IBM recense les cyberattaques à haut risque pour 2014

Noms, adresses e-mail, mots de passe, numéros de cartes bancaires : plus de 500 millions de jeux de données personnelles ont été volés en 2013. Mais sur les milliards d'alertes émises par les équipements de sécurité installés dans les entreprises*, seules quelques centaines cachent des **cyberattaques** à haut risque.

C'est l'une des problématiques soulevées par IBM dans la dernière édition de son **Cyber Security Intelligence Index** (document PDF, 12 pages). L'exposition médiatique du phénomène s'est intensifiée (selon nos confrères d'ITespresso), générant une prise de conscience globale quant aux nouveaux enjeux de la sécurité informatique… jusqu'au sein des chaumières. Leur réputation écornée, les entreprises doivent aujourd'hui retrouver la confiance de leurs clients tout en veillant constamment sur leurs actifs numériques et plus particulièrement leur propriété intellectuelle.

Pas tout protéger, mais viser juste

Les terminaux et les données en circulation sur le réseau sont si nombreux qu'il est généralement impossible de tous les encadrer. A défaut de pouvoir tout protéger, il faut viser juste, par exemple avec l'aide d'outils analytiques. En moyenne, **moins de 1%** des événements détectés par les équipements et logiciels de sécurité **recèlent réellement des menaces pouvant mener à l'exposition ou au vol de données**. Parmi eux, 95% sont dus – intégralement ou partiellement – à une erreur humaine : mauvaise configuration, utilisation des identifiants et mots de passe par défaut, perte ou vol d'ordinateurs portables ou de téléphones, mobiles, ouverture de pièces jointes ou d'URL malveillantes, etc.

D'une année à l'autre, l**a finance/assurance** reste le secteur le plus visé (23,8% des incidents), devant l'industrie (21,7%) et l'information-communication (18,6%). Le commerce et les services sociaux, respectivement à 6,2% et 5,8%, sont ciblés à cause de leurs relations directes avec les consommateurs, qui leur fournissent des informations financières.

Au marché noir, les cartes bancaires se revendent dans la fourchette de 25 à 100 dollars selon la date d'expiration et l'éventuelle présence du code de sécurité à trois chiffres. Elles sont souvent utilisées indirectement, en l'occurrence pour acheter des cartes-cadeau ou prépayées qui servent à acquérir des biens, lesquels sont ensuite revendus.

Mais il faut faire vite pour les cybercriminels : avec l'extension de la couverture médiatique, les nouvelles circulent vite et de nombreuses cartes sont désactivées par leur propriétaire avant d'avoir pu être exploitées. Les Etats-Unis, où l'on utilise encore un système de bande magnétique par opposition à la puce électronique, constituent une cible de choix.

L’éclectisme des cyberattaques

Comment les cybercriminels s’y prennent-ils ? **Dans 38% des cas, ils s’appuient sur du code malveillant** : logiciels tiers, chevaux de Troie, enregistreurs de frappe (keyloggers)… De plus en plus sophistiqués, les outils deviennent aussi plus accessibles à l’initiative des communautés de hackers.

Dans 19% des cas, les cyberattaques impliquent **des accès non autorisés**, souvent par force brute, mais aussi par élévation de privilèges après intrusion dans un réseau. IBM illustre cette situation en citant l’exemple d’un individu qui pénètre dans une propriété et parvient ensuite à infiltrer la maison en suivant quelqu’un qui possède les clés.

Tout en bas de l’échelle, **le déni de service (DoS)** n’est exploité que dans **2% des attaques** répertoriées comme importantes. Dans beaucoup de cas, la bande passante est insuffisante pour causer des dommages. C’est sans compter les protections ad hoc mises en place par de nombreuses entreprises.

Dans **56% des cas, les attaques proviennent exclusivement de personnes externes** à l’entreprise. Mais **17% des incidents impliquent un collaborateur** d’autant plus difficile à détecter qu’il se trouve… en interne. Il arrive aussi que les employés servent involontairement de passerelles pour les pirates informatiques. Notamment via les réseaux sociaux et les messageries électroniques, qu’ils sont susceptibles d’utiliser à des fins personnelles dans le cadre professionnel.

** IBM s’appuie sur des milliards de données collectées en 2013 via les équipements de sécurité installés par ses clients. L’échantillon a été « normalisé » de sorte qu’un client typique est une entreprise de 1000 à 5000 salariés ayant déployé une moyenne de 500 équipements de sécurité sur son réseau.*

A lire aussi :

En 2013, la facture de la cybercriminalité évaluée à 445 milliards de dollars

Sécurité : cybercriminalité, cyberattaques, cybervictimes