Suite de la page 44

R&D, lesquels scrutent les infrastructures des clients. Un travail de fourmi. Mais qui paie. Plus de 55.000 vulnérabilités déjà répertoriées. Au prix d'importante ressources, on s'en doute. La plateforme Security Intelligence Operations de Cisco occupe un demi millier de salariés. Le prix à payer pour remonter les informations de quelque 700.000 équipements qui contribuent à la base de réputation et pour la mise à jour des règles de sécurité (pour le filtrage e-mail, web, firewall et IPS). L'objectif est de créer un véritable maillage sécuritaire.

Tous ces réseaux mondiaux, comme le Smart Protection Network de Trend Micro, permettent de dresser des typologies et des comportements d'attaques via du reporting. Mieux: la collaboration entre tous ces fournisseurs existe puisqu'un lien unique, le mitre.org géré par le MIT, fédère toutes les vulnérabilités existantes. Bref, les attaques sont plus difficiles à mener pour les pirates, les entreprises se sécurisent de plus en plus. Auparavant, les attaques étaient relativement aisées avec, pour les pirates, un rendement maximum. ■

Builders & Breakers. Le «hacking» en noir et blanc

Des hackers en «guest speakers» à Luxembourg! C'était au Centre de Conférence de Luxembourg, le 1er décembre, en prélude à la soirée de gala 2011 de IT One.

«En 1450, le dictionnaire anglais définissait le hacker comme celui qui coupe en morceaux», nous informe le Partner & Strategy Officer de Geneva Solution, Victor Emmanuel de Sa, spécialiste en micro-puces et codage appliqué, inventeur aussi de Quantum Dana, solution exploitée par Quantum Properties pour sécuriser les e-services. *«Il passe, dans les années cinquante, pour un étudiant espiègle, devient dans les sixties un petit génie pour finir, aujourd'hui, comme voyou ou criminel informatique!»*

Chemin atypique, pour un individu difficile à classer tant ses facettes sont multiples, voire opposées. Le hacker cherchera toujours a repousser les limites du soit-disant «impossible». Défier les systèmes sécurisés, essayer de trouver la faille qui fera de lui le super-utilisateur d'un système distant... mais sans détruire. Il regarde, copie, imprime, modifie. *«Il visite ce que d'autres ont construit»*, illustrait fort bien, en ouverture de colloque, Kamel Amroune, IT One Managing Partner.

° Victor Emmanuel de Sa, Chief Hacking Officer, spécialiste de la sécurité et membre de l'équipe «Routards», vice-championne du monde du célèbre concours DEFCON en 2008, 2009, 2010 et 2011. Directeur de la stratégie de Geneva Solutions SA, il est reconnu internationalement comme expert en informatique et sécurité.

° Marc Maiffret, Chief Hacking Officer, co-fondateur de eEye Digital Security, société spécialisée en sécurité de réseau. Marc Meiffret est connu pour, entre autres faits, sa découverte du premier virus Microsoft «RedCode» et ses différents témoignages au Congrès des Etats-Unis pour des questions de cybersécurité et de protection d'infrastructure.

«En blanc, on peut dire qu'il est un virtuose des systèmes informatiques, un professionnel de la programmation, une élite de la science informatique. En noir, on dira qu'il est un utilisateur cherchant à accéder à des données confidentielles par des chemins illégaux, un cambrioleur très spécialisé», complète Emmanuel de Sa. Des raccourcis qui montrent l'ambiguïté que nous entretenons avec ce type de prédateur. Tantôt Robin des Bois, tantôt le diable en personne; nous le jugeons non pas sur ses crimes, mais sur la nature de ses crimes. Il dénonce un scandale, il est saint; il peut être aussi criminel!

