

# **Périphériques de stockage amovibles : une menace réelle pour la sécurité des informations en entreprises**

**Tribune d'Alexei Lesnykh  
Responsable du Développement International et  
de la Stratégie Produit de DeviceLock**

*À vingt-neuf ans, Daniel Harrington, analyste dans une société internationale de services et d'ingénierie informatique, n'aurait jamais imaginé se retrouver au cœur d'un scandale qui retentirait jusqu'au gouvernement britannique. Fin octobre dernier, une unité de stockage amovible lui appartenant était retrouvée dans un parking public à proximité d'un pub dans la ville anglaise de Cannock. Cette affaire serait passée inaperçue si l'objet en question n'avait été utilisé pour stocker les mots de passe ultra-secrets permettant d'accéder à la base de données de services en ligne du gouvernement britannique.*

Outre la négligence, cet incident a mis en évidence une préoccupation majeure dans le secteur de la sécurité informatique, qui n'a cessé de s'intensifier au cours des dernières années : la diffusion de données confidentielles et sensibles n'a jamais été aussi simple. Les périphériques de stockage amovibles compliquent la tâche des professionnels de la sécurité.

## **Une problématique nouvelle : la sécurisation du patrimoine informationnel**

L'information est l'une des ressources les plus précieuses des entreprises. Tout comme les autres actifs vitaux, elle doit être protégée. Toute faille de sécurité à ce niveau peut entraîner des préjudices majeurs pour les entreprises concernées.

Depuis quelques années, le Ponemon Institute évalue ces dommages. Selon un rapport publié en 2008, le préjudice moyen résultant d'un incident isolé peut atteindre plusieurs millions de dollars. Les sociétés basées aux États-Unis sont les plus affectées : chaque brèche de sécurité informatique leur coûtant en moyenne 6,6 millions de dollars. Les sociétés anglaises et allemandes s'en sortent un peu mieux, chaque incident de ce type se traduisant respectivement par un préjudice moyen de 1,73 million de livres sterling et 2,41 millions d'euros<sup>1</sup>.

Cela représente beaucoup d'argent. Les fuites de données sont ainsi devenues l'une des premières priorités des services en charge de la sécurité en entreprises. Il semblerait cependant que la plupart des organisations n'adoptent pas la meilleure approche en la matière, se contentant souvent de sécuriser les voies de fuites potentielles qui sont loin d'être la cause première du problème.

---

<sup>1</sup> Ponemon Institute, « 2008 Annual Survey: Cost of a Data Breach. » (Rapports pour les États-Unis, le Royaume-Uni et l'Allemagne)

L'exemple le plus simple en est peut-être la focalisation générale sur la protection contre les « menaces extérieures », comme les logiciels malveillants (malware), le courrier publicitaire non sollicité (spam) et le piratage informatique. Si la réalité de ces menaces ne fait aucun doute, elles ne représentent, selon le Ponemon Institute<sup>2</sup>, pas plus de 7% du nombre total des incidents (aux États-Unis). La cause des 93% des failles de sécurité restantes est liée à des actions du personnel en place, en d'autres termes des collaborateurs disposant des droits d'accès à des informations confidentielles.

Les dispositifs de stockage amovibles actuels offrent un support idéal pour la fuite de données. Ils sont difficiles à contrôler (à la différence du courrier électronique, par exemple) et offrent généralement une capacité suffisante pour stocker tous types de données, y compris des informations sensibles.

## Quelques solutions

Chaque société doit commencer par déterminer si la valeur de ses données justifie une interdiction d'utilisation totale de dispositifs amovibles au niveau de ses points d'accès terminaux. En théorie, il est possible de désactiver tous les ports et les lecteurs des PCs avant leur remise aux employés. Ainsi, avant d'envisager une stratégie de protection des données stockées sur des clés USB, des téléphones intelligents capables de se synchroniser sur les postes de travail et d'autres types d'appareils mobiles à connectivité plug-and-play, il convient de se poser la question suivante : « Les avantages liés à l'utilisation de ces outils sont-ils supérieurs aux risques de fuite de données associés ? ».

À en juger par les pratiques actuelles, la plupart des entreprises ne souhaitent pas priver leurs collaborateurs de ces dispositifs, qui sont souvent synonymes d'augmentation de la productivité. Cela se comprend facilement : sans clé USB, il ne serait pas toujours possible d'animer une présentation ou de travailler occasionnellement depuis son domicile. C'est pour cette raison que les solutions radicales telles que la désactivation totale des ports physiques ou l'installation d'un matériel pour les rendre inopérants ne sont que très rarement utilisées, et seulement dans certains services où sont traitées des informations ultra-confidentielles. À la place, les entreprises préfèrent déployer des logiciels de protection reconnus pour leur efficacité et leur ergonomie.

