AVOCATS

SCHELLENBERG WITTMER

FÉVRIER 2019

Newsletter

Auteurs:
Roland Mathys, LL.M. (LSE)
Andreas Hösli, LL.M.

ICT / CRIMINALITÉ ÉCONOMIQUE ET MISE EN CONFORMITÉ

Réaction face aux cyberattaques – Quel comportement adopter?

Les risques liés aux cyberattaques à l'encontre des entreprises et de leurs dirigeants ne cessent de croître. Bien que conscientes de l'existence de menaces résultant de ces risques potentiels, les entreprises ne savent souvent pas comment réagir en cas d'attaques avérées, en particulier s'il y a lieu d'impliquer les autorités (principalement les autorités pénales spécialisées en matière de cybercriminalité ou encore la centrale d'enregistrement MELANI).

1 LES CYBERATTAQUES, MISE EN PÉRIL DE LA VIE DES ENTREPRISES

La presse relate presque quotidiennement des cas de **cyberattaques**. La cybercriminalité est devenue depuis longtemps un modèle d'affaire attrayant pour des malfaiteurs dont le niveau de professionnalisme ne cesse d'augmenter et dont la cible est le plus souvent des **entreprises** et leurs **dirigeants**.

La médiatisation de graves cyberattaques ayant paralysé les systèmes informatiques d'entreprises et d'institutions publiques – notamment d'hôpitaux – au moyen de logiciels de cryptage (mot-clé *NotPetya*) a amené à une **prise de conscience** des sphères dirigeantes quant à la problématique. Des mesures concrètes font toutefois toujours défaut. Outre les **pertes financières** massives (se comptant parfois en centaines de millions) et les **atteintes à la réputation** des entreprises concernées, les attaques contre des infrastructures essentielles peuvent également avoir de graves conséquences sociales. Elles génèrent notamment des craintes justifiées quant au risque d'éventuelles **amendes** dues à des fuites de données à caractère personnelles (Règlement général européen sur la protection des données, **RGPD**). Pour cette raison, les cyberattaques représentent des **risques opérationnels** pour les entreprises susceptibles, dans certains cas, de mettre en péril l'existence de celles-ci. Ces situations doivent donc être traitées avec des mesures adéquates. Il est d'importance capitale que **les cadres d'entreprises se saisissent de cette problématique** afin d'éviter le scénario catastrophe.

2 ASSAILLANTS CRÉATIFS

Les **méthodes d'attaque** sont nombreuses et exploitent notamment les failles de sécurité informatique (logicielle ou de matériel), l'inadéquation des mots de passe ainsi que la "vulnérabilité humaine". En outre, la protection réduite des appareils connectés à Internet (*Internet des objets*, par ex., les caméras de sécurité) offrent des possibilités d'attaque considérables. La méthode courante est celle des attaques par *Distributed Denial of Service* (DDoS) (correspondant au fait d'inonder un réseau en envoyant un grand nombre de requêtes pour le surcharger et le paralyser temporairement) ou le *phishing* (obtention frauduleuse de données confidentielles, par ex., au moyen d'e-mails hameçon). L'exécution de paiements non autorisés (prétendument sur instruction de la direction de l'entreprise) est pour sa part connue sous le nom d'arnaque au président. Plus récemment et de façon fréquente, le chan-

tage est observé sous forme de *ransomware* (rançongiciel), où des logiciels malveillants cryptent des données ou des réseaux entiers et une rançon (sous forme de monnaie cryptée telle que le *Bitcoin* par ex.) est demandée pour le décryptage.

Tel qu'indiqué dans notre **newsletter de février 2018**, la **prévention**, l'**action** et la **réaction** sont d'une importance capitale dans le traitement juridique des cyberrisques. Pourtant, de nombreuses entreprises restent encore démunies quant à l'attitude à adopter en cas de cyberattaque. En particulier, se pose la question de savoir s'il est nécessaire d'annoncer un cyber-incident aux autorités et quelle serait, le cas échéant, l'autorité compétente pour intervenir.

"Les cyberattaques ciblent souvent les entreprises et leurs dirigeants."

3 EN PRINCIPE: PAS D'OBLIGATION D'ANNONCER

En cas de cyberattaque majeure, il appartient (dans l'idéal) aux *Computer Security Incident/Emergency Response Teams* (CSIRT/CERT) de l'entreprise de prendre immédiatement les mesures nécessaires pour limiter le dommage et pour rétablir son bon fonctionnement.

