Comment contrer les nouvelles menaces en Cybersecurité contre le système d’information ?

Comment contrer les nouvelles menaces en Cybersecurité contre le système d’information ?

CIO a organisé la Matinée Stratégique « Cybersécurité : les nouvelles menaces contre le système d'information » à Paris le 16 février 2016 en partenariat avec Eset, HP Inc., Level 3, Skyhigh Networks, VMware, A2JV (Evals.fr) ainsi que trois associations de référence Clusif, CESIN et Cigref. Plus d'une centaine de responsables IT présents ont échangé sur un sujet d'une grande actualité.
En matière de cybersécurité, il reste beaucoup à faire, d'autant que même les bases ne sont pas totalement maîtrisées par les entreprises. C'est ce qui ressortait de l'étude Comment protéger le SI contre les nouvelles cybermenaces ? réalisée par CIO et présentée à l'occasion de la Matinée Stratégique Cybersécurité : les nouvelles menaces contre le système d'information. Les résultats complets sont en téléchargement sur le présent site web.

Cette conférence a eu lieu au Centre d'Affaires Paris Trocadéro le 16 février 2016. Elle a été organisée par CIO en partenariat avec Eset, HP Inc., Level 3, Skyhigh Networks, VMware et A2JV ainsi que trois associations de référence (Clusif, CESIN et Cigref). Durant tout l'événement, les participants ont pu interroger les intervenants au travers de l'appli web mobile Evals.fr d'A2JV.

La cybersécurité face au cloud
Parmi les sujets d'actualité du moment pour les DSI, il y a bien sûr le cloud. Et, en matière de cybersécurité, le cloud reste avant tout un problème avant d'être une solution. « On a l'impression que les responsables sécurité et ceux qui mettent en oeuvre des services cloud ne se parlent pas » a déploré Joël Mollo, Regional Director Southern Europe & Middle East de Skyhigh. Or, selon le baromètre publié par l'assureur Allianz, la cybersécurité est un frein croissant à l'adoption du cloud.
Certes, cela ne stoppe pas sa forte croissance : moins de six cents recours à des services cloud en moyenne dans chaque entreprise début 2014 contre plus de mille fin 2015. Mais certains SaaS peu sécurisés et adoptés en mode shadow IT, par exemple un service gratuit de compression de PDF en ligne, posent de vraies questions de sécurité alors qu'ils sont choisis à cause de leur simplicité. Sécuriser les données envoyées dans des services cloud est donc un impératif a rappelé Joël Mollo.

Joël Mollo, Regional Director Southern Europe & Middle East de Skyhigh s'est interrogé : « Comment appréhender une adoption sereine des Services Cloud ? »

Mais le cloud n'est pas la seule faiblesse. C'est ce qu'a montré François Beauvois, Commissaire de police, Chef de la Division Anticipation à la Direction centrale de la police judiciaire, à la Sous-Direction de la lutte contre la cybercriminalité du Ministère de l'Intérieur. Trop souvent, on se demande « Que fait la police ? ». François Beauvois, qui s'intéresse à toutes les formes de cybercriminalité, a apporté la réponse, rappelant au passage les conséquences de la cybercriminalité sur les entreprises françaises.

François Beauvois, Commissaire de police, Chef de la Division Anticipation à la Direction centrale de la police judiciaire, Sous-Direction de la lutte contre la cybercriminalité (Ministère de l'Intérieur) a ensuite présenté les tendances de la cybercriminalité visant les entreprises et les précautions à prendre.

La cybercriminalité : un risque croissant dans un monde de plus en plus connecté
Les risques sont d'autant plus grands que les systèmes d'information sont de plus en plus complexes et connectés voire interconnectés. « La transformation digitale des sociétés est une imbrication digitale de clouds hybrides, d'objets connectés, etc. » a décrit Christophe Belmont, Sales Engineer chez Level 3 Communications. Il a ainsi rappelé les grandes craintes publiées en 2014 sur les systèmes industriels Scada. Or, avec l'IoT et les objets connectés, c'est un peu le Scada partout, y compris chez Monsieur Toulemonde.
Il ne peut pas exister d'arme secrète magique et omnipotente face aux attaquants qui utilisent des techniques très diverses pour déjouer les protections classiques des systèmes d'information. Mais il faut combiner plusieurs approches et vecteurs.

Christophe Belmont, Sales Engineer chez Level 3 Communications est intervenu sur le thème : « Cyber-sécurité : mieux gérer vos risques dans un environnement de plus en plus connecté ».

