

La sécurisation des terminaux informatiques : le remède aux menaces sur les données des entreprises

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

L'environnement des entreprises devenant de plus en plus dynamique, mobile et distribué, une grande quantité d'informations confidentielles, dont des données client privées, sont créées, utilisées et stockées sur les ordinateurs de bureau et portables des employés. Et, la popularité des systèmes de stockage amovibles, tels que les clés USB et les cartes mémoire, n'a cessé de croître. Ces accessoires sont désormais plus abordables, portables et dissimulables. Ils offrent aussi une capacité de stockage et une vitesse de téléchargement suffisantes pour faciliter le vol ou la perte de gros volumes de données, de très grande valeur, en quelques instants.

Autre facteur contribuant à l'augmentation des brèches internes, les employés maîtrisent désormais un certain nombre de méthodes simples (et donc potentiellement dangereuses) qui facilitent la fuite des données à partir des ports locaux de leur poste de travail. Lorsqu'ils ne disposent pas des équipements nécessaires pour copier des données d'un ordinateur vers une mémoire flash ou un autre système *plug-and-play* standard, ils peuvent envisager de synchroniser les données entre leur PC et leur système mobile personnel (PDA) ou leur smartphone. Ensuite, il reste la bonne vieille méthode consistant à imprimer des documents sensibles et à les sortir de l'entreprise.

Dans la mesure où ces fuites locales n'utilisent pas les communications réseau, les mécanismes de protection traditionnels (pare-feu, systèmes de détection d'intrusion et de prévention, filtrage des e-mails et du contenu Web) ne permettent pas de les prévenir. Ces fuites créent une faille considérable dans le système habituel de protection des informations : les systèmes réseau de prévention contre la fuite des données (DLP). Les entreprises recherchant une technique d'immunisation contre les menaces internes doivent comprendre que, si ces systèmes tant vantés sont efficaces pour filtrer le contenu des applications et services de communication réseau (e-mails, messagerie instantanée, réseaux *peer-to-peer*, etc.), ils sont impuissants face aux fuites de données intervenant au niveau des terminaux informatiques. Même si les entreprises dépensent des centaines de milliers d'euros pour mettre sur pied une solution DLP complète, les employés pourront toujours subtiliser des informations via une clé USB, un smartphone ou une simple copie imprimée contenant des données de valeur.

Nouvelle protection nécessaire : agents DLP au niveau des terminaux informatiques

Bien qu'il soit facile de démontrer l'inefficacité d'une approche centrée « sur le réseau » en matière de sécurité des données d'entreprise, force est de constater que cette approche reste pourtant largement utilisée en pratique. Cette situation devrait changer dans la mesure où des études révèlent que les brèches de sécurité via des ports ou des périphériques locaux (mémoire amovible, synchronisation avec des smartphones, impression de documents) sont bien plus courantes que celles qui ont lieu sur les canaux en réseau (e-mail, messagerie instantanée, P2P), en particulier dans la mesure où ces canaux sont isolés des utilisateurs internes du fait des contrôles au niveau du réseau.

Les statistiques rassemblées à partir de plusieurs études de marché, dont le rapport « 2008 Annual Study: Cost of a Data Breach » (Étude annuelle 2008 : Coût d'une brèche de sécurité des données) réalisée par le Ponemon Institute¹, confirme cette situation. Cette étude établit clairement que dans le monde entier, le coût des brèches de sécurité supportées par les entreprises ne cesse d'augmenter.

Par conséquent, les professionnels de la sécurité informatique et les dirigeants des entreprises sont de plus en plus convaincus de la nécessité d'installer des agents de surveillance complets directement sur les terminaux informatiques pour en assurer la protection, la plupart des solutions DLP étant incomplètes et favorisant les fuites.

Des agents DLP locaux, pour une protection essentielle au niveau des terminaux informatiques

Cet état de fait prouve que l'approche consistant à attendre la solution DLP hybride idéale (réseau + terminaux informatiques) semble malavisée pour traiter un mal interne déjà déclaré. Il ne fait aucun doute que les fonctions et la qualité des agents DLP « locaux » (c'est-à-dire placés au niveau des terminaux informatiques) seront d'une importance capitale et qu'ils intégreront les trois principales tendances technologiques qui dominent actuellement toutes les discussions sur les systèmes DLP, à savoir les filtres de contenu, les mécanismes de contrôle d'accès contextuels et le cryptage. Il est donc prudent d'établir une stratégie reposant sur des solutions de pointe dans chacun de ces domaines, à l'instar des logiciels de sécurité éprouvés actuellement sur le marché.