En parler ou pas? Surtout ne pas se taire, répond en écho Emmanuel de Sa. Le sujet ne doit pas être tabou. Dénonçons et échangeons nos idées pour qu'avance enfin la sécurité informatique, conseille-t-il. Une pique non dissimulée contre les éditeurs de systèmes de protection qui, à le croie, ne s'engagent que peu. *«La sécurité n'est technique qu'à 20%, aussi la bonne application des 80% restants aidera à mieux comprendre les tenants et aboutissants du business. Apprenons également à utiliser nos outils avant de fabriquer quelque chose, comme le faisaient les artisans d'hier! Allons de la racine à la feuille en questionnant les vendeurs à propos de la méthodologie opérationnelle de leurs solutions. Osons demander aux ingénieurs ce que nous voulons. Faisons du renforcement à chaque étape. Oublier un seul élément revient à laisser une porte ouverte. Vérifions sans cesse la charge du système, contrôlons le périmètre de notre informatique.»* Et surtout, conclut Emmanuel de Sa, «ne faisons aucun compromis sur les fondamentaux!»

Autre profil, Marc Maiffret. Hacker depuis l'âge de 13 ans. Quatre ans plus tard, il fonde eEye avec un «gourou», son maître à penser. Cette société, alors nouvelle venue dans le monde de la sécurité informatique et dont Marc Maiffret est le «Chief Hacking Officer», développe un nouveau scanner de vulnérabilités. Et se fait très rapidement remarquer. *«Nous avons pu publier de nombreuses failles critiques liées aux produits Microsoft»*, précise-t-il non sans fierté. A tel point que la plupart des virus et autres vers -Code Red, Sasser, etc.- qui vont secouer le Web naissant s'appuieront sur ces failles. *«Le hacker fait aujourd'hui partie du crime organisé, comme maillon d'un chaîne dont le but est de nuire à la société ou de tirer un maximum de profit au départ de données volées ou piratées»*, assure-t-il. Et de laisser tomber, telle une sentence: *«Aujourd'hui, les profits de la criminalité informatique dépassent ceux du trafic de la drogue!»*

Et nous, simples utilisateurs? Et nos entreprises, si souvent victimes? Pour Marc Maiffret, venu tout spécialement de Los Angeles, la bonne nouvelle est que *«95% des attaques lancées sont prévisibles car lancées sur des vulnérabilités connues.»* Et de souligner en rafale

«qu'une bonne configuration est synonyme de bonne sécurité.» Mais aussi que: *«l'insécurité n'est pas le seul fait d'un problème au niveau du système d'exploitation»*, *«qu'il faut toujours faire la différence entre le hype et le réel ou plus exactement entre le vent et la réalité du terrain»*, *qu'il faut éduquer et tout surveiller, y compris les développements internes, points d'entrées privilégies des voltigeurs de la cambriole informatique!»*...

Passionnant, intéressant... Mais finalement qu'en pense l'informaticien luxembourgeois? Comment perçoit-il la menace? Saisissant la balle au bond, IT One a profité de l'occasion pour prendre le pouls à la centaine d'informaticiens réunis au Centre des Conférence. A la question *«une entreprise peut-elle se protéger elle-même contre des attaques ciblées?»*, 46 % des présents ont répondu oui, 46% non tandis que 8% pensent que cela ne risque pas d'arriver au Grand-Duché. Surprenant!

A la question *«comment une entreprise peut-elle résoudre le problème du hacking?»*, 68% pensent que les bonnes pratiques limitent les risques, 24% misent sur la technologie et la formation pour arrêter l'assaut d'un hacker et 8% croient que la technologie peut stopper un hacker du dimanche! Quant à savoir «comment réagir aux stratégies nouvelles des hacher?», 78% répondent par un changement d'approche, 17% par davantage d'investissements en sécurité... et 5% préfèrent attendre et voir!

Ces réactions sont autant d'interrogations. Le sujet n'a pas laissé insensible, c'est indéniable... Les pistes à suivre? Celles du bon sens, répondent indirectement les deux spécialistes.

De cette conférence, on retiendra encore que les «hackers éthiques», qui œuvrent à une amélioration permanente du niveau de sécurité, ont encore du travail pour longtemps. Après dix ans passés à eEye, Marc Maiffret a décidé de tourner la page. Il veut «explorer» d'autres voies. Il reste l'un des propriétaires de la société et continue d'apporter son aide en matière de stratégie, mais compte désormais s'investir principalement dans la formation: sensibilisation à la sécurité, bien sûr, mais aussi méthodes de recherche de failles. Son avenir est assuré.

Jean-Claude Quintart