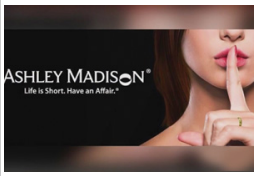
L’individu cible des cyber attaques

L’individu cible des cyber attaques

Si les cyberattaques les plus marquantes ont visé des grands comptes ou des acteurs industriels majeurs, les PME se voient de plus en plus menacées. Reste à faire comprendre à un dirigeant, qu'au-delà de la taille de son entreprise, ce sont les individus – lui compris – qui sont visés.



En août 2015, les données (32 millions de comptes) du site de rencontres extraconjugales, Ashley Madison, ont été piratées.
Tavish Vaidya, doctorant de l'université de Georgetown à Washington, documente depuis quelques années le nombre et l'importance des cyberattaques du XXIe siècle. Il livrait récemment dans la MIT Technology Review, son top 20 où l'on retrouve l'assaut du ver Stuxnet sur des centrifugeuses iraniennes en 2010 ou l'infection en décembre 2013 par des hackers chinois des ordinateurs de membres européens du G20 lors de la réunion de l'organisation internationale à Saint-Pétersbourg.

La faille est toujours humaine

Mais la nature de ces cyberattaques très médiatisées, qui ont touché de grandes organisations, ne joue pas forcément à l'avantage de ceux qui veulent provoquer une prise de conscience chez les dirigeants.
« Longtemps, la cybersécurité n'a concerné que les grands comptes. Et, chez la majorité de nos interlocuteurs en entreprise, la réponse reste encore : "ces sociétés sont très connues. Ce n'est pas comme nous, qui sommes beaucoup plus petits… Et ceci, même si la donne a changé" », explique Sergio Loureiro, président et cofondateur de SecludIT, une start-up créée en 2011 qui propose de réaliser en continu des scans automatiques de vulnérabilité sur les infrastructures des entreprises.
« Nous constatons que les grands groupes ont progressivement élevé leur niveau de sécurité, compliquant et rendant moins intéressant le fait d'attaquer directement leurs systèmes. Par contre, cela a encouragé les assaillants à s'en prendre aux PME… qui sont souvent leurs prestataires », détaille PierreYves Popihn, directeur technique de NTT Com Security (ex-Integralis), la filiale cybersécurité du groupe de télécommunications japonais.
Les entreprises, de plus en plus ouvertes sur leur écosystème, risquent alors de se compromettre les unes les autres… Malgré ses impacts résolument business, la cybersécurité traîne une étiquette trop « technique » auprès des directions générales, qui s'en défaussent sur le responsable de la sécurité des systèmes d'information (RSSI) ou le responsable informatique. Or, le message martelé par les experts est tout autre : dans la majorité des cas, la faille est humaine.
« 100 % des entreprises que nous testons ont au moins une faille critique dans leur système d'information, et nous sommes toujours arrivés à accéder à des informations confidentielles sur les collaborateurs ou les clients… Mais une fois qu'un attaquant a mis le pied dans l'entreprise, il va viser des individus en particulier, pour obtenir davantage, fait valoir Sergio Loureiro. Dans ces conditions, le PDG peut tout aussi bien être le maillon faible que la standardiste. »
Un exemple récent illustre justement le rôle important de « l'ingénierie sociale » pour exploiter les failles de sécurité.

