L'entreprise victime d'une cyberattaque : quelles réponses juridiques ?

0

12 Jun 2014 ANSSI, cyberattaque, cybercriminalité, cyberespace by Aurelie Magniez

Les rapports d'analyse les plus récents et notamment le rapport de recherche du groupe américain de sécurité informatique FireEye intitulé « Pandemonium : Etats nations, la sécurité nationale et de l'Internet » confirment que la France fait partie des pays les plus visés en Europe en 2013 par les cyberattaques dites « avancées » comme l'Allemagne, l'Angleterre, la Suisse. Si aucun pays n'est aujourd'hui à l'abri des cyberattaques, il en est de même de l'entreprise qui, quel que soit son domaine d'activité, est également une cible très convoitée dans le cyberespace.

Louer une machine revient aujourd'hui à moins d'un dollar. La capacité d'attaquants à mettre en péril les systèmes d'information de l'entreprise est aujourd'hui basée sur des technologies disponibles et très accessibles. Avec 730 millions d'adresses IP actives au premier trimestre 2013 (Rapport trimestriel « State of the Internet », Akamai du 05 août 2013), les cyberattaques ciblent en priorité les entreprises (35%), l'e-commerce (32%), les médias (22%). L'entreprise connectée est une cible de choix, certains secteurs sont d'ailleurs plus vulnérables que d'autres : les activités à haute valeur ajoutée basées sur l'innovation, les technologies et le e-commerce sont les premières cibles des cyberattaques (15% des attaques). Face à la facilité de déclenchement et de réalisation d'une cyberattaque, l'entreprise qui n'est pas une victime consentante, choisit souvent de se taire pour préserver son image et sa réputation.

Selon le Forum Economique Mondial, la cybercriminalité pourrait engendrer une perte pour l'économie mondiale de 2 200 milliards d'euros d'ici 2020 (soit l'équivalent du PIB de la France en 2012). Trouver l'origine d'une attaque, utilisant des milliers ou des millions de machines réparties dans des dizaines de pays dans le monde, conduit souvent l'entité qui a été attaquée à renoncer à engager une action en justice. Pourtant, dans le même temps, en l'absence d'action en justice de l'entreprise, c'est la confiance des utilisateurs d'Internet qui est fortement atteinte et fragilisée surtout dans l'hypothèse d'une augmentation et d'une aggravation des cyberattaques.

Le cyberespace est parfois appelé aussi le 9ème continent, après l'Amérique du Nord, l'Amérique du Sud, l'Europe, l'Antarctique, l'Asie, l'Afrique, l'Océanie et la surface sur le globe terrestre représentant les mers et les océans. Il est aussi considéré comme le cinquième élément de conflictualité après l'air, l'espace, la terre et la mer.

Le cyberespace malgré son caractère transnational et international n'est pas hors du champ du droit même si le droit en vigueur n'est pas comparable à l'ensemble des réglementations disponibles pour encadrer les autres éléments de conflictualité, que sont la mer ou l'espace aérien. Cette contribution présente le cadre juridique applicable au cyberespace en montrant la portée mais aussi les limites et incohérences du droit du cyberespace. Elle précise les postures, ainsi que des tactiques et stratégies de cybersécurité et cyberdéfense pouvant être mises en œuvre par l'entreprise face à une cyberattaque.

Un arsenal juridique international encore insuffisant

Une législation internationale balbutiante

Parmi les acteurs de la gouvernance de l'Internet, certains réclament l'adoption d'un cadre juridique international pour le cyberespace. Il en est ainsi du secrétaire général de l'Union Internationale des Télécommunications (UIT) et de la position de la France, laquelle dans sa stratégie nationale en matière de défense des systèmes d'information (janvier 2011), encourage également «le renforcement ou l'édiction de règles juridiques dans le cyberespace ». Pour d'autres, l'édiction d'un cadre juridique international serait en tout état de cause illusoire, en raison des problématiques techniques résultant de l'identification du ou des auteurs d'une attaque et des problématiques de conservation des preuves sur la paternité de l'attaque et de l'attaquant.

