Sélection du mois d'octobre 2015

La hausse majeure des cyberattaques

Un constat unanime :
De nombreuses études et avis d'expert sont venus démontrer pour octobre 2015 l'augmentation majeure des cyberattaques avec, pour corollaire, un coût de plus en plus important.

Une étude du cabinet Mc Affee et du Center for Strategic and International Studies évalue les pertes à plus de 360 milliards d'euros par an dans le monde. Selon Kasperky, il y aurait eu en 2014, 237 millions d'attaques informatiques contre 500 000 en 2004, une véritable « explosion », (BFM Business, 02/10/15) soulignant que Windows et Android sont les systèmes les plus piratés. Cette augmentation exponentielle est également soulignée par la sixième édition d'une enquête du Ponemon Institute chiffrant pour l'année 2015 une augmentation de 20 % par rapport à 2014 et de 82 % depuis la première édition de l'étude. Elle est en lien avec l'extension d'Internet dans le monde, qui compte désormais plus de 3 milliards d'utilisateurs.

D'autres éléments chiffrés indiquent que la situation va perdurer. Le marché mondial de la cyber-assurance devrait tripler d'ici 2020 pour atteindre 6,6 milliards d'euros.

La France particulièrement touchée :
Les entreprises françaises sont particulièrement visées. Une étude de PricewaterhouseCoopers (PwC) y constate une augmentation de 51% des cyberattaques en un an alors que la tendance mondiale indique une hausse de 38%. La perte est en moyenne de 3,7 millions d'euros en cas d'attaque. Websense, une société spécialisée dans la cybersécurité, estime que 36% des entreprises françaises ont été victimes d'une attaque au cours des 12 derniers mois. Une enquête réalisée par Orange Business Service a porté ce chiffre à 43% des entreprises industrielles en 2014 où les PME ne sont pas épargnées. Plus d'un tiers ayant été touchées.

Quel est le mode opératoire ?
Huit infections sur dix sont provoquées par l'envoi de mails, généralement parce l'utilisateur a ouvert une pièce jointe contenant un logiciel malveillant. L'identité de l'envoyeur doit être reconnue avant toute ouverture de pièces jointes, son adresse web vérifiée. Il ne faudrait même pas ouvrir un mail si l'on ne connaît pas l'expéditeur selon l'avis des experts invités aux Assises de la sécurité et des systèmes d'information à Monaco parmi lesquels Guillaume Poupard, directeur de l'ANSSI (Agence nationale de la sécurité des systèmes d'information).

Cependant, une vérification scrupuleuse de l'identité de l'envoyeur n'est pas une garantie absolue, car selon Kaspersky Lab France, présent également, il est facile pour quelqu'un qui connaît un peu l'informatique d'usurper l'identité d'un autre et d'envoyer un mail en se faisant passer pour un proche ou un collègue après avoir pris

des renseignements sur les traces que laissent les personnes sur les réseaux sociaux, entre autres. Une petite PME d'Annoeulin, DB VetPro, qui fabrique des vêtements pour professionnels a eu sa boîte mail piratée. Une fois en possession des données bancaires de ses fournisseurs chinois, les virements leur étant destinés ont été détournés pour un préjudice de 52 000 euros (La Voix du Nord, 17/07/2015).

Dans quel but ?
Eugène Kasperky distingue trois grands types de menaces informatiques. La cybercriminalité qui veut récupérer de l'argent, le cyberespionnage qui s'intéresse aux données, et le cybersabotage visant la cessation d'activité.

Concernant la tendance actuelle, l'étude de PwC souligne que 34 % des incidents viennent d'employés de la compagnie attaquée. Une part grandissante des fournisseurs et prestataires est également constatée. En fait, une majorité d'attaques seraient menées par d'anciens employés de l'entreprise. Philippe Trouchaud, responsable sécurité chez PwC précise que souvent, c'est l'employé qui cherche à se venger et va chercher à voler des données pour les revendre, les donner à un journaliste ou les publier sur Internet (Le Parisien, 15/10/15). Une affaire de ce genre est actuellement en cours aux Etats-Unis où un ancien employé de Tribune Média, Matthew Keys, chargé des réseaux sociaux à l'agence de presse Reuters, est accusé d'avoir fourni à des membres d'Anonymous des mots de passe pour accéder à un serveur permettant ainsi aux pirates de modifier un article en ligne du Los Angeles Times (Ouest-France, 08/10/15).

Les attaques de la concurrence ne sont pas à négliger. En 2014, un communiqué de PwC soulignait la hausse du phénomène. C'est ce qu'indique également Thierry Rouquet, cofondateur de Sentryo (spécialisée dans la cybersécurité) en déclarant qu'une « entreprise à la moralité douteuse » peut désormais procéder à une attaque informatique pour quelques dizaines de milliers d'euros en passant par une officine mafieuse. La cybercriminalité étant passée, d'actes commis par des pirates isolés à de véritables « services » du crime organisé où la spécialisation est de mise. Un expert canadien, directeur de la recherche chez Deloitte évoque également cette sophistication plus importante des attaques, avec pour conséquence, une gravité qui va de pair. Il n'est pas le seul. C'est le même constat chez Hewlett-Packard.

Comment s'en prémunir ?
L'explosion du phénomène a conduit l'État à réagir par une campagne d'information à destination du grand public par 4 clips inspirés de la télé-réalité, « La Hack Academy » qui soulignent les principales imprudences des internautes. Il peut s'agir d'une première étape à titre personnel. Pour les entrepreneurs, l'ANSSI a dressé une liste de prestataires de la cybersécurité (certifié par une qualification), sur laquelle pourront s'appuyer les entreprises demandeuses. Un référent de l'ANSSI va également être nommé dans les treize régions françaises pour une approche plus locale. Il peut être opportun de s'en rapprocher (www.ssi.gouv.fr).