2011 ou l'autre visage du cyber-activisme

Les environnements informatiques évoluent et avec eux, les enjeux sécuritaires auxquels sont confrontées agences gouvernementales, organisations et entreprises. Alors qu'un calme plat s'était fait ressentir en 2010, l'année 2011 a marqué une forte recrudescence des menaces.

Ainsi s'énoncent les principales conclusions de la cinquième édition d'une étude que mène depuis 2004 le Verizon Risk Team, en collaboration avec la police fédérale australienne, les services secrets américains, l'agence néerlandaise contre la cybercriminalité et les autorités irlandaises. Sur l'exercice 2011, les intéressés ont recensé pas moins de 855 incidents qui ont impliqué le vol de quelque 174 millions de données. À des années-lumière de ces vieillissants *script kiddies* qui aspiraient à la renommée, même éphémère, les nouveaux *hackers* ciblent l'information au-delà de l'infrastructure. Les postes de travail ne constituent guère plus qu'une passerelle à des desseins autrement plus sombres et imprévisibles.

À cet égard, **Chris Novak**, *manager général* pour le compte du *Verizon Business Investigative Response Team*, évoque la percée du cyberactivisme, à l'origine de 58 % des attaques. Passé les sempiternelles motivations financières (accaparer des identifiants bancaires, extorquer des fonds…), les informations confidentielles sont dorénavant régulièrement étalées sur la place publique. Le Printemps arabe et le mouvement Occupy Wall Street ont agi tels des catalyseurs. De nouvelles conceptions du piratage ont émergé. Cerner les motivations des attaquants et appréhender leur comportement relève désormais d'un véritable défi.

Plus d'attaques, plus de victimes

Au rang des victimes, toutes les entités sont concernées. *« Les grandes organisations ne sont plus les seules à être affectées »*, précise Chris Novak. Et d'ajouter : *« tout n'est plus seulement fonction de la réputation ; aussi, les petites entreprises essuient de plus en plus d'affronts. »* En outre, l'ensemble des secteurs d'activité et des corps de métier sont susceptibles de subir des attaques informatiques.

La finance et l'assurance (28 % des cas) restent en bonne position, au même titre que le commerce (12 %). Les administrations publiques (7 %) et les transports (5 %) sont plus épargnés. Les attaques par déni de service (DDoS) conservent la faveur des pirates, loin devant une foule d'autres techniques logicielles (*keyloggers*, *backdoors*, force brute) et les *malwares*. Le spectre géographique s'étend à 36 pays, contre 24 en 2010.

Cloud et mobilité

Nouvelles coqueluches des entreprises, *cloud* et terminaux mobiles restent des concepts abstraits à plus d'un titre. Leur contrôle échappe encore à de nombreuses DSI. Et pourtant, Verizon juge leur impact *« négligeable pour l'heure »*. Concernant l'infonuagique, les travaux en amont incombent aux prestataires techniques tiers, « *qui mettent du cœur à l'ouvrage et assurent une protection optimale des données* », selon Chris Novak. Quant au phénomène du BYOD, s'il va en s'accroissant, les enjeux sécuritaires qui en découlent relèvent encore de l'anecdote.

Certes, il convient d'uniformiser les politiques de déploiement des flottes mobiles et d'en tenir

informé les collaborateurs dans l'optique d'éviter les mauvaises manipulations, elles aussi à la source de certaines vulnérabilités. Mais seulement 4 % des attaques ont pour origine un poste de travail interne au réseau d'entreprise. Le reste provient d'agents externes.

« Mieux vaut prévenir que guérir »

Au dire de Chris Novak, il s'agit d'opter pour une stratégie proactive. L'anticipation prime alors que 96 % des failles qu'exploitent les *hackers* sont jugées peu sophistiquées, résorbables moyennant une simple redéfinition des périmètres sécuritaires et surtout d'une passivité à remiser au placard : actuellement, la découverte d'une faille de sécurité prend souvent plusieurs semaines. Le délai moyen se compte parfois en mois. D'où la nécessité de mener des analyses en amont, à l'appui d'un processus de *reverse engineering*.

Crédit image : © drx – Fotolia.com