La cyber-guerre est déclarée

	La cyber-guerre est déclarée

« La cybercriminalité est un fléau mondial. » Le constat dressé par Jean-Louis Bruguière, Premier Vice-Président honoraire du Tribunal de Grande Instance de Paris, est sans appel. Et l'ancien coordinateur du pôle antiterroriste l'a martelé à la tribune de l'EMLyon, à l'invitation d'Acteurs de l'Économie et du cabinet d'avocats d'affaires CMS Bureau Francis Lefebvre.

Avec la cybercriminalité, une nouvelle forme de guerre est ouverte. « On dénombre près de 120 000 cyber-attaques par jour dans le monde. Et la courbe est exponentielle », selon les chiffres rapportés par Jean-Louis Bruguière. Différentes menaces existent et touchent les États, les entreprises et leurs collaborateurs. Les attaques contre les États et leurs institutions sont généralement l'œuvre d'États étrangers ou d'organismes dépendants de ces États et relèvent d'une véritable cyber-guerre.

Jean Louis Bruguière, 1er vice président honoraire du TGI de Paris, ancien coordinateur du pôle antiterroriste.

Impossible répression

Dans des situations de crise internationale, des stratégies cybernétiques d'attaque émergent. Leurs auteurs sont difficiles à identifier, d'où une impossible répression. De plus, celle-ci nécessite une coopération judiciaire internationale, compliquée à mettre en œuvre. C'est donc en totale impunité que les criminels agissent. « Chine, Corée du Nord, Iran, Russie… les pays agresseurs sont connus », dénonce Jean-Louis Bruguière. Quelles ripostes existent ? Les États européens ont agi en ordre dispersé et moins précocement que les États-Unis. En France, l'Ansi se charge de la lutte contre la cybercriminalité. Cette entité s'est développée de façon rapide et efficace. Mais Internet a profondément bouleversé la stratégie opérationnelle des organisations terroristes, qui ont mis en place des sites web impossibles à décrypter destinés au recrutement des djihadistes ou au maniement des engins explosifs et qui utilisent les réseaux sociaux pour diffuser leur propagande.

Vulnérabilité française

« Les entreprises sont-elles de simples victimes ou doivent-elles se considérer comme de véritables acteurs dans la lutte contre ces attaques ?, interroge Jean-Louis Bruguière. C'est tout l'enjeu de la lutte contre la cybercriminalité. » Les cyber-attaques sont très variées de la part de hackers qui s'adaptent toujours à la riposte. La France figure au 15e rang mondial des attaques, et dans le top 5 européen des attaques ciblées. « La vulnérabilité française vient du fait de la mollesse des cibles nationales », analyse l'ancien juge. Parmi les attaques : le phishing ou hameçonnage, la captation de données, l'interception de communications, le « rançogiciel ».

Culture de la sécurité

Les sociétés attaquées doivent bénéficier du concours des États et de leur fournisseur d'accès pour se protéger. Elles doivent aussi remédier aux failles de sécurité de leur système. La responsabilité des entreprises s'élargit à celle de leurs collaborateurs. « Les collaborateurs doivent prendre conscience du rôle qu'ils ont à jouer dans la sécurité informatique. » Ainsi, ne pas exposer son matériel informatique, générer de solides mots de passes, encadrer l'utilisation des réseaux sociaux. De même, ne pas utiliser des terminaux professionnels dans la sphère privé. « Sachez qu'un smartphone est un espion à distance. »

Gisèle Ducrot, expert en ingenierie et prévention

Typologie du cybercriminel

Répondant à Jean-Louis Bruguière, Gisèle Ducrot, experte en ingénierie et prévention, Philippe Eyraud, président de Mixel Agitateurs, Xavier Vahramian, avocat associé CMS Bureau Francis Lefebvre Lyon, Yves Veret, Senior Advisor de l'information Calao Finance, et André Viau, président de Sofired, ont débattu sous la houlette de Bernard Jacquand. Et sont revenus dans le détail sur la prévention de la cybercriminalité. Selon André Viau, il est difficile d'évaluer les cas de cybercriminalité, « car ils sont peu déclarés ». Les motivations des cybercriminels sont variables : goût du hacking, défense d'une idéologie, recherche de gain. Et Xavier Vahramian de dresser une typologie des attaques : escroqueries, vol de données, y compris par des salariés de l'entreprise, attaques à la réputation des entreprises. Ou de leurs dirigeants, comme le rappelle Philippe Eyraud, victime d'une campagne diffamatoire de la part d'un ancien salarié pour le faire accuser de pédophilie.

Philippe Eyraud, président de Mixel agitateur

Analyse de vulnérabilité

Les entreprises, leurs dirigeants et leurs collaborateurs sont exposés à des menaces sans en avoir vraiment connaissance, déplore Gisèle Ducrot, qui préconise une « nécessaire éducation aux cyber-risques ». « Contre lesquels des solutions existent », rassure Yves Veret, qui insiste sur la nécessité d'utiliser des outils de protection de confiance et certifiés par l'Ansi et préconise de procéder à une analyse systématique de vulnérabilité des systèmes. Car l'entreprise et leurs dirigeants sont responsables de leur cyber-sécurité. Des obligations s'imposent d'ailleurs aux entreprises, rappelle Xavier Vahramian, au titre des lois Informatique et Libertés et celle sur l'Économie numérique, telle la déclaration de fichiers de données personnelles. Et Philippe Eyraud de rappeler la responsabilité du chef d'entreprise quant à la vérification de la nature des données contenues sur ses serveurs, « surtout en cas de contenus illicites téléchargés par des collaborateurs ».

Xavier Vahramian, avocat associé CMS bureau Francis Lefebvre Lyon

Degré d'exposition

Réseaux sociaux, clouding, smartphones… les degrés d'exposition aux cyber-risques sont exponentiels. Cependant, pour Yves Veret, « on ne peut pas fuir l'évolution des technologies, même si elles sont génératrices de risques. Il faut donc être capable de les mesurer pour pouvoir y répondre ». Ainsi, l'externalisation du stockage de données doit être entourée de mesures drastiques de sécurité, insiste Xavier Vahramian. Et André Viau de conclure sur la correspondance des stratégies de défense des espaces cyber et maritimes. Outre la défense embarquée, un système de vigie peut également être mis en place, complété par l'assistance des institutions publiques, jusqu'à la poursuite physique des cybercriminels.

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

Source : http://acteursdeleconomie.latribune.fr/debats/conferences/2014-12-15/la-cyber-guerre-est-declaree.html
Par Nicolas Rousseau