CYBERCRIMINALITÉ

Vol de données, alerte au phishing !

À l'ère du tout numérique, les entreprises doivent rester vigilantes pour ne pas être « hameçonnées ».

BÉNÉDICTE GRAULLE,
avocate au cabinet
Jones Day

La cybercriminalité ne cesse de se développer. En 2014, près de 320 millions de programmes malveillants étaient créés dans le monde, soit près de 1 million par jour, selon l'étude Symantec reprise en 2015 dans le rapport « Enjeux et difficultés de la lutte contre la cybercriminalité » de l'Institut national des hautes études de la sécurité et de la justice. Tant les particuliers que les entreprises sont touchés par ces cyberattaques, parmi lesquelles figure le phishing ou hameçonnage. Il s'agit d'arnaques informatiques visant à dérober les données confidentielles. Phénomène installé depuis plusieurs années, le phishing est un véritable fléau.

Des conséquences irréversibles

Le phishing revêt deux formes impliquant l'envoi à une cible d'un courrier électronique provenant prétendument d'une entreprise de confiance comme une banque, un site de commerce en ligne... La première technique consiste à envoyer un e-mail contenant un lien qui, une fois ouvert, installe un logiciel malveillant (malware) sur l'ordinateur dans le but d'extraire des données sensibles. L'intrusion d'un malware dans le système informatique d'une entreprise peut avoir des conséquences irréversibles, les pirates ayant accès à l'ensemble de ses informations et données confidentielles (identifiants réseaux, coordonnées bancaires, fichiers clients, secrets de fabrication, pièces comptables...). Une telle intrusion peut déstabiliser l'entreprise cible et conduire à une interruption longue et coûteuse de ses services, comme ce fut le cas lors de l'attaque contre la chaîne de télévision TV5 Monde au début de l'année 2015. Le second type d'e-mail de phishing invite le destinataire à se connecter, par le biais d'un lien hypertexte, sur un site internet fallacieux, une copie du site original d'une entreprise dont l'identité a été usurpée, avec un logo et une mise en page identiques. Prétextant généralement une mise à jour du service, le message demande à la victime de remplir un formulaire et de communiquer des informations confidentielles le concernant.

La technique du phishing repose donc sur la crédulité des internautes. Il s'agit de les piéger en leur faisant croire à la véracité du courrier électronique. Les données récoltées sont ensuite directement exploitées ou vendues à des organisations sur le marché noir.

L'ENJEU

- La technique de l'hameçonnage se développe avec des conséquences ravageuses sur les entreprises.

LA MISE EN ŒUVRE

- Mettre en place des actions de sensibilisation des salariés au phishing
- Développer des bonnes pratiques de sécurité sur internet
- Connaître l'arsenal répressif

Les auteurs de phishing se révèlent être de véritables professionnels. En amont, ceux-ci entreprennent de longues et fastidieuses investigations sur les usages des internautes, leur réseau familial et amical ainsi que leur utilisation d'internet. Leurs attaques, élaborées « sur mesure », sont particulièrement ciblées et ne cessent de gagner en efficacité.

Pour répondre aux menaces croissantes auxquelles les entreprises font face, le législateur a introduit des délits autonomes et spécifiques visant notamment à réprimer les actes de phishing numérique. L'usurpation d'identité numérique, créée par la loi Lopsi II du 14 mars 2011, réprime ainsi « le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération ». D'autres délits, tels que l'introduction frauduleuse de données dans un système de traitement automatisé de données ou la collecte frauduleuse de données à caractère personnel, sont autant d'infractions susceptibles d'être reprochées aux auteurs de phishing numérique.

Sensibiliser à la vigilance

Les attaques de phishing affectent principalement la confiance placée dans les entreprises. Pour éviter ces situations, elles doivent mener des campagnes d'information et de sensibilisation auprès de leurs employés et clients. C'est en effet par leur biais que les pirates ont accès aux données sensibles et confidentielles de l'entreprise. Outre les logiciels antivirus ou anti-spam, des moyens de lutte à l'échelle individuelle doivent être mis en œuvre. Il convient notamment d'éviter de communiquer des informations personnelles ou sensibles sur les réseaux sociaux, ou encore d'inciter à l'utilisation d'outils de détection de liens frauduleux. Il faut également apprendre à s'interroger sur les courriers électroniques suspects en se posant les bonnes questions. L'offre est-elle trop séduisante ? Pourquoi le directeur de l'entreprise envoie-t-il ce courriel un dimanche soir ? Pourquoi solliciter un nouveau paramétrage du mot de passe alors que cela a déjà été effectué récemment ? Quid de la syntaxe ? Enfin, il faut habituer les salariés à vérifier que l'URL est sécurisée (https://) et à toujours faire preuve de vigilance en cas de réception d'un courrier électronique non sollicité. ■

D.R.