## Systèmes de contrôle d'accès

Aujourd'hui, l'évolution des techniques de protection implique le déploiement de logiciels qui contrôlent les droits d'accès des utilisateurs aux ports d'ordinateurs et aux imprimantes, ainsi que les connexions locales entre les ordinateurs et les téléphones intelligents ou les assistants personnels. À la différence des mesures physiques qui bloquent radicalement l'accès, ces solutions permettent un contrôle « sur mesure » et centralisé des droits. À l'aide d'une console d'administration unique, le responsable de la sécurité détermine quels utilisateurs peuvent accéder à quels ports, sur quels ordinateurs et à quels moments de la journée. En outre, ces systèmes autorisent la mise en place de flux de travail qui facilitent l'octroi de droits d'accès pour des opérations spécifiques, à la demande des utilisateurs.

---

<sup>2</sup> Ponemon Institute, « 2008 Annual Survey: Cost of a Data Breach. » (Rapport pour les États-Unis)

Dès lors que le système de contrôle interdit à un utilisateur d'accéder à un port, une interface ou une imprimante spécifique, il n'y a plus de risque de dispersion de données. Dans les autres cas, une fuite est toujours possible, même s'il est facile d'en limiter les conséquences grâce à la réplication de données. Cette fonction (offerte par un nombre limité de solutions aujourd'hui disponibles) conserve une copie de toutes les données transférées vers une base de données centralisée. Ainsi, la personne en charge de la sécurité peut à tout moment vérifier quelles données ont quitté le système, sur chacun des canaux locaux de transmission.

La plupart des solutions utilisées pour gérer l'accès aux connexions et ports locaux permettent de définir des règles s'appuyant sur le type de données transmises. Un responsable de la sécurité peut ainsi configurer le système de façon à autoriser le transfert de certaines données (fichiers Microsoft Word, par exemple) sur des appareils mobiles, tout en bloquant d'autres types de documents (fichiers PDF, par exemple). En d'autres termes, le système ne contrôle pas seulement les opérations de transmission de données, il filtre également les types de données transférées.

## **Système DLP**

Cette fonctionnalité équipe notamment les systèmes de contrôle d'accès référencés comme « produits DLP » (Data Leak Prevention = prévention contre la fuite de données). Selon Rich Mogull<sup>3</sup>, expert reconnu dans le domaine de la sécurité, les systèmes DLP se caractérisent par une analyse approfondie du contenu des données sortantes. Les solutions de ce type déterminent la légitimité d'une opération donnée en utilisant des techniques de filtrage de contenus.

Les systèmes DLP sont prometteurs. Les principaux acteurs du marché de la sécurité informatique investissent d'ailleurs massivement dans le développement de ces technologies. Toutefois, en l'état actuel, il n'existe aucun système DLP vraiment complet et capable de surveiller les données transmises via des ports locaux vers des dispositifs amovibles. En voici les raisons principales.

Tout d'abord, les techniques actuelles de filtrage de contenus n'empêchent pas complètement les erreurs de type « faux positifs » (blocages intempestifs) et « faux négatifs » (opérations autorisées qui n'auraient pas dû l'être). La précision du filtrage de contenus atteint ainsi difficilement un niveau compris entre 80 et 85 %.

En second lieu, l'analyse de contenus en profondeur est un processus très exigeant en ressources. Lorsqu'un courrier électronique est envoyé, les systèmes DLP interceptent le message et l'analysent au niveau du serveur SMTP, qui dispose toujours de la puissance de calcul requise. Mais si ces données sont copiées localement, cette approche devient naturellement impossible.

C'est pourquoi les développeurs de systèmes DLP doivent faire un compromis : soit le système envoie des répliques des données vers le serveur et attend sa décision, soit il les analyse localement. Le premier cas suppose un trafic considérable sur le réseau, d'où des retards conséquents (temps nécessaire au transfert d'un film en haute définition via le réseau, par exemple). Dans le second scénario, c'est la qualité de l'analyse qui est compromise : comme aucun ordinateur personnel ne dispose d'assez de puissance pour gérer ce type de processus, il faudrait utiliser un algorithme plus simple, et donc moins fiable, pour analyser les données.

---

<sup>3</sup> Livre blanc : « *Understanding and Selecting a Data Loss Prevention Solution* »  
<http://securosis.com/reports/DLP-Whitepaper.pdf>

Mais une autre raison (étroitement liée à la première) rend difficile l'utilisation des systèmes DLP pour la gestion des ports locaux. En raison des exigences inhérentes au filtrage de contenus, les systèmes DLP ont été initialement conçus comme des solutions de passerelle, ce qui explique pourquoi leurs composants agents n'ont pas encore atteint un niveau de maturité suffisant. Bien sûr, ils sont capables de filtrer des données. Mais, les capacités de contrôle de tous les types de ports et de canaux présentant des risques de fuite de données. De même, la flexibilité des règles DLP locales sur les ordinateurs terminaux, sont toujours moins probantes que sur des systèmes de passerelle bien conçus qui filtrent le contenu des communications réseau.