L'unique instrument juridique à vocation internationale du droit du cyberespace est la convention internationale sur la cybercriminalité adoptée à Budapest le 23 novembre 2001 par le Conseil de l'Europe. Cette convention est en effet le seul instrument juridique international contraignant concernant la cybercriminalité. Cette convention comporte des dispositions de coopération judiciaire dans la lutte contre les différentes formes de cybercriminalité.

La France a ratifié la convention internationale du Conseil de l'Europe sur la cybercriminalité qui est entrée en vigueur le 1er mai 2006. Cette convention prévoit des dispositions de coopération judiciaire dans la lutte contre toutes les formes de cybercriminalité, en prenant en compte les faits ou les atteintes réalisées par l'utilisation de nouvelles technologies de communication. La France a également conclu différentes conventions bilatérales de coopération judiciaire en matière pénale applicable à des faits impliquant l'utilisation de nouvelles technologies et d'atteintes portées à des systèmes d'information.

Les réponses juridiques européennes

Si la législation internationale du cyberespace se révèle encore balbutiante du fait des nombreuses difficultés d'application, le droit européen est encore très en retard face aux cyberattaques dont l'entreprise est la victime malgré un certain nombre d'instruments juridiques existants.

La construction du droit européen du cyberespace qui n'a débuté qu'en 1995 pourrait toutefois servir de modèle pour légiférer au plan international.

La résolution du Conseil sur l'interception légale des télécommunications (1995)

Cette résolution du Conseil, la première à traiter les interceptions légales des communications, répond à l'objectif de disposer de normes comparables pour simplifier les interceptions sur le plan technique.

La directive 2006/24 sur les données de connexion (2006)

Cette directive faisait écho au plan européen à la convention internationale de Budapest de 2001. Elle a été invalidée très récemment par la Cour de Justice de l'Union Européenne (CJUE) par un arrêt du 8 avril 2014 au motif que la directive était contraire aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne. Cette directive jusqu'à l'arrêt récent de la CJUE était l'un des piliers fondateurs du droit du cyberespace.

Compte tenu de l'arrêt de la CJUE, au niveau français, les dispositions pertinentes en matière de conservation des données de connexion qui demeurent applicables sont les dispositions des articles L. 34-1 du Code des postes et des communications électroniques (CPCE) concernant les enquêtes judiciaires et L. 34-1-1 du CPCE concernant les enquêtes administratives. L'ensemble des autorités compétentes apprécie actuellement de manière circonstanciée l'impact de cette décision européenne sur le droit français.

La directive 2008/114/CE concernant le recensement et la désignation desinfrastructures critiques européennes (2008)

Cette directive qui constitue la première étape d'une approche progressive a pour objet de recenser et désigner les infrastructures critiques européennes (ICE), et d'évaluer la nécessité d'améliorer leur protection en définissant des méthodes communes de recensement et de désignation des risques, menaces et vulnérabilités touchant les points d'infrastructure pouvant être définies.

Bien que cette directive ne concerne actuellement que les secteurs de l'énergie et des transports, de nouveaux secteurs pourraient être ajoutés à l'occasion de son réexamen.

La directive 2013/40/UE relative aux attaques contre les systèmes d'information (2013)

Cette directive rapproche le droit pénal des États membres dans le domaine des attaques contre les systèmes d'information en fixant des règles minimales concernant

la définition des infractions pénales et les sanctions applicables, et de renforcer la coopération entre les autorités compétente. Sa transposition doit intervenir au plus tard en 2015.

Le principal apport de cette directive est l'incrimination de nouvelles infractions telles que l'accès illégal à des systèmes d'information, l'atteinte illégale à l'intégrité d'un système ou des données, l'interception illégale effectuée par des moyens techniques, de transmissions non publiques de données informatiques à destination, en provenance ou à l'intérieur d'un système d'information. Ces infractions pénales sanctionnent le fait d'inciter à commettre l'une des infractions précitées, mais également le fait de participer ou de se rendre complice ainsi que la tentative de commettre l'une des infractions précitées.