Outre certaines obligations d'information *ad hoc* pour les sociétés cotées et les obligations légales de notification dans certains secteurs (applicables par exemple aux établissements financiers réglementés, aux fournisseurs de services de télécommunication ou aux entreprises actives dans le secteur de la santé), une cyberattaque n'est actuellement **soumise à aucune obligation d'annonce** à une autorité suisse. Il peut toutefois exister une obligation de notifier une cyberattaque qui a mené à une **violation de la protection des données** en application du RGPD. L'inclusion d'une telle règle est aussi prévue dans le cadre de l'actuelle révision de la Loi fédérale sur la protection des données (**LPD**).

4 LES ANNONCES MELANI

Les cyberattaques peuvent être signalées à la Centrale fédérale d'enregistrement et d'analyse pour la sûreté de l'information (**MELANI**) via le formulaire d'annonce (www.melani.admin.ch). L'annonce peut également se faire de façon anonyme, ce qui rend cependant impossible une réponse de la part de MELANI. Ces annonces - environ 8'000 par an - permettent à MELANI de se faire une idée précise de la situation globale des cyberattaques en Suisse. MELANI exploite également une plateforme permettant de signaler les **activités de phishing** (www.anti-phishing.ch) et de régulièrement assurer la désactivation rapide des sites de phishing en Suisse. Indépendamment de MELANI, l'art. 15 de l'Ordonnance sur les domaines Internet (**ODI**) offre la possibilité, en cas d'abus présumé (en particulier *phishing* et diffusion de logiciels malveillants), de bloquer les noms de domaines par l'intermédiaire de l'opérateur de registre (SWITCH).

La mission de MELANI consiste principalement en la protection et le support des **exploitants d'infrastructures critiques** (par exemple dans les secteurs financiers, énergétiques, des télécommunications et de la santé). La plateforme offre à ce nombre limité d'usagers le support nécessaire pour faire face aux cyberattaques, notamment par le biais des analyses techniques effectuées par son organe associé, le **GovCERT** (CERT de l'Administration fédérale). En outre, MELANI permet des échanges confidentiels avec d'autres exploitants d'infrastructures critiques. Les services de MELANI ne sont cependant pas disponibles (ou ne le sont que dans la mesure du possible) aux autres entreprises (telles que les particuliers et les PME qui n'exploitent pas d'infrastructures critiques; l'étendue des activités de MELANI doit être élargie à l'avenir, voir ci-dessous). MELANI ne mène pas non plus d'investigations proprement dites, cette responsabilité incombant aux autorités de poursuite.

5 L'IMPLICATION DES AUTORITÉS PÉNALES

5.1 LA POURSUITE PÉNALE 2.0

Les poursuites pénales dans le domaine du numérique posent aux autorités des défis majeurs et novateurs. Les auteurs des attaques sont en principe des professionnels qui agissent le plus souvent depuis l'étranger et utilisent le dénommé *darknet*. En outre, beaucoup de **nouvelles questions juridiques** se posent et attendent d'être clarifiées par les hautes instances judiciaires, par exemple en ce qui a trait à la confiscation des données volées.

"Les autorités de poursuite pénale en matière de cyber sécurité ont un savoir-faire spécifique."

Afin de tenir compte de l'évolution croissante de la criminalité dans le domaine numérique, de nombreux cantons ainsi que la Confédération ont mis en place des **unités dévouées** chargées d'enquêter spécifiquement sur les cybercrimes. Depuis 2013, le canton de Zurich dispose même de son propre **centre de compétence en cybercriminalité** regroupant des spécialistes du ministère public et de la police. Ce centre a permis de nombreux succès, tels que la restitution de bitcoins volés à leurs propriétaires lésés. En 2017, 240 procédures ont été clôturées, dont 23 % par voie d'ordonnance pénale, 10 % par un renvoi en accusation et 67 % par un classement ou une suspension de la procédure.

