AVOCATS

SCHELLENBERG WITTMER

FÉVRIER 2018

Newsletter

Auteur:
Roland Mathys

ICT / PROTECTION DES DONNÉES

Prévention, action, réaction – le traitement juridique des cyberrisques

La numérisation de l'économie entraîne un transfert de la criminalité économique vers l'environnement numérique. Rares sont les entreprises qui n'ont pas encore été ciblées ou touchées par une cyberattaque. Bien que les entreprises prennent conscience de cette nouvelle menace, une certaine confusion règne quant aux mesures à prendre pour s'en prémunir et, le cas échéant, y faire face.

1 INTRODUCTION

Dernièrement, les **cyberattaques** se sont répandues et ont pris de l'ampleur. Les cas les plus spectaculaires, tels que celui de *ransomware* "Petya", qui a temporairement paralysé les systèmes informatiques de nombreuses grandes entreprises, ont attiré l'attention sur ce danger. Aujourd'hui, des cyberattaques ont lieu quotidiennement. Dans des études récentes, près de 90% des entreprises interrogées ont déclaré avoir été visées par des cyberattaques au cours des douze derniers mois.

Les cyberattaques touchent **pratiquement toutes les entreprises**, indépendamment de leur secteur d'activité, de leur taille ou de leur localisation. Les groupes internationaux de sociétés financières sont aussi touchés que les PME locales. Ainsi, les cyberrisques et la cybercriminalité sont aujourd'hui considérés comme l'une des **plus grandes menaces** pour les entreprises. Dans ces circonstances, il est surprenant de constater que les mesures de défense et de réaction aux cyberattaques mises en place par les entreprises sont souvent inexistantes ou sommaires.

Ce **retard dans la mise en œuvre de mesures de défense ou de réaction** peut être observé, par exemple, au regard du temps qui s'écoule entre une cyberattaque réussie et sa découverte : dans environ 85% des cas, une cyberattaque réussie n'est détectée qu'après cinq mois. En moyenne, une attaque reste inaperçue environ 250 jours, soit près de huit mois. Pendant cette période, l'entreprise touchée est particulièrement vulnérable et les assaillants ne subissent aucun désagrément.

Cette newsletter expose divers moyens permettant de gérer les cyberrisques **d'un point de vue juridique**. Une distinction est opérée entre trois phases successives, soit la prévention pour parer aux attaques, l'action immédiate en cas d'attaque (réussie) et la réaction à une attaque.

2 PRÉVENTION

2.1 NÉCESSITÉ

La prévention, c'est-à-dire la mise en œuvre de mesures visant à empêcher les cyberattaques d'atteindre leur cible, devrait constituer le point de départ de toute stratégie de

défense contre les cyberattaques. De telles mesures ne sont pas seulement recommandées à des fins d'autoprotection ou pour la sauvegarde de la réputation de l'entreprise, mais sont également partiellement prescrites par la loi et font ainsi partie du *compliance* **de l'entreprise**.

"Dans environ 85% des cas, une cyberattaque réussie n'est détectée qu'après cinq mois."

Les lois applicables en Suisse n'imposent pas d'obligation générale et exhaustive de **prévention des cyberrisques**. Toutefois, cette tâche peut être considérée comme faisant partie intégrante de la responsabilité de la haute direction de la société (art. 716a CO) et donc comme **une obligation du conseil d'administration**. Cette obligation est concrétisée, par exemple, par le Code suisse de bonne pratique pour la gouvernance d'entreprise de l'association faîtière des entreprises suisses *economiesuisse*, selon lequel le conseil d'administration veille à ce que la gestion des risques et le système de contrôle interne soient adaptés à l'entreprise (principe 20). Compte tenu de la menace actuelle, la prévention des cyberrisques est l'une des mesures qui doit être prise par le conseil d'administration.

La loi sur la protection des données **(LDP)** concrétise l'obligation de prévention en lien avec les données personnelles. En effet, elle stipule que les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures techniques et organisationnelles appropriées (art. 7 LDP); la portée concrète de cette disposition est explicitée dans l'ordonnance relative à la loi sur la protection des données (**OLDP**; voir art. 8 et suivants). Le projet de révision de la LDP (**le projet**) aborde la problématique de la sécurité des données en se fondant d'avantage sur le risque (voir art. 7 du projet). A titre d'exemple, le message relatif au projet mentionne expressément la protection contre les logiciels malveillants (FF 2017 6941 et suivantes, 7031). Quant au règlement général sur la protection des données de l'UE (**RGPD**), qui entrera en vigueur le 25 mai 2018, il fait également de la sécurité des données un principe clé (art. 32 RGPD).

Il existe également des règles explicites pour la prévention des cyberrisques dans certains secteurs de l'économie, en particulier dans **le secteur bancaire et financier**. La circulaire 2008/21 "Risques opérationnels - banques" de l'Autorité fédérale de surveillance des marchés financiers **(FINMA)** stipule, depuis le 1er juillet 2017, que la direction de l'entreprise doit mettre en place un concept de gestion des cyberrisques (principe 4). Ce concept devrait couvrir au moins les aspects suivants:

> Identification du potentiel des menaces spécifiques;

> Protection des processus d'affaires et de l'infrastructure technologique;

> Détection et enregistrement en temps réel des cyberattaques;

> Réponse aux cyberattaques par des mesures rapides et opportunes;

> Garantie de la reprise des opérations commerciales normales dans les meilleurs délais