Filtrage de contenu

Modélisés sur la façon dont les humains identifient et trient des informations (généralement des documents texte), les filtres de contenu sont destinés à reconnaître des modèles de données, à interroger des données structurées et à noter le statut de confidentialité des données, puis à en autoriser ou à en interdire l'accès en fonction des profils utilisateur établis. Comme de tels mécanismes s'adaptent parfaitement au modèle prédominant de sécurité des informations centré sur les données, certains experts affirment que le filtrage de contenu offre le moyen le plus efficace et le plus autonome pour la protection contre les brèches de données, y compris celles perpétrées au niveau des terminaux de l'entreprise. Cependant, dans la pratique, même les technologies de filtrage de contenu les plus avancées s'avèrent insuffisantes par rapport à cet objectif, en particulier les filtres de contenu des agents dédiés aux terminaux informatiques. Ces filtres se situent loin derrière les fonctionnalités et les performances de leurs équivalents réseaux, avec qui ils partagent néanmoins les mêmes risques d'erreurs, tels que les faux négatifs ou les faux positifs. La précision de ces systèmes dépasse rarement 80 à 85 %. Et, le temps constant d'ajustement et de correction consacré par les administrateurs et les utilisateurs de bonne foi ne s'améliore pas. Pour être réellement reconnues sur le marché, les capacités de filtrage de contenu au niveau des terminaux informatiques devront être améliorées, en commençant par deux défis évidents : une meilleure adaptation à la nature distribuée des terminaux informatiques actuels et la prise en compte de la différence fondamentale entre les protocoles de transfert de données via les ports locaux et via les canaux du réseau.

¹ Ponemon Institute, « 2008 Annual Survey: Cost of a Data Breach. » (Études portant sur les États-Unis, l'Allemagne et le Royaume-Uni)

Contrôles contextuels des ports et périphériques

Il semble évident que pour produire des agents DLP locaux de haute qualité, les technologies de filtrage de contenu ne sont tout simplement pas suffisantes. Elles doivent être associées aux composants d'un second type de solution de prévention contre la fuite des données sur les terminaux informatiques : les logiciels de contrôle des ports et périphériques. Il existe aujourd'hui plusieurs solutions de gestion et de contrôle d'accès aux ports et périphériques qui utilisent des fonctions de vérification du contexte pour couvrir la plupart des vulnérabilités associées aux terminaux informatiques. Certaines de ces solutions ont été éprouvées sur le terrain depuis plus de dix ans.

Selon la définition donnée par Forrester Research², les technologies de contrôle des ports et des périphériques des terminaux informatiques représentent une classe des mécanismes DLP contextuels qui ne basent pas l'analyse et le filtrage sur le contenu des données, mais sur un ensemble de paramètres définissant l'environnement immédiat des données. Ces outils identifient notamment « qui » accède aux données (l'identifiant de l'utilisateur ou du groupe), « leur point de départ et leur destination » (interfaces, ports, classes de périphériques, types de périphériques et identifiants de périphériques uniques), « quand » (le moment), « où » (localisation du terminal informatique et vérification de sa connexion ou pas à un réseau protégé) et « dans quel format » (par exemple, le type de fichier) ces données sont consultées, etc. Une stratégie de protection viable contre les fuites au niveau des terminaux informatiques devrait commencer par la mise en place d'outils de contrôle contextuel éprouvés, puis se poursuivre avec l'ajout d'agents de filtrage de contenu au niveau des terminaux informatiques, à mesure que des versions fiables sont disponibles. Les deux technologies ne sont pas en conflit et ne se chevauchent pas, mais se complètent sur des couches différentes pour fournir une « protection en profondeur ».

Dans le futur, les agents DLP locaux devront fournir un contrôle contextuel sur les flux de données pour *l'ensemble* des canaux de communication possibles. En d'autres termes, ils devront couvrir les trois canaux locaux déjà couverts par les meilleurs programmes de contrôle des ports et périphériques :

- Clés USB, cartes de mémoire flash et autres dispositifs mémoire *Plug-and-Play* standard (lecteurs MP3, appareils photo numériques, etc.) ;
- Synchronisations de données quotidiennes entre les terminaux informatiques et les smartphones et PDA connectés localement (par exemple Windows Mobile, iPhone, Palm, Blackberry) ;
- Canaux d'impression de documents (contrôle du spoleur d'impression local/réseau, imprimantes virtuelles) ;

Et ils devront fournir un contrôle contextuel des communications réseau :

- Données échangées via des applications réseaux très répandues — e-mail, messagerie instantanée, FTP, Web, réseaux sociaux, partage de fichiers P2P, etc.

Outre le contrôle de tous les types de canaux de transmission des données, le composant de contrôle des ports et périphériques d'une solution DLP locale complète doit pouvoir contrôler (c'est-à-dire *intercepter, analyser, filtrer* et *consigner*) les opérations réalisées sur les données d'un ordinateur à tous les principaux niveaux contextuels : ports locaux/interfaces, périphériques, canaux de sélection des données et types de données (par exemple, les formats de fichiers).