Le **Ministère public de la Confédération** mène dans les domaines qui ressortent de sa compétence, plusieurs procédures complexes en matière de cybercriminalité. La Police judiciaire fédérale dispose de son propre département informatique forensique/cybercriminalité. Par ailleurs, l'Office fédéral de la police (**Fedpol**) exploite une plateforme sur laquelle tout incident lié à la cyber sécurité peut être signalé (www.cybercrime.admin.ch).

5.2 LA PLAINTE PÉNALE

En cas de cyberattaques d'envergure, il convient d'examiner si, outre le traitement de l'attaque par le service informatique interne de l'entreprise concernée (par exemple au moyen d'une enquête interne), une éventuelle notification à MELANI et l'intervention des autorités pénales sont appropriées.

Alors que l'entreprise concernée (ou son CSIRT/CERT) se concentre principalement sur sa propre défense vis-à-vis de la cyberattaque (qui peut perdurer dans le temps) et sur le rétablissement du fonctionnement normal des affaires,

la tâche principale des autorités pénales est la **conservation des preuves** ainsi que la **localisation et l'identification** des auteurs présumés. Cela peut être très utile par la suite, en vue de l'éventuelle **restitution** des valeurs volées.

Les investigations impliquent souvent l'utilisation de **mesures de surveillance secrètes** (cf. art. 269 ss du Code de procédure pénale, **CPP** ainsi que la Loi fédérale sur la surveillance de la correspondance par poste et télécommunication, **LSCPT**). Tel est le cas, par exemple, de la collecte d'e-mails non lus sur le serveur du fournisseur qui permet de procéder à une surveillance en temps réel.

> "Dans la plupart des cas, il n'existe pas d'obligation spécifique de signaler les cyberattaques."

En règle générale, les chances de succès d'une enquête pénale sont considérablement plus élevées si les cyberattaques sont signalées **rapidement** après qu'elles aient eu lieu. Les procureurs spécialisés en cybercriminalité sont formés pour ouvrir immédiatement une enquête en cas d'urgence. Idéalement, ils travaillent en étroite collaboration avec les services informatiques de l'entreprise concernée. Les **preuves** souvent utiles comprennent les adresses IP et les URL, les données secondaires ou les fichiers de journalisation (*logfiles*).

Bien que l'on ne dispose pas de statistiques fiables, on peut supposer qu'un **grand nombre de cyberattaques** contre des entreprises **ne sont pas signalées**. D'une part, toutes les attaques ne sont pas identifiées et, d'autre part, de nombreuses entreprises sont réticentes à porter les incidents à l'attention des autorités, notamment en raison de l'atteinte **éventuelle à leur réputation**. Si une enquête pénale aboutit à un procès, celui-ci est généralement ouvert au public, de sorte que toutes les informations sensibles de l'entreprise concernée se retrouvent divulguées. Néanmoins, les infractions en question - telles que les infractions contre la sécurité informatique (art. 143, 143bis, 144bis, 147 et 150 du Code pénal, **CP**), la fraude (art. 146 CP), l'extorsion (art. 156 CP) ou les services de renseignements économiques (art. 273 CP) - sont en partie des infractions poursuivies d'office qui doivent être investiguées indépendamment de la volonté du plaignant. La réticence des entreprises à devoir partager avec des tiers des informations sensibles (par exemple concernant leur propre infrastructure informatique) est compréhensible. Ces réserves peuvent être contrées, dans la mesure du possible, par des **discussions préliminaires informelles** avec le ministère public. Dans ce contexte, la disponibilité du ministère public de respecter toute déclaration ultérieure dite de "désintérêt" de la part de l'entreprise qui a dénoncé l'affaire doit être clarifiée. En outre, la restriction du droit de consulter les dossiers afin de protéger les intérêts privés de l'entreprise à la confidentialité (art. 108 CPP) peut également être envisagée.

5.3 L'ENTRAIDE JUDICIAIRE 2.0

En raison de la nature transnationale des crimes, les chances de succès des enquêtes pénales dépendent dans une large mesure du bon fonctionnement de l'**entraide judiciaire** avec d'autres pays. Les expériences varient considérablement d'un pays à l'autre.