Une lutte d'ego

La société BRM Mobilier, PME des Deux-Sèvres spécialisée dans l'aménagement de médiathèques et bibliothèques, a été placée en redressement judiciaire début septembre 2015, après que des malfaiteurs se sont fait passer tour à tour, par e-mail et téléphone, pour le président de cette entreprise de 44 salariés, et pour ses avocats. Les juges ont prononcé le redressement judiciaire avec poursuite des activités jusqu'au 11 mars 2016, le temps de retrouver un repreneur éventuel. Cette « arnaque au président » a permis de détourner 1,6 million d'euros par l'intermédiaire de la responsable administrative et financière de la société. *« Contrairement à une attaque à base de code malicieux, où un collaborateur ouvre une fausse pièce jointe d'e-mail, par exemple une facture, l'arnaque au président ne fait pas appel à un malware, il s'agit avant tout d'une escroquerie »*, note Charles Rami, expert cybersécurité chez Proofpoint, une entreprise américaine qui se spécialise notamment sur la protection des e-mails.
« Dans le cas de BRM, l'arnaque n'a sans doute pas été montée au hasard. Elle s'est déroulée juste après une importante entrée d'argent. Il est possible que l'entreprise ait été préalablement infectée par un cheval de Troie étudiant l'environnement financier et bancaire de l'entreprise. L'usurpation de l'identité en e-mail, elle, est très simple techniquement », décrit-il plus précisément. Un avis partagé par Pierre-Yves Popihn, qui estime que 15 % des cyberattaques en France servent avant tout à faire de la reconnaissance pour se voir ensuite presque littéralement « ouvrir la porte » de l'entreprise par un de ses salariés ou le dirigeant lui-même.

Cette usurpation d'identité peut-elle provoquer un déclic chez les dirigeants ?

« Tout le monde est concerné, mais deux populations sont très sensibles. Les personnes du service IT qui testent des usages et des technologies dans l'entreprise comme ils le feraient à leur domicile ; et les membres du top management, qui souhaitent connecter au SI leurs propres outils, leur smartphone personnel par exemple, même si cela peut entraîner des complications en termes de sécurité. Ces acteurs disposent souvent de comptes à privilège, c'est-à-dire des "clés" du système d'information, même quand cela n'est pas nécessaire au quotidien », témoigne Sandro Lancrin, architecte Sécurité SI et RSSI de Radio France.
Il souligne d'ailleurs, que cette problématique des individus revient trop régulièrement à une lutte d'ego, un directeur s'offusquant que l'un de ses subalternes dispose de droits informatiques et pas lui…

> **"Toutes les entreprises que nous testons ont au moins une faille critique dans leur SI"**
> Sergio Loureiro
> *président et cofondateur de SecludIT*

Malgré tout, la « conscience cyber » fait petit à petit son chemin en entreprise. Les affaires grand public, comme le vol de données du site d'adultère Ashley Madison l'été dernier, contribuent à attirer l'attention. *« C'est à double tranchant,* note Mounir Chaabane, conférencier Eucles pour l'Institut national des hautes études de la sécurité et de la justice, une émanation de la délégation interministérielle à l'Intelligence économique, *en donnant tant de visibilité à des affaires comme l'arnaque au président de BRM ou Ashley Madison, on se focalise sur des cas presque anecdotiques vu la diversité des formes que peut prendre une attaque. Ce vers quoi il faudrait tendre, c'est une culture qui mette les individus en face de leurs responsabilités, qu'ils soient PDG, trésorier, agent des ressources humaines ou administrateur système. »* Une culture bien plus présente dans d'autres pays, de la Finlande aux Etats-Unis, où des dirigeants ont déjà été tenus responsables des conséquences de cyberattaques menées contre leurs entreprises, et mis à la porte. Ainsi, le PDG et fondateur d'Ashley Madison n'a pas tardé à quitter son poste : l'an dernier, dans un entretien télévisé, il avait décrit les serveurs du site comme étant « impénétrables »…

A lire également

Suite à l'affaire BRM de Bressuire, la chambre de commerce et d'industrie des Deux-Sèvres a publié un guide « Spécial Arnaque », destiné aux chefs d'entreprise face aux nouvelles formes d'escroquerie, notamment la cybercriminalité. Pour le consulter : http://bit.ly/1ijoKRH.
Lire aussi les 22 fiches thématiques sur « La sécurité économique au quotidien », publiées par la Direction interministérielle à l'intelligence économique, http://bit.ly/1iOEGow

---

Réagissez à cet article
Source : http://www.alliancy.fr/a-laffiche/securite/2015/11/30/cybersecurite-lindividu-pour-cible