Skadden

PRIVACY & CYBERSECURITY UPDATE

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP & AFFILIATES

JUNE 2013

Flaming Worms, Stuxnets et autres Cyber Menaces – La Réponse de l'Union Européenne

Les médias n'ont de cesse de se faire l'écho d'attaques de botnet à l'assaut de Spamhaus, de flaming worms voleurs d'informations stratégiques au Moyen-Orient ou des dommages causés par Stuxnet, l'arme fatale capable de détruire les réacteurs nucléaires iraniens. Derrière ces néologismes barbares se cache une réelle et sérieuse menace contre grand nombre d'entreprises : les cyber-attaques. Vu l'importance et l'étendue des données informatiques stockées par les entreprises aujourd'hui, tout accès clandestin est de nature à provoquer des conséquences dommageables allant du cauchemar diplomatique au préjudice financier significatif. Or, en matière de cyber-attaques, de récents exemples ont démontré qu'aucune structure n'est trop grosse ni trop sophistiquée pour être à l'abri.

Averties des risques encourus, les entreprises doivent prendre des mesures appropriées tout en se conformant à un environnement réglementaire mondial en perpétuelle évolution. En plus des mesures édictées par les Etats-Unis pour lutter contre les risques d'atteinte à la cyber-sécurité[1], la Commission Européenne a publié une proposition de directive pour la sécurité des réseaux et de l'information[2]. Si elle est adoptée, la directive imposera d'importants changements dans la manière dont les entreprises européennes et toutes celles qui font des affaires en Europe utilisent les technologies de l'information.

Propagation et Coûts des Cyber-Attaques

Face à l'augmentation du nombre de hackers et des infiltrations illégales des systèmes d'information publics et privés, les autorités gouvernementales et le secteur privé se sont intéressés à l'exposition aux cyber-attaques des systèmes d'information sensibles. Il est désormais connu que le profil du cybercriminel peut correspondre à celui d'un adolescent hacker, d'un opportuniste cherchant à voler de l'argent, d'un hacker "sophistiqué" motivé par le désir de neutraliser les systèmes informatiques des entreprises, ou encore à celui d'un agent étatique prolongeant, au moyen d'armes informatiques, la guerre et l'espionnage traditionnels dans le domaine du numérique. Le cyber-espionnage économique est particulièrement intrusif. Le Ministre des finances français a été infiltré fin 2010 et en 2012, et même les bureaux de l'ancien Président Sarkozy ont été infectés[3].

En 2012 seule une entreprise de l'Union Européenne sur quatre disposait d'une politique régulièrement actualisée de sécurisation des technologies de l'information et de la communication, laissant les Etats Membres vulnérables et mal préparés pour repousser le nombre grandissant de cyber-attaques sophistiquées[4]. Parmi ces Etats-Membres, les gouvernements français et allemands se sont fait les hérauts de la nécessité d'une action décisive[5].

Mesures de Cyber-sécurité Prises par l'UE

Le 7 février 2013, la Commission Européenne a publié une proposition de directive sur la sécurité des réseaux et de l'information conçue pour mettre en œuvre la stratégie de cyber-défense de la Commission pour un Internet ouvert, sûr et sécurisé. Afin de remplir ces objectifs, la Commission, constatant que l'approche fondée sur la base du volontariat jusqu'alors suivie en matière de sécurité des réseaux et de l'information était insuffisante pour obtenir les résultats escomptés[6], a souligné la nécessité pour les 27 Etats-Membres de travailler de manière unie avec un degré d'exigence et des objectifs législatifs communs. La Commission fait état de ce que les Etats Membres ne sont pas tous au même niveau – certains disposant de capacités plus importantes

LEARN MORE

Si vous avez des questions relatives à cet article, n'hésitez pas à contacter l'équipe Skadden.

Pierre Servan-Schreiber
Paris
+33.1.55.27.11.30
pierre.servan-schreiber@skadden.com

Stuart D. Levi
New York
+1.212.735.2750
stuart.levi@skadden.com

Shari L. Piré
Paris
+33.1.55.27.11.43
shari.pire@skadden.com

Joshua F. Gruenspecht
Washington, D.C.
+1.202.371.7316
joshua.gruenspecht@skadden.com

68, rue du Faubourg
Saint-Honoré
75008 Paris, France
Telephone: +33.1.55.27.11.00

Four Times Square
New York, NY 10036
Telephone: +1.212.735.3000

WWW.SKADDEN.COM

et étant mieux équipés pour défendre leurs réseaux et systèmes informatiques que d'autres[7]. Cette disparité de capacité et de préparation est considérée par la Commission comme un obstacle à la coopération et la collaboration effective des Etats-Membres, sans lesquelles l'existence d'une cyber-protection à l'échelle de l'UE reste illusoire[8].