Dans ce contexte, la *Convention sur la cybercriminalité* (*Convention on Cybercrime*, **CCC**) du Conseil de l'Europe, entrée en vigueur pour la Suisse le 1er janvier 2012 – également signée par des Etats comme les Etats-Unis, l'Australie et le Japon – est particulièrement importante. L'un des objectifs de la CCC est de faciliter l'assistance judiciaire dans le domaine du cyberespace. En particulier, l'art. 32 al. b CCC prévoit l'**accès direct** aux données (ou la réception de celles-ci) situées sur le territoire d'un autre Etat contractant, à condition que le **consentement** de la personne légalement autorisée à divulguer les données en question ait été obtenu (il s'agit notamment du cas d'un fournisseur étranger de services Internet qui s'est réservé un tel droit dans les directives d'utilisation des données vis-à-vis de ses clients). Toutefois, selon la jurisprudence du Tribunal fédéral, la collecte transfrontalière souveraine de données (soit sans consentement) des autorités pénales suisses auprès de prestataires domiciliés à l'étranger est inadmissible en application du **principe de territorialité**, l'entraide internationale en matière pénale étant justement prévue à cet effet (BGE 141 IV 108; *JdT 2015 IV p. 207*).

Du point de vue inverse (soit l'accès des autorités étrangères à des données situées en Suisse), le *Clarifying Lawful Overseas Use of Data Act* (**CLOUD Act**), entré en vigueur aux Etats-Unis en mars 2018, prévoit que les autorités judiciaires américaines peuvent accéder (par l'intermédiaire de fournisseurs d'accès) aux données situées hors des Etats-Unis. Ce pouvoir d'accès souverain aux données localisées en Suisse est potentiellement en conflit avec l'art. 271 CP (actes exécutés sans droit pour un Etat étranger).

6 PERSPECTIVES

Dans le cadre de la Stratégie nationale de protection de la Suisse contre les cyberrisques 2018-2022 (SNPC II), sont prévues en particulier, la création d'un **Centre de cybercompétence** sur le plan fédéral et d'une Cyber-force de l'armée. Les premières décisions stratégiques en la matière ont été prises par le Conseil fédéral fin janvier 2019. En particulier, le mandat de MELANI doit être élargi afin que des services puissent être offerts pour l'ensemble de l'économie et que des avertissements et des informations puissent être diffusés au public. En outre, le Centre de compétence à situer auprès du Département fédéral des finances doit être habilité à **donner des directives** à d'autres services fédéraux en cas d'incidents cybernétiques. L'**introduction d'une obligation de signaler** les cyberattaques (en particulier pour les exploitants d'infrastructures critiques) est également envisagée. Une **dynamique législative** considérable s'observe par ailleurs à l'échelle internationale.

7 CONCLUSION

Au regard de la digitalisation grandissante, les entreprises (et les particuliers) doivent être préparés à faire face aux risques posés par les **cyberattaques, ceux-ci étant destinés à augmenter à l'avenir**. En cas d'attaque, des mesures rapides et effectives doivent être prises. Si les annonces faites à MELANI sont particulièrement utiles pour les exploitants d'infrastructures critiques, l'implication des autorités judiciaires est à envisager sérieusement pour toute autre entreprise (et particulier) affectée par une cyberattaque devant être traitée rapidement.

Contacts

Le contenu de cette Newsletter ne peut pas être assimilé à un avis ou conseil juridique ou fiscal. Si vous souhaitez obtenir un avis sur votre situation particulière, votre personne de contact habituelle auprès de Schellenberg Wittmer SA ou l'un des avocats suivants répondra volontiers à vos questions:

A Genève:

Louis Burrus

Associé
louis.burrus@swlegal.ch

Clara Poglia, MAS in Criminology

Associée
clara.poglia@swlegal.ch

A Zurich:

Roland Mathys, LL.M. (LSE)

Associé
roland.mathys@swlegal.ch

Andreas Hösli, LL.M.

Associate
andreas.hoesli@swlegal.ch

SCHELLENBERG WITTMER SA / Avocats

ZURICH / Löwenstrasse 19 / Case postale 2201 / 8021 Zurich / Suisse / T +41 44 215 5252
GENÈVE / 15bis, rue des Alpes / Case postale 2088 / 1211 Genève 1 / Suisse / T +41 22 707 8000
SINGAPOUR / Schellenberg Wittmer Pte Ltd / 6 Battery Road, #37-02 / Singapour 049909 / www.swlegal.sg

www.swlegal.ch

Cette Newsletter est disponible en français, anglais et allemand sur notre site internet www.swlegal.ch.