² The Forrester Wave: Data Leak Prevention, 2nd trimestre 2008
(http://www.forrester.com/rb/Research/wave%26trade%3B_data_leak_prevention%2C_q2_2008/q/id/45542/t/2)

Avec une technologie de contrôle des ports et périphériques de haute qualité, il devrait également être possible de contrôler la direction du flux de données, quelles actions doivent être consignées et quelles données doivent faire l'objet d'un cliché instantané pour une analyse plus approfondie.

Pour répondre rapidement aux attentes de leurs clients en matière de protection optimale contre les fuites au niveau des terminaux informatiques, certains fournisseurs de systèmes de sécurité réseau ont cherché à compléter leurs outils réseau avec des agents DLP locaux offrant un contrôle contextuel limité, c'est-à-dire couvrant uniquement un ou deux canaux de fuite. Ils ont essayé de promouvoir ces solutions comme étant « complètes » parce qu'elles intégraient un module de filtrage de contenu. Mais cela revient à protéger une maison en ajoutant des verrous sur une porte et en négligeant les autres entrées possibles. Les données peuvent facilement être volées. Il suffit d'une porte à l'arrière laissée ouverte à l'utilisateur.

Cryptage

Il est illusoire de penser que des technologies de cryptage constituent à elles seules une solution de contrôle d'accès complète. Bien qu'il existe des mécanismes de protection très fiables pour les « données au repos » (ou DAR - *Data at Rest*) et les « données en mouvement » (ou DIM - *Data in Motion*), les solutions de cryptage ne peuvent pas protéger les « données en cours d'utilisation » (ou DIU - *Data In Use*). Le mode DIU implique en effet que les données soient décryptées et accessibles aux utilisateurs et aux applications. Cependant, il ne fait aucun doute que les composants de cryptage des supports amovibles — et, dans le futur, les composants de cryptage des objets de données — devront soit être intégrés aux agents DLP locaux, soit être complétés en intégrant les opérations effectuées sur ces terminaux. Le but de cette intégration serait d'associer logiquement cryptage, contrôle du contenu et contextualisation dans une stratégie globale de protection de données. Ainsi, les agents seront capables de spécifier les types ou éléments de données à crypter avant stockage sur des supports amovibles ou envoi sur des canaux de communication.

Quelle protection ultime ?

Un mélange équilibré de toutes les technologies évoquées ci-dessus (filtrage de contenu, contrôle des ports et périphériques et cryptage), probablement réalisé à l'origine en regroupant les meilleurs produits puis en évoluant vers une solution DLP intégrée de contrôle des terminaux informatiques, permettra d'obtenir une protection véritablement efficace contre l'épidémie mondiale de « menaces internes » et de réduire les dommages subis par les entreprises du fait des brèches de données provoquées par la négligence d'utilisateurs et les actions malveillantes.

Au final, les agents DLP locaux auront autant d'importance dans les stratégies DLP que les systèmes DLP réseau. Tout d'abord, ils contrôleront les canaux locaux de transmission de données qui ne peuvent pas être contrôlés à partir du réseau (par exemple, la copie des fichiers sur un support amovible). Ensuite, ils pourront exécuter le filtrage de contenu du trafic pour les terminaux informatiques qu'ils protègent, améliorant ainsi notablement les performances des systèmes DLP basés sur le réseau. Ils augmenteront donc de ce fait la portée de la solution tout en maintenant son faible coût. En fait, lorsque des agents DLP locaux complets seront en place, ils assureront la plus grande part du traitement DLP et contrôleront toutes les opérations d'entrée et de sortie de données opérées au niveau des terminaux informatiques de l'entreprise, tandis que les systèmes DLP réseau garantiront la majeure partie des fonctions (tout aussi importantes) de support et d'exécution de la solution DLP hybride globale.

Cependant, en dépit d'une publicité massive et d'une définition erronée du DLP, ce scénario « DLP hybride intégré Terminaux informatiques + Réseau/terminaux informatiques » n'existe tout simplement pas sur le marché actuel. Face à ce constat, il est préférable de continuer à utiliser les composants les meilleurs et les plus abordables pour se protéger autant que possible, en attendant le jour où ce « Graal sacré » (et le budget informatique qui l'accompagne) verront le jour.

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.

Contact presse :

Mediasoft Communications – Carole Scheppler

Carole.scheppler@mediasoft-rp.com - 01 55 34 30 00

DeviceLock et le logo DeviceLock sont des marques commerciales déposées de DeviceLock, Inc. Tous les autres noms de produits, marques de service et marques commerciales sont des marques de leur propriétaire respectif.