En l'état actuel du droit, seules les entreprises de télécommunications sont tenues de mettre en œuvre des mesures de gestion des risques et de signaler les incidents affectant les réseaux et systèmes informatiques[9], tandis que seuls les responsables du traitement[10] doivent mettre en place des mécanismes de sécurité afin d'assurer la protection des informations personnelles[11]. En tant que telle, la législation actuelle reste muette sur la gestion des incidents survenant dans les secteurs autres que celui de la télécommunication, tels que les secteurs des transports, des bourses de valeurs, de l'aéronautique, des médias, de l'énergie ou de la banque qui chacun pourrait être lourdement affecté par des violations d'infrastructures informatiques[12]. La Commission estime qu'à défaut de régime légal plus complet, les Etats Membres manquent peut-être d'incitation pour signaler ou évaluer les failles, gérer les risques ou concevoir les solutions appropriées[13].

La Proposition de Directive vise, entre autres, à combler ce vide. En cas d'adoption, la Proposition de Directive exigera des administrations publiques et des acteurs de marché la mise en œuvre et le maintien de mesures de gestion des risques ainsi que la signalisation des atteintes importantes affectant les réseaux et systèmes informatiques aux autorités compétentes[14]. La Commission sera investie de l'autorité nécessaire pour imposer les formats et procédures prévalant à la notification de ces incidents[15]. De plus, les administrations publiques et les acteurs de marchés concernés seront tenus de fournir l'information nécessaire pour évaluer la sécurité de leurs réseaux et systèmes informatiques et seront soumis à des audits de sécurité réguliers dont les résultats seront transmis aux autorités compétentes[16]. Des sanctions pourront être infligées à ceux qui ne satisferaient pas ces tests de sécurité[17].

Quelles Entreprises Seraient Affectées?

La Proposition de Directive définit la notion d'acteur de marché en y incluant certains prestataires de services de la société de l'information ainsi que les opérateurs d'infrastructures critiques essentielles "au maintien de fonctions économiques et sociétales vitales dans le domaine de l'énergie, des transports, des services bancaires, des bourses de valeurs et de la santé[18] ." Une annexe à la Proposition de Directive fournit une liste non exhaustive d'acteurs de marché qui inclut les réseaux sociaux, les moteurs de recherche, les services informatiques en nuage, les opérateurs sur les marchés du gaz et de l'électricité, les exploitants de raffinerie et d'autres infrastructures de traitement, les transporteurs aériens, les chemins de fer et le secteur des services logistiques, certains établissements de crédit, les contreparties centrales/chambres de compensation ainsi que les hôpitaux et les entités fournissant des soins de santé[19].

Différences entre les Projets de Réglementation Relatifs à la Cyber-sécurité

Au moment où la Proposition de Directive est débattue en Europe, un régime théoriquement moins normatif est en train de prendre forme aux Etats-Unis. Un récent décret (*executive order*) américain (le Décret Cyber-Sécurité) appréhende le partage d'information et la réglementation relative à la cyber-sécurité des infrastructures sensibles. Ces "infrastructures sensibles" s'entendent des actifs du secteur privé dont la perte, le disfonctionnement ou la destruction affecterait gravement la sécurité, la santé publique ou la prospérité économique des Etats-Unis[20]. La Directive Présidentielle *(Presidential Directive*) accompagnant le Décret Cyber-Sécurité laisse entendre que les différentes catégories d'acteur de marché visées par la Proposition de Directive en UE pourraient être à terme soumises à de nouvelles obligations aux Etats-Unis en vertu du Décret Cyber-Sécurité. Les catégories d'entités concernées par les projets de réglementation ne sont pas cependant parfaitement parallèles. Contrairement à la Proposition de Directive, le Décret Cyber-Sécurité et la Directive Présidentielle identifient explicitement les secteurs de l'alimentation, de l'agriculture et les industries sensibles parmi les secteurs visés, mais excluent les services informatiques en nuage, les réseaux sociaux et les moteurs de recherche[21].