La première table ronde sur « La protection technique des systèmes » a réuni Frédéric Carricaburu, DSI et RSSI du groupe SFA, et Benoit Guennec, président fondateur de Connected Object / Eedomus. D'un côté, le DSI de SFA a justement expliqué l'état des lieux en matière de cybersécurité dans une entreprise classique. De l'autre, le patron de Connected Object / Eedomus a expliqué comment il sécurisait les objets connectés qu'il met en circulation.

La première table ronde a réuni, de gauche à droite, Frédéric Carricaburu, DSI et RSSI du groupe SFA, et Benoit Guennec, président fondateur de Connected Object / Eedomus.

La sécurité des datacenters doit être révisée
La transformation numérique amène aussi des changements dans les infrastructures, notamment les datacenters. La virtualisation, base technique de la cloudification, a en effet bouleversé le fonctionnement des datacenters depuis 2009. La cloudification est non-seulement un facteur de consolidation et donc d'économies mais aussi d'agilité, donc de changements réguliers. Depuis 2011, les réseaux aussi se virtualisent massivement. « Le modèle de sécurité des datacenters est dépassé » a donc jugé Ghaleb Zekri, NSX Senior Systems Engineer chez VMware.
En particulier, le trafic de données entre machines au sein même de la zone de confiance (dans une logique périmétrique) s'est grandement accru. Ghaleb Zekri a rappelé : « si l'on demande au firewall d'analyser tout le trafic, y compris interne, il est vite dépassé ». D'où la recommandation d'adopter une approche par contrôle des entrées/sorties de chaque machine virtuelle au lieu de remonter tout le trafic au firewall principal.

Ghaleb Zekri, NSX Senior Systems Engineer chez VMware, a montré « Pourquoi faut-il changer le modèle de sécurité dans les datacenters ? »

Les imprimantes sont des objets connectés
Outre les datacenters, des objets a priori anodins ont eux aussi beaucoup changé : les imprimantes. Devenues des multifonctions, en fait de vrais serveurs, elles sont aussi de ce fait des objets connectés. Or, négligées, elles n'en sont que plus dangereuses. Alexandre Huart, consultant mandaté par HP, a concédé : « toutes les forteresses de la planète sont tombées un jour ». Mais autant tenter de retarder l'échéance.
« Depuis vingt ans, HP a l'expérience de la sécurisation des imprimantes » s'est-il réjouit. Et il y a des bases à ne pas négliger : rétention des impression jusqu'à identification du propriétaire du document (pour faire face aux vols de documents papiers), chiffrement des flux entrant, chiffrement du disque dur… Et puis il y a aussi des méthodes plus complexes : signature du BIOS et du système d'exploitation, contrôle des 150 paramètres de sécurité par des superviseurs…

Alexandre Huart, consultant mandaté par HP, a ensuite été interrogé sur le thème « Risques et dangers des imprimantes multifonctions »

La bêtise humaine étant la première faille d'un système d'information, la seconde table ronde sur « contrer les faiblesses humaines et les risques financiers comme juridiques » a réuni Jean-Paul Mazoyer, président du cercle Cybersécurité du Cigref, Jean-François Louâpre, vice-président du CESIN (Club des Experts de la Sécurité et du Numérique), et Martine Guignard, administrateur du CLUSIF (Club de la Sécurité des Systèmes d'Information Français). Quelques bonnes pratiques ont ainsi été rappelés.

La seconde table ronde a réuni, de droite à gauche, Jean-Paul Mazoyer, président du cercle Cybersécurité du Cigref, Jean-François Louâpre, vice-président du CESIN (Club des Experts de la Sécurité et du Numérique), et Martine Guignard, administrateur du CLUSIF (Club de la Sécurité des Systèmes d'Information Français).

Issu d'une entreprise à risque, le grand témoin de la matinée a été Farid Illikoud, Responsable Sécurité et Conformité au PMU. Tout est en effet réuni pour faire de cette entreprise un cauchemar : des flux financiers innombrables, des sites sur tout le territoire, un secteur ultra-réglementé…

Farid Illikoud, Responsable Sécurité et Conformité au PMU, a été le grand témoin de la matinée.

Enfin, pour terminer la matinée, le quart d'heure du coach a abordé la délicate question « Recruter, retenir et manager les équipes sécurité ».

Patricia Cabot, Fondatrice du cabinet Spsearch (à droite), et Caroline Tampigny, Consultante associée du cabinet Spsearch, ont ainsi confirmé que les profils en sécurité sont en forte tension et qu'il est difficile de retenir les meilleurs. Mais quelques bonnes pratiques peuvent aider … [Lire la suite]

Réagissez à cet article

Source : *Cybersécurité : contrer les nouvelles menaces contre le système d'information*