La cybercriminalité à l’encontre des entreprises s’industrialise

	La cybercriminalité à l’encontre des entreprises s’industrialise

Un écosystème professionnalisé de cybercriminels mène la danse.
Pas d'électrochoc dans les entreprises après l'affaire Sony : les investissements restent insuffisants.
Sony débordé par les cybercriminels
Phishing, escroquerie, espionnage, vol de secrets industriels… Si ces phénomènes ne sont pas nouveaux, la cybercriminalité ne s'est jamais aussi bien portée.
Bernard Cazeneuve n'a pas manqué de rappeler la réalité de cette menace au Forum international de la cybersécurité, qui s'est tenu à Lille la semaine dernière. « Des attaques de plus en plus sophistiquées touchent principalement les entreprises et visent à leur voler des données stratégiques, parfois en très grande quantité », a fait valoir le ministre de l'Intérieur. Si le phénomène est difficile à chiffrer, il connaît une montée en puissance. Pourquoi ? « La technologie explose. Il y a de plus en plus d'applications. Plus on développe vite, plus le risque de bugs augmente», explique Jean-Michel Orozco, président de CyberSecurity chez Airbus Group (ex-Cassidian).
Au quotidien, les entreprises doivent lutter contre la petite délinquance, peu sophistiquée mais rentable. « Les entreprises ont été fortement touchées par les "cryptolockers" », explique Eric Freyssinet, chef de la division de lutte contre la cybercriminalité de la Gendarmerie nationale. Des pirates bloquent des PC, et exigent des rançons pour les débloquer. Bien sûr, celui qui paie ne récupère pas pour autant ses données.
« Les anciennes menaces s'industrialisent. Les banques, par exemple, souffrent beaucoup d'attaques en déni de service [rafale d'attaques dont le but est de bloquer les systèmes] ou de phishing », explique Michel Van Der Berghe, à la tête d'Orange Cyberdefense. Plus élaboré, « le "spearphishing" permet d'envoyer des e-mails ultraciblés personnalisés par secteur identifié, l'armement, le transport… » dit Eric Freyssinet. C'est grâce à un e-mail très bien personnalisé que la Syrian Electronic Army a réussi, ces derniers jours, à pirater « Le Monde ».

Des PME très exposées
Les PME sont particulièrement exposées aux faux placements, où la victime verse de l'argent à un tiers soi-disant spécialisé dans les placements à haut rendement. Selon la gendarmerie, ce type d'attaque représente les « trois quarts des escroqueries » qui concernent les entreprises. Plus connue, « l'arnaque au président » consiste à extorquer de l'argent à une entreprise en se faisant passer pour son dirigeant. Parmi les victimes, Michelin, qui a perdu 1,6 million d'euros.
L'espionnage – de secrets industriels ou commerciaux –, un fléau auquel font face les entreprises depuis deux ou trois ans, ne requiert pas non plus de techniques ultrasophistiquées. « Un mot de passe faible, type 1 2 3 4 5 6, sur un équipement de réseau ou une application peut suffire », estime Stanislas de Maupeou, directeur-conseil cybersécurité chez Thales. Dans ce cas-là, la difficulté consiste surtout à identifier les intrusions.

Cellules « N-Tech » : la gendarmerie aussi s'arme face à la cybercriminalité

Pas facile de lutter contre ces attaques à grande échelle. Car, en face, on a affaire, non pas à des groupements organisés, mais à un écosystème criminel. « Sur le "dark Web", on trouve des publicités pour des attaques en kit. Il y a même des réductions ! » explique Michel Van Der Berghe. « Ceux qui vendent les virus ne sont pas ceux qui les collectent. Deux personnes différentes à deux bouts de la France peuvent se mettre d'accord pour développer un virus. Elles communiquent sur Tor, sur certains forums ou sur des messageries instantanées comme Jabber », explique le lieutenant-colonel.
De leur côté, les entreprises restent insuffisamment armées. Le piratage massif de Sony, victime d'un vol à grande échelle de données, n'a pas créé d'électrochoc. Chez Thales, un seul client exerçant dans le même domaine que Sony, et expliquant qu'il ne pourrait supporter une attaque d'une telle ampleur, a appelé, chez Airbus aucun.

Pas seulement des moyens
Beaucoup de dirigeants n'ont pas encore fait grand-chose. « Les moyens seuls ne suffisent pas. Il faut aussi un plan, avec une gouvernance qui sait quoi faire en cas de problème », détaille Jean-Michel Orozco, d'Airbus CyberSecurity, qui estime qu'un grand groupe devrait dépenser entre 8 et 11 % de son budget informatique en sécurité. On est loin du compte. « Aujourd'hui, on est à 3 ou 4 %. Or, en cas de problème, si l'on doit remonter entièrement un système, cela peut coûter 20 % du budget IT », estime Stanislas de Maupeou, qui rappelle qu'au regard des outils existants, la lutte contre le fléau est à la portée de tous.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lesechos.fr/tech-medias/hightech/0204110358637-la-cybercriminalite-a-lencontre-des-entreprises-sindustrialise-1087050.php
Par Sandrine Cassini