## **Systemes IRM**

Outre les systèmes de contrôle d'accès des ports / périphériques et les systèmes DLP, il existe une autre méthode de protection, souvent délaissée par les spécialistes. Les systèmes de gestion des droits relatifs à l'information, également appelés « systèmes IRM » (pour Information Rights Management), ne limitent d'aucune manière l'utilisation des dispositifs de stockage amovibles tout en parvenant à réduire de manière significative les risques de fuite de données.

Les systèmes IRM standard sont basés sur 2 mécanismes : le balisage de confidentialité et le chiffrement. Chaque fichier protégé par un système IRM est placé dans un conteneur chiffré et associé à une balise spéciale définissant les droits d'accès à ce fichier. Ainsi, dans un système IRM, même si le conteneur en question finit par sortir du réseau, il sera inutilisable à moins de disposer des droits d'accès au document.

En matière de gestion des données transférées vers des dispositifs de stockage amovibles, cette approche équivaut plus ou moins au chiffrement obligatoire des données exportées sur des unités amovibles, souvent utilisé par des systèmes contrôlant les droits d'accès aux ports et aux périphériques. Les solutions de type IRM permettent aux utilisateurs d'exporter des données confidentielles uniquement si elles sont chiffrées, ce qui signifie que les données d'une entreprise sont toujours protégées contre les fuites accidentelles, mais rarement contre les attaques malveillantes. En outre, l'efficacité des systèmes IRM est étroitement liée au nombre de fichiers balisés et aux types de modifications que les utilisateurs sont autorisés à exécuter. Dans la pratique, le balisage des fichiers revient à classer toutes les données d'une entreprise, un processus très gourmand en ressources et en temps.

## **Conclusion**

Nous sommes encore très loin de la situation idéale où seules des données personnelles ou publiques pourraient être copiées sur des unités de stockage amovibles. Les méthodes utilisées pour se protéger contre les menaces liées à de tels périphériques devront permettre d'établir un compromis entre convivialité, sécurité et coût de la solution. Les systèmes DLP à base de filtrage de contenus souvent cités ne sont pas encore capables de résoudre le problème des fuites de données locales au niveau des ordinateurs des employés, ce qui explique pourquoi ils restent de facto une solution de niche.

En l'état actuel des choses, les méthodes de protection les plus efficaces (qui sont aussi souvent les plus fiables et les plus économiques) consistent à mettre en place des systèmes de contrôle simples d'accès, offrant des capacités de contrôle contextuel complètes et des fonctions élémentaires, mais optionnelles, de filtrage de contenus. Ces solutions s'attaquent au cœur des problèmes de sécurité liés aux dispositifs mobiles et répondent à la plupart des besoins des entreprises.

### A propos d'Alekei Lesnykh



Responsable du développement international et de la stratégie produit de DeviceLock, Alexei Lesnykh a rejoint la société en 2007. Avec plus de 10 ans d'expérience en sécurité informatique, son expertise s'étend à de multiples domaines : la sécurité des réseaux, les infrastructures publiques, la gestion de l'authentification et de l'identification ainsi que la voix sur IP et le calcul virtuel.

Avant de rejoindre DeviceLock, Alexei Lesnykh était analyste indépendant, contribuant au développement de stratégies d'entreprises et de produits et travaillant à la mesure des risques d'investissement pour le compte de sociétés internationales. Ses expériences précédentes l'ont conduit à prendre part au développement à l'international de start-up russes : TrustWorks Systems B.V. ou ELVIS-PLUS, par exemple.

Alexei Lesnykh est titulaire d'un Master en sciences informatiques obtenu à l'institut des technologies électroniques de Moscou.

### À propos de DeviceLock Inc.

Depuis sa création en 1996, DeviceLock Inc. (précédemment connu sous le nom de SmartLine Inc.) fournit le logiciel de sécurité pour points d'extrémité DeviceLock® aux entreprises qui utilisent les technologies Microsoft. DeviceLock® est actuellement installé sur plus de 4 millions d'ordinateurs dans plus de 58 000 entreprises du monde entier, comme des institutions financières, des opérateurs de télécommunications, des administrations locales et nationales, des réseaux militaires sécurisés et des établissements d'enseignement. DeviceLock Inc. est une entreprise internationale qui possède des bureaux aux Etats-Unis (en Californie à San Ramon), au Royaume-Uni (à Londres), en Allemagne (à Ratingen), en Russie (à Moscou) et en Italie (à Milan). Pour obtenir plus d'informations, consultez le site [www.deviceclock.com/fr](http://www.deviceclock.com/fr).

DeviceLock et le logo DeviceLock sont des marques commerciales déposées de DeviceLock, Inc. Palm® est une marque commerciale de Palm, Inc. Windows Mobile® et Windows Active Directory® sont des marques commerciales de Microsoft Corporation, déposées aux États-Unis et dans d'autres pays. Tous les autres noms de produits, marques de service et marques commerciales sont des marques de leur propriétaire respectif.

### Contact presse :

Mediasoft Communications – Emmanuelle Bureau du Colombier  
[Ebdc@mediasoft-rp.com](mailto:Ebdc@mediasoft-rp.com) - 01 55 34 30 00