DeviceLock

Fuite de données : une question de discipline ?

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

Les préjudices occasionnés par la fuite de données dans les entreprises ne cessent de croître à travers le monde. Cette tendance se développe même sur le marché des PME. Selon l'enquête consacrée par Symantec à la protection des informations des PME en 2010[1], celles-ci placent les fuites de données en tête de toutes les menaces pour leur activité. En France, l'étude menée par l'Institut Ponemon sur les fuites informatiques en 2009 estime que le coût de chaque dossier compromis s'élève en moyenne à 89 euros. 3 principaux facteurs viennent accentuer cette tendance.

Une tendance alarmante

Le premier tient à la prolifération en entreprise des terminaux mobiles et des applications destinés au grand public, tels que les smartphones, les tablettes Internet ainsi que les logiciels Web 2.0. Dans le même temps, il ne fait aucun doute que les médias sociaux, les réseaux peer-to-peer, la messagerie instantanée, les blogs et le Webmail ont fait la preuve de leur grande efficacité dans une économie moderne centrée sur Internet. Du reste, ces outils se sont d'ores et déjà imposés comme incontournables dans l'environnement professionnel. Cependant, du point de vue de la sécurité des informations, ils créent de nouveaux risques de fuites de données contre lesquels ni les solutions classiques de sécurisation des réseaux, ni les anti-virus ne peuvent lutter. De même qu'au début de cette année, de vastes fuites de données dues à un usage inapproprié du partage de fichiers P2P ont été découvertes par la Federal Trade Commission dans près d'une centaine d'entreprises américaines[2].

Deuxième facteur, ces dix dernières années, les vecteurs de menaces externes pour la sécurité informatique des entreprises ont changé : plutôt que de cibler les infrastructures informatiques, il s'agit désormais de chasser les données et, plus précisément, les données de valeur. Le cyber-crime s'est parfaitement bien organisé et dégage aujourd'hui un chiffre d'affaires annuel de l'ordre de mille milliards de dollars[3]. Autre aspect important, les cyber-menaces modernes visent plus souvent les postes de travail, car ceux-ci sont moins bien protégés que les serveurs et renferment de grandes quantités d'informations personnelles ou professionnelles. Les attaques externes gagnent en complexité, combinant non seulement des technologies logicielles et réseau de pointe, mais aussi toute la puissance de l'ingénierie sociale pour infecter les postes avec des programmes malveillants (*malwares*). Il suffit d'un clic imprudent sur un lien dans un spam pour qu'un poste de travail se retrouve contaminé par un programme capable d'intercepter les données issues d'une recherche dans la mémoire tampon, et de les mettre subrepticement de côté afin de les envoyer ultérieurement.

[1] Symantec 2010 Global SMB Information Protection Survey (http://bit.ly/aFfMqj)

[2] Widespread Data Breaches Uncovered by FTC Probe (www.ftc.gov/opa/2010/02/p2palert.shtm)

[3] Fatal System Error, Joseph Menn, janvier 2010 (http://fserror.com/)

Enfin, le troisième facteur est d'ordre humain. Les fautes professionnelles ou les actes de négligence représentent une phase essentielle de la plupart des scénarios de fuite de données sur les postes de travail. En dépit des règlements et des chartes, des formations spéciales, des sanctions et des pénalités administratives, la nature humaine est immuable : même les collaborateurs les plus loyaux continueront de commettre des erreurs par inadvertance, les curieux de mettre leur nez là où ils ne devraient pas, et les employés indélicats de rechercher délibérément des informations de grande valeur. C'est pourquoi, la discipline en matière de communication de données et de sécurisation du stockage sur les postes de travail doit être assurée par des moyens qui ne dépendent pas de la nature humaine, à savoir un outil qui autorise de manière transparente toutes les actions des utilisateurs sur la base de leurs fonctions et qui peut bloquer toute tentative accidentelle ou délibérée d'intervention en dehors de ce cadre prédéfini.

C'est exactement le but des solutions de prévention des fuites de données (DLP, Data Loss Prevention) sur les postes de travail. Celles-ci ont pour principale finalité la mise en œuvre précise du principe de « moindres privilèges » lors de l'octroi aux utilisateurs de droits pour les opérations de transfert et de stockage de données sur le poste de travail. Par conséquent, les solutions DLP pour les postes de travail éliminent par anticipation tous les scénarios de fuite de données liées à des autorisations excessives accordées aux salariés. Du point de vue de la gestion des risques, cela a pour effet immédiat de réduire le risque de voir des informations sensibles circuler sans contrôle à partir des ordinateurs de l'entreprise, que ce soit par suite de simple négligence ou de malveillance.

La capacité d'analyser le contenu des communications permises et de filtrer les données non autorisées est une autre caractéristique des solutions DLP, qui accroît nettement leur efficacité en tant qu'outil destiné à faire respecter une discipline de sécurité sur les postes de travail. Elles ne se bornent pas seulement à bloquer les opérations et données restreintes, mais elles tiennent également à jour des enregistrements détaillés et – si nécessaire – des copies au sein d'une base de données centralisée, disponible à des fins d'audits de sécurité et d'investigations en cas d'incident. En dehors de l'objectif premier (repérer, identifier et sanctionner les collaborateurs négligents ou malveillants), cette fonctionnalité incite implicitement mais fortement le personnel à ne pas enfreindre les règles en place pour la sécurisation des données. Dès lors que chacun sait que les communications et transferts de données à partir de son poste sont surveillés et enregistrés, le fait de « se sentir observé » développe dans le subconscient une certaine autodiscipline, une sorte d'« agent DLP » interne, qui protège souvent les données des entreprises avec davantage de fiabilité que les technologies les plus élaborées. Cette autodiscipline ajoute une dimension notable – bien qu'intangible – aux solutions DLP et double leurs performances. En particulier, la fiabilité d'un système DLP est également accrue du fait que l'« agent DLP » interne est actif en permanence et supplée virtuellement le système en cas de panne ou de maintenance.

Dans le domaine de la sécurité des informations, la fuite de données et le manque de discipline sont donc si intimement liés en termes de contexte, de processus et d'impact qu'une solution qui neutralise l'un des ces deux aspects a pour conséquence d'atténuer l'autre. En jouant sur les mots, il serait possible de faire dire au sigle DLP « Discipline Loss Prevention » afin de conseiller aux responsables de la sécurité informatique de s'intéresser de près aux aspects discipline et auto-discipline des solutions DLP à tous les stades d'un projet DLP. Par-dessus tout, cela les aiderait également à répondre aux attentes de la direction et des utilisateurs, ainsi qu'à évaluer avec réalisme et interpréter correctement les résultats du projet.

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 sous le nom de SmartLine, DeviceLock, Inc. fournit des solutions logicielles de contrôle et de protection des informations en entreprises de toutes les tailles et tous les secteurs d'activité. Avec plus de 4 millions d'ordinateurs protégés dans plus de 60 000 organisations de par le monde, DeviceLock compte une vaste clientèle institutionnelle, parmi laquelle des établissements financiers, des organismes publics nationaux et fédéraux, des réseaux militaires classés, des prestataires de soins de santé, des entreprises de télécommunications et des établissements scolaires. DeviceLock, Inc. est une société internationale comptant des agences à San Ramon (Californie, États-Unis), Londres (Royaume-Uni), Ratingen (Allemagne), Moscou (Russie) et Milan (Italie).

Contact presse :

Mediasoft Communications – Carole Scheppler
Carole.scheppler@mediasoft-rp.com - 01 55 34 30 00