Le décret Cyber-Sécurité prévoit une procédure selon laquelle le Département de la Sécurité Intérieure (*Department of Homeland Security*) (DHS) évalue le besoin d'édicter des mesures de régulation en matière de cyber-sécurité à l'égard d'activités à infrastructures sensibles[22] et charge l'Institut National des Normes et de la Technologie (*National Institute of Standards and Technology*) (NIST) de développer un système conçu pour fournir aux propriétaires d'infrastructures sensibles et aux acteurs des mesures et contrôles, qui, si adoptés, peuvent réduire les risques liés à la cyber-sécurité[23]. Alors que le Décret Cyber-Sécurité prévoit que la mise en place du système par le secteur privé reste libre, il a été demandé à certains organismes chargés de la réglementation de secteurs spécifiques de remédier aux déficiences détectées par le DHS[24]. Plus spécifiquement, le Décret Cyber-Sécurité exige de chacun de ces organismes d'examiner l'ensemble de sa réglementation à la lumière des conclusions du DHS. Si le cadre réglementaire s'avère inefficace pour contrer les risques en matière de cyber-sécurité, les organismes auront à charge, dans la limite de leurs pouvoirs respectifs, d'assurer la mise en conformité de leur secteur d'activité avec les recommandations fournies par le système du NIST[25]. En conséquence, les exploitants d'infrastructures sensibles implantées aux Etats-Unis seraient prudents de considérer le système du NIST de la manière dont leurs homologues de l'UE auront à considérer la Proposition de Directive – comme un régime réglementaire obligatoire.

En raison de ces différentes manières de réguler les réseaux et systèmes privés aux Etats-Unis et en UE les acteurs pourraient croire à tort que les mesures de sécurité qu'ils ont adoptées pour se conformer à l'un de ces régimes réglementaire ou législatif suffisent pour satisfaire à l'autre. Les acteurs susceptibles d'être assujettis aux deux régimes devront rester attentifs car ces deux types d'approche vont continuer d'évoluer dans les prochains mois.

Prochaines Etapes

La Proposition de Directive a été soumise au Parlement européen et au Conseil pour discussion et adoption. En cas de vote favorable, les Etats Membres disposeront de 18 mois pour la transposer ou l'incorporer à leur législation nationale respective. Pendant cette période, les acteurs concernés par la Proposition de Directive devraient commencer à évaluer la sécurité de leur systèmes actuels comme si la Proposition de Directive était déjà en vigueur, de manière à identifier les vulnérabilités auxquelles ils devront remédier.

De manière plus générale, toutes les entreprises privées devraient continuer de surveiller étroitement ce domaine et entreprendre les étapes nécessaires à la réduction des risques associés aux cyber-menaces.

---

1 *Voir* Antoinette C. Bush, Stuart D. Levi, Ivan A. Schlager, John M. Beahn et Joshua F. Gruenspecht, "Privacy and Cybersecurity Updated: President Issues Cybersecurity Executive Order", *Privacy & Cybersecurity Update*, 13 fév. 2013 http://www.skadden.com/newsletters/Privacy_and_Cybersecurity_President_Issues_Cybersecurity_Executive_Order.pdf ; voir aussi Antoinette C. Bush, Stuart D. Levi, Ivan A. Schlager, John M. Beahn et Joshua F. Gruenspecht, "Privacy & Cybersecurity Update: NIST Issues Request for Information on Critical Infrastructure Cybersecurity Practices", 5 mars 2013 http://www.skadden.com/sites/default/files/publications/Privacy_Cybersecurity_Update_%20NIST_Issues_Request_for_Information_on_Critical_Infrastructure_Cybersecurity_Practices.pdf.

2 Proposition de Directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union (Proposition de Directive) Bruxelles, 7 fév. 2013 http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_fr.pdf.

3 Saskya Vandoorne, "Cyber attack hit French Finance Ministry," government says, CNN, 7 mars 2011 http://www.cnn.com/2011/WORLD/europe/03/07/france.cyberattack/index.html?_s=PM:WORLD; Emmanuelle Paquette, "Cyberattaque contre l'Élysée: la défense de Washington", L'Express, 20 nov. 2012 http://lexpansion.lexpress.fr/high-tech/cyberattaque-contre-l-elysee-la-defense-de-washington_361245.html.

4 Voir discours de Neelie Kroes à la Commission Européenne, "Towards a coherent international cyberspace policy for the EU," 30 janv. 2013, prononcé à l'occasion de la Global Cyber Security Conference à Bruxelles,

http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=9568 (Discours à la Commission), p. 3 ; voir aussi Communiqué de presse de la Commission Européenne "Un plan de cybersécurité de l'UE pour protéger l'internet ouvert et les libertés en ligne", 7 fév. 2013 http://europa.eu/rapid/press-release_IP-13-94_fr.htm (Communiqué de Presse UE).

