

## La Menace Intérieure

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

« Les technologies ont considérablement évolué, impactant fortement les entreprises, leurs équipes et leurs méthodes de travail. Nous sommes désormais ultra-mobiles ... les ordinateurs portables ont remplacé les postes de travail fixes ... les connexions à Internet se font via des réseaux sans fil accessibles presque partout ... et n'importe quel téléphone intelligent peut pratiquement tout faire.

Il n'y a pas si longtemps, les affaires se concluaient rarement ailleurs qu'au bureau. Un employeur n'éprouvait aucune difficulté à assurer le suivi de ses équipes. Il savait que tous ses actifs, et notamment les informations confidentielles, demeuraient parfaitement protégés sous un seul toit.

Aujourd'hui, les entreprises agissent à l'international. Les équipes travaillent à distance, dotées de nombreux périphériques et autres gadgets, capables de stocker de nombreuses données, de l'album souvenir des dernières vacances à la base de données clients.

Cette mobilité a un coût : l'insécurité. Les mécanismes de contrôle d'accès aux réseaux et les solutions antivirales actuelles ne suffisent plus à assurer la sécurité des données.

La mobilité, sous toutes ses formes et avec toutes ses composantes, fait courir à l'entreprise un sérieux risque sécuritaire, qui ne fait que croître...

Les réseaux informatiques deviennent beaucoup trop vulnérables face aux menaces posées par l'élément qu'ils essaient d'intégrer à tout prix : le périphérique distant. La prolifération des téléphones portables intelligents, des assistants personnels et des clés USB implique concrètement que la plupart des collaborateurs d'une entreprise utilisent désormais des périphériques professionnels et personnels pour stocker des quantités énormes de données, parfois éminemment confidentielles.

Comment les responsables informatiques peuvent-ils alors gérer les problèmes de sécurité posés par ces nouvelles habitudes ?

### ***L'évaluation de vulnérabilité***

Il est important d'identifier avec précision les services de l'entreprise utilisant régulièrement des périphériques de stockage mobiles. Des plans d'action précis pourront alors être définis en conséquence.

### ***La politique de protection***

Les fuites de données peuvent être accidentelles ou intentionnelles. Il est donc indispensable de sensibiliser les collaborateurs à l'importance de la protection des données et aux implications légales liées à un détournement ou à un vol.

### ***La réduction et la limitation de l'accès aux données***

Être capable de définir qui accède à quelle information permet de mieux contrôler le mouvement des données stratégiques. Plus une donnée est simple à copier, plus il est difficile d'en assurer la confidentialité et la sécurisation. Il est donc primordial d'accorder les bons niveaux d'accès aux bonnes personnes. Le chiffrement des données sur les périphériques mobiles est également une mesure qui peut s'avérer très utile.

### ***Le contrôle des données***

Aux Etats-Unis, par exemple, de nombreuses entreprises ne permettent plus à leurs collaborateurs de pénétrer dans les locaux avec des périphériques personnels disposant d'une capacité de stockage. Cette pratique est de plus en plus courante, mais elle ne résout pas tous les problèmes. En fait, l'investissement dans certaines technologies visant à contrôler les données et à empêcher leur copie ou leur impression sans trace doit être un élément incontournable de toute stratégie de protection contre les pertes ou les vols de données.

Grâce aux outils de sécurisation des données aux points de connexion, les entreprises peuvent permettre à leurs équipes d'emporter des données sensibles sur leurs ordinateurs portables ou leurs clés USB sans pour autant en pénaliser la facilité d'accès. Ces outils offrent aux directions informatiques l'équilibre parfait qu'elles recherchent. L'utilisateur exige un accès simple et rapide, alors que son service informatique revendique une sécurisation totale ... deux visions difficilement compatibles avec les exigences actuelles. L'ajout d'une authentification par mot de passe permet de contrôler l'identité des personnes accédant à certains systèmes. Un logiciel de sécurisation des périphériques permet de son côté de protéger les données contre toute tentative de vol de matériel ou d'attaque via un port USB.

Ce n'est pas tant l'adoption de ces périphériques et autres gadgets qui pose un problème aux responsables de la sécurité informatique, c'est plus la manière dont ils sont utilisés. Il est donc absolument indispensable de sensibiliser les équipes à la nécessité de modifier leurs habitudes, afin qu'elles se conforment à un ensemble de mesures de sécurité : sécurisation des périphériques, authentification multi-facteurs, voire technologies de pistage – à la James Bond – pour les plus distraits... »

***A propos d'Alexei 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 3 millions d'ordinateurs dans plus de 55 000 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