Cette directive prévoit en effet des sanctions sévères lorsque l'attaque contre un système d'information est commise par une organisation criminelle, ou que la cyberattaque est menée à grande échelle, en affectant un grand nombre de systèmes d'information, y compris lorsque l'attaque a pour objectif de créer un réseau zombie, ou lorsqu'une cyberattaque cause un préjudice grave, y compris lorsqu'elle est menée via un réseau zombie. Cette directive prévoit également des sanctions plus sévères que les sanctions existantes lorsqu'une attaque est menée contre une infrastructure critique des États membres ou de l'Union.

L'ensemble des instruments juridiques qui constituent les piliers du cyberespace européen sont également complétés par l'adoption par l'Union européenne d'une stratégie globale de cybersécurité ainsi que par les procédures d'identification et de recensement des infrastructures critiques européennes.

Les réponses juridiques françaises

Outre la convention internationale de Budapest et les principaux instruments de droit européen, le cadre juridique français en matière de cyberespace s'articule autour de deux axes :

Les restrictions à la liberté de communication

La loi 2004-575 pour la confiance dans l'économie numérique du 21 juin 2004 prévoit que la liberté de communication par voie électronique peut être limitée par le respect de la dignité de la personne humaine, de la liberté et de la propriété d'autrui, du caractère pluraliste de l'expression des courants de pensée et d'opinion et par la sauvegarde de l'ordre public.

En outre, la loi prévoit que l'autorité judiciaire peut prescrire en référé ou sur requête, à toutes personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature ou, à défaut, à toute personne dont l'activité est d'offrir un accès à des services de communication au public en ligne informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services, toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne.

La loi précitée prévoit également en matière de détection des sites web utilisés à des fins illicites, sous peine de sanctions pénales, que les deux catégories de personnes visées ci-dessus doivent mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance ce type de données.

Ces personnes ont également l'obligation, d'une part, d'informer promptement les autorités publiques compétentes de toutes activités illicites qui leur seraient signalées et qu'exerceraient les destinataires de leurs services, et, d'autre part, de rendre publics les moyens qu'elles consacrent à la lutte contre ces activités illicites.

La répression de l'utilisation d'Internet à des fins de terrorisme

Notre code pénal comporte également de nombreuses dispositions permettant de réprimer l'utilisation d'Internet à des fins de terrorisme. La loi du 5 mars 2007 a en effet introduit dans la loi du 29 juillet 1881 sur la liberté de la presse, un dispositif permettant de réprimer les faits d'apologie ou de provocation à commettre un acte de terrorisme résultant de messages ou informations mis à disposition du public par un service de communication en ligne, sous peine d'arrêt du service de communication en ligne.

Enfin, il convient d'avoir à l'esprit que le code pénal et en particulier l'article L. 323-1 incrimine le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données, ces faits étant punis de deux ans d'emprisonnement et de 30 000 euros d'amende.

La sensibilisation de l'ensemble de l'entreprise aux cyberattaques

L'entreprise qui souhaite anticiper une cyberattaque doit tenir compte du caractère protéiforme des cyberattaques et des profils et motivations des cyberattaquants pour choisir la posture la plus appropriée à adopter.

Le caractère protéiformes des cyberattaques

Les cyberattaques peuvent être classées en trois catégories :

- Les cyberattaques par déni de service lesquelles consistent à saturer une machine ou un système d'information en réseau sur Internet en dirigeant vers celle-ci ou celui-ci un volume très important de requêtes, jusqu'à ce que la machine ou le système ne soit plus capable de fonctionner ;
- Les cyberattaques portant atteintes à l'intégrité des données ou portant altération aux données ;
- Les cyberattaques visant à détruire les systèmes d'information.

