

SÉCURITÉ DU POSTE DE TRAVAIL

Le problème se situe entre la chaise et l'écran !

Le titre de cet article vient d'un aphorisme fort employé par les responsables de la sécurité informatique aux États-Unis. Il a pour finalité de démontrer que malgré tous les outils que l'on peut mettre en place, le maillon faible est l'utilisateur. Comble de malchance, celui-ci devient le maître du jeu en apportant dans l'entreprise, ses usages, ses matériels. La tendance est plutôt de suivre et de contrôler ses faits et gestes plutôt que de lui interdire certaines actions.

Stefan Tanase, un chercheur du laboratoire de recherche sur les attaques de Kaspersky, ne l'indique pas seulement ironiquement : « Vous devez élever votre niveau de paranoïa au plus haut niveau. » Ce niveau de paranoïa doit en fait être en rapport avec les pratiques des utilisateurs dans les entreprises. Pour beaucoup leur comportement est assez déplorable avec des smartphones jailbreakés laissant des failles de sécurité béantes ou encore des transferts des données d'entreprises sur leur messagerie personnelle pour travailler le soir ou le week-end. Bref, la plupart des comportements de l'utilisateur sont susceptibles de

donner des boutons aux RSSI. Sensibilisation et formation sont souvent un point de départ intéressant. Un autre est de pouvoir responsabiliser l'utilisateur et de s'appuyer sur des outils dont l'utilisateur comprend l'utilité et qu'il ne le vive pas comme une contrainte, ce qui entraverait ses désirs les plus profonds d'épanouissement dans l'entreprise! Autre changement d'importance, les outils de traçabilité ont suivi pendant longtemps

des adresses IP. Aujourd'hui, ils tracent des événements et des personnes pour les authentifier et les identifier comme nous l'a précisé Luis Delabarre, directeur technique chez Trend Micro France : « Le talon d'Achille est l'utilisateur. Pour éviter les problèmes il faut suivre le principe du KISS, Keep It Simple and Secure. »

Le minimum à mettre en place concerne les suites classiques de protection des postes de travail qu'ils soient dans l'entreprise ou nomades. Antivirus et antispam forment le kit de survie minimal. Il est cependant nécessaire de les choisir simples d'utilisation et d'automatiser au maximum les mises à jour et autres processus de protection pour limiter les interventions manuelles de l'utilisateur de la solution. Des fournisseurs comme Fortinet ou Netgear proposent des



UTM, des appliances regroupant la plupart de ces fonctions sur un serveur spécifique et spécialisé.

L'authentification forte

Autre aspect des problèmes que peut rencontrer un responsable de la sécurité avec l'ouverture des frontières de l'entreprise : la nécessité de s'assurer que la personne qui se connecte au système d'information soit bien la bonne et que celle-ci possède bien le droit d'accéder aux informations qu'elle demande. De la même manière, en interne, la personne doit montrer patte blanche pour accéder à certaines informations, applications... Philippe Fauchay, le nouveau directeur général de RSA France, explique : « *Le but est de renforcer les défenses en profondeur et de proposer différents mécanismes comme des systèmes de PKI – système de gestion à clé publique. Ces systèmes peuvent être fournis sous forme de services hébergés.* »

Là encore, la réglementation a été un moteur dans le domaine. Les exigences, par exemple dans les jeux en ligne, a rehaussé le niveau demandé habituellement dans le secteur du Web. Des acteurs comme Keynectis qui vient de reprendre Open Trust, ont d'ailleurs pu se mettre en valeur à cette occasion. Cette entreprise française vient d'obtenir une certification de l'ANSSI pour son coffre-fort électronique K.EEP. La solution sert de séquestre et d'outil de traçabilité sur les données des jeux en ligne.

Dans la même veine, Olfeo, un spécialiste français de solutions de proxy et de filtrage d'URL, vient de lancer un produit qui permet d'authentifier et de conserver les logs d'utilisateur sur des réseaux publics d'invités dans les entreprises (filaire et Wi-Fi). Ce produit correspond d'ailleurs à une obligation légale afin de limiter l'accès à des contenus condamnables par la loi. De son côté, Safenet a étendu sa solution de SSO aux applications en SaaS dont Salesforce.com et Google Apps.