5 Le gouvernement français recommande de renforcer les standards de sécurité imposés aux activités exercées dans les secteurs sensibles, de développer les outils de gestion des risques et de les rendre disponibles aux PME et de mener, dans les limites de la réglementation, des tests sur la sécurité des logiciels et sur les moyens de réponse aux attaques. Antton Achiary, Joël Hamelin et Dominique Auverlot, *La Note d'analyse, n°324, Centre d'analyse stratégique*, mars 2013. Le Ministre Fédéral de l'Intérieur allemand a publié plusieurs projets d'amendements, qui, en cas d'adoption, imposeraient aux exploitants d'infrastructures sensibles d'informer l'Agence Fédérale Allemande pour la Sécurité de l'Information (BSI) de toute atteinte portée à leur cyber-sécurité. *Voir* Projet du Ministre Fédéral de l'Intérieur http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_it-sicherheitsgesetz.pdf;jsessionid=B3769DFABA3DFAD5C7FE3DF0B59948F9.2_cid287?__blob=publicationFile.

6 Exposé des motifs de la Proposition de Directive § 1.1 (Motifs de la Directive).

7 *Id.*

8 *Id.*

9 *Voir* Directive 2009/140/CE du Parlement européen et du Conseil du 25 novembre 2009, Art. 13 bis, modifiant les directives 2002/21/CE relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, 2002/19/CE relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexions et 2002/20/CE relative à l'autorisation des réseaux et services de communications électroniques. La réglementation Française est plus large. En France, les opérateurs télécoms et les fournisseurs d'accès à Internet sont tenus de signaler les atteintes à la sécurité des données à la Commission Nationale de l'Informatique et des Libertés. Voir Ordonnance n° 2011-2012 du 24 août 2011 relative aux communications électroniques.

10 Un responsable du traitement est "la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel". Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données (la "Directive Protection des Données"). A titre d'exemple sont considérés comme responsables du traitement les banques, les compagnies aériennes, les chemins de fer, les hôpitaux et hôtels. Le 25 janvier 2012, la Commission a publié une proposition de règlement visant à remplacer la Directive Protection des Données. Voir Proposition de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:FR:PDF.

11 *Voir* Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

12 *Voir* Motifs de la Directive.

13 *Voir* Stratégie de Cybersécurité de l'Union Européenne : *un cyberespace ouvert, sûr et sécurisé*, Communication conjointe au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, 7 fév. 2013, p. 6 http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_fr.pdf.

14 Proposition de Directive Art. 14. Les microentreprises sont exemptées des obligations en matière de gestion des risques et de signalisation instaurées par la Proposition de Directive. *Voir Id.*, qui définit la notion de microentreprise conformément au sens de l'Art. 3 de la Recommandation de la Commission 2003/361/CE du 6 mai 2003 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:fr:PDF.

15 *Id.*

16 *Id.*

17 *Voir* Proposition de Directive Art. 17, qui dispose que les Etats Membres fixent des règles relatives aux sanctions applicables en cas d'infraction aux dispositions nationales adoptées en vertu de la Proposition de Directive.

18 Proposition de Directive Art. 3.

19 Proposition de Directive Annexe II.

20 The White House – Office of the Press Secretary, "Executive Order: Improving Critical Infrastructure Cybersecurity", 12 fév. 2013, § 2. La directive présidentielle accompagnant le Décret Cyber-Sécurité définit les infra-

structures sensibles en y incluant les 16 secteurs suivants : chimie, infrastructures commerciales, communications, industries sensibles, barrages hydrauliques, industrie militaire, services d'urgence, énergie, services financiers, nourriture et agriculture, installations gouvernementales, services de santé et santé publique, technologies de l'information, services nucléaires, systèmes de transport, eau et systèmes de traitement de l'eau. *Voir Presidential Policy Directive* PPD-21: *Critical Infrastructure Security and Resilience*, 12 fév. 2013 (Directive Présidentielle).

21 "Le Secrétaire [à la Sécurité Intérieure] (*Secretary of Homeland Security*) n'a pas vocation à identifier de produits de technologie informatique commercialisés ou de services de technologie informatique au consommateur en vertu du présent article." Décret Cyber-Sécurité § 9.

22 Décret Cyber-Sécurité § 10.

23 Décret Cyber-Sécurité § 7a.

24 Décret Cyber-Sécurité § 10.

25 *Id.*