opérations sur les périphériques amovibles
 - audit des périphériques utilisés et des opérations effectuées
 - remontée des opérations bloquées par StormShield
 - configuration fine des niveaux de log afin d'optimiser le trafic réseau
- Contrôle de l'utilisation des périphériques Bluetooth
- Contrôle de l'utilisation des périphériques Wi-Fi
 - contrôle du mode ad-hoc
 - contrôle du mode d'authentification et de cryptage (Open, WEP, WPA, WPA2...)
 - contrôle des points d'accès (par SSID, adresse MAC...)
 - Politiques applicables dynamiquement en fonction du contexte
 - Port USB constamment disponible pour les besoins hors stockage

Vers une protection proactive, complète et inégalée

Parce que le poste de travail reste le talon d'Achille de toute organisation, il nécessite une sécurisation renforcée. Une politique de contrôle des périphériques de stockage

et des connexions sans fil doit s'accompagner de la mise en place de mécanismes de protection contre l'ensemble des menaces (virus, vers, spywares, chevaux de Troie, clés usb...). La vision technologique de SkyRecon consiste à intégrer des fonctionnalités complémentaires afin d'atteindre un niveau de sécurité maximal sur les postes client tout en évitant la multiplication des agents et des consoles d'administration.

StormShield apporte ainsi une protection optimale contre tous les types de menaces, sans base de signature, à travers une seule console d'administration et un seul agent sur le poste.

StormShield Security suite

- Chiffrement automatique des fichiers à la volée et/ou du disque dur entier
- Système proactif de prévention d'intrusion
- Host-IPS (incluant anti-keylogging et anti-buffer overflow)
- Anti-virus et anti-spyware
- Firewall réseau, système et applicatif
- Contrôle des accès aux applications
- Mise en conformité
- Contrôle des périphériques amovibles
- Protection Wifi
- Politique de sécurité contextuelle
- Monitoring de l'actualité du poste de travail

« StormShield de SkyRecon est une solution puissante et unique permettant de répondre à l'ensemble des problématiques de sécurité des postes de travail. »

Marc Jalabert,
Director of Business & Marketing Operations -
Microsoft France