Selon le Gartner, le simple marché du Single Sign ON (SSO) s'est monté à 183 millions de dollars pour 2011 en croissance de 9%. Il devrait de plus se développer sur d'autres environnements et la croissance devrait continuer sur ce rythme jusqu'en 2015. Ces systèmes d'authentification forte s'étendent désormais aux environnements mobiles. Ainsi, RSA vient de porter sa technologie SecurID sur plusieurs environnements mobiles. Ces apports technologiques deviennent importants quand on les compare à la croissance du nombre des logiciels malveillants dans les environnements mobiles. Selon G Data, un éditeur allemand de solutions de sécurité pour les postes de travail et les serveurs, les malwares mobiles ont crû de 270% lors du premier semestre de cette année. Une autre source, le rapport de la X Force d'IBM, indique que les problèmes de sécurité provenant de terminaux mobiles vont doubler cette année.

Des éditeurs comme ZScaler proposent d'aller plus loin en poussant au plus près des utilisateurs les politiques de sécurité des entreprises en passant par le Cloud et par une cascade de systèmes de caches partout dans le monde.

Tracer les utilisations dans le SI

Toutes ces solutions visent à suivre et à contrôler les actions des utilisateurs du SI. En clair, qui fait quoi, quand et comment? Pendant longtemps, et ce n'est pas totalement fini, les entreprises ont choisi d'interdire certains usages. Devant la lame de fond et certaines justifications parfois spéculieuses, elles ont préféré contrôler et maîtriser les possibilités d'accéder aux réseaux sociaux ou à des applications pas forcément à vocation professionnelle à première vue. 64% des entreprises en France interdi-



Une vue de l'écran sur le poste client dans la solution de BitDefender.

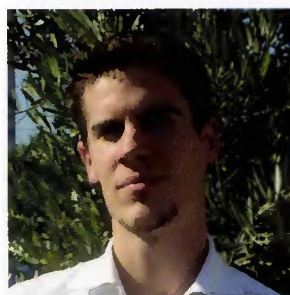
sent encore l'accès aux différents réseaux sociaux selon des chiffres collectés par Kaspersky Labs. C'est beaucoup moins que d'autres pays (Italie et Espagne dépassent les 70%). Les applications possibles sur ces réseaux font que cette méthode est de moins en moins valide. Ainsi, Enterasys a développé une solution, ISAAC, qui permet de gérer les équipements IT par ces réseaux sociaux.

Par ailleurs, des solutions apparaissent pour contrôler les utilisations des réseaux sociaux. Device Lock a ainsi développé une offre pour éviter la fuite de données sensibles sur le réseau Google + qui jusqu'à récemment a connu un développement très rapide.

Cyrille Barthélémy, chez Intrinsec, une entité du groupe Neurones spécialisée dans l'intégration et le conseil aux entreprises sur les questions de sécurité, constate que « *brider les gens et les accès passe de moins en moins bien. Les solutions de traçabilité sont réservées à ce qui est réellement sensible. Une approche pourrait être d'utiliser ce type de solutions pour simuler un incident et de le re-*

constituer pour expliquer pourquoi tracer et comment l'utiliser. ». Il constate aussi que le travail préliminaire autour des référentiels est désormais effectué. « *Nous avons d'importantes demandes pour des revues d'habilitation pour des référentiels centraux mis en place.* »

Sur ce point, la situation a évolué assez rapidement dans les 18 derniers mois. Il ne constate cependant pas d'emballement autour de la mise en œuvre de solutions d'identification et de gestion des accès ou autour du SSO. Il semble là encore que le levier de la réglementation soit nécessaire pour que les entreprises passent à la mise en place de solutions de ce type. Jean-Noël de Galzain, qui conduit les destinées de Wallix, ajoute : « *La traçabilité est le moyen valable pour les DSI et l'utilisateur de savoir ce que la personne a fait. Il est possible alors de vérifier la responsabilité de l'entreprise, du salarié ou d'un tiers. En fait, ces systèmes permettent à l'entreprise de se protéger mais aussi à l'utilisateur de conserver aussi un moyen de contrôle sur la confidentialité des données qui le concerne.* » ■



« Nous avons d'importantes demandes pour des revues d'habilitation pour des référentiels centraux mis en place »

Cyrille Barthélémy (Intrinsec)