Les profils et motivations des cyberattaquants

La dernière étude réalisée par Rand Corporation sur les marchés noirs de la cybercriminalité révèle que sur un plan géostratégique les domaines d'expertise et les champs d'actions des cyberattaquants varient d'un pays à l'autre. En effet, selon cette étude, « c'est en Chine, en Amérique latine et en Europe de l'Est que les cybercriminels sont les plus actifs pour les attaques malicielles » tandis que les cyberattaquants russes, « se distinguent plutôt sur le plan de la qualité ». Rand Corporation a par ailleurs relevés que les cybercriminels localisés au Vietnam sont spécialisés dans le piratage du commerce électronique

Ainsi que cela été rappelé, l'identification de l'origine de la cyberattaque ainsi que la paternité du déclenchement sont autant de problèmes techniques qui peuvent réduire la portée et surtout l'efficience du droit du cyberespace.

Les postures

La première posture de l'entreprise souhaitant anticiper le risque de cyberattaque consiste à mettre en place une politique de cybersécurité adaptée à ses besoins et à ses systèmes d'information, lui permettant de réduire de manière drastique le temps qui s'écoule avant la découverte de la cyberattaque, ce qui implique d'implémenter dans son système d'information des capteurs d'informations pertinents et protégés contre des cyberattaques.

Dans la mesure où les cyberattaques sont protéiformes et que les vulnérabilités d'un système d'information sont multiples, il est certain que l'entreprise ne peut pas protéger chaque élément de son système d'information avec le même niveau de protection. C'est la raison pour laquelle, la deuxième posture pour l'entreprise, consiste pour pouvoir assainir le système d'information en cas de cyberattaque, à segmenter le système d'information de l'entreprise. En le segmentant, l'entreprise pourra ainsi plus facilement rendre étanche tout ou partie du système d'information en cas de cyberattaque.

Les recommandations aux DSI et RSSI

Selon le rapport annuel de PandaLabs, il était possible en 2012 de trouver sur Internet pas moins de 26 millions de codes malveillants disponibles en téléchargement. Pour l'ANSSI, la majeure partie des attaques informatiques sur lesquelles elle est intervenue auraient pu être évitées si des règles d'hygiène en matière informatique avaient été appliquées par les entreprises. Il est donc en premier lieu de la responsabilité des équipes dirigeantes dans l'entreprise d'être sensibilisées aux risques que représentent les cybermenaces et aux conséquences extrêmement lourdes que pourraient avoir l'absence d'adoption d'une politique de sécurité pertinente et adaptée au système d'information de l'entreprise.

Le plus grand défi pour l'entreprise reste encore l'insuffisance de sensibilisation de l'ensemble des personnels face à l'ingéniosité des cyber-délinquants et au caractère protéiforme des cyberattaques. Notre principale recommandation à l'attention des DSI et des RSSI est de s'assurer qu'ils disposent bien d'une politique de sécurité connue de tous et dont l'application doit être régulièrement contrôlée et auditée. Il est également recommandé aux DSI et aux RSSI de s'assurer qu'ils ont bien mis en œuvre les « 40 règles d'hygiène informatique » disponible sur le site de l'ANSSI.

L'ANSSI met également à la disposition des DSI et RSSI un ensemble d'autres guides et recommandations qui sont très accessibles y compris aux TPE permettant de sécuriser les postes de travail et les serveurs, mais également la messagerie ou encore les liaisons sans fil dans l'entreprise.

Didier Gazagne,
Avocat
Docteur en droit
Directeur des département Energie, Intelligence économique, Cybersécurité et Cyberdéfense
Alain Bensoussan Selas Avocats – Réseau Lexing

Alain Bensoussan-Avocats est un cabinet d'avocat entièrement dédié au droit des technologies avancées depuis 1978. Pour la 3e année consécutive depuis 2010, il a été distingué par ses pairs, « Best Lawyer » de l'année dans le domaine du Droit des nouvelles technologies.
Site : http://www.alain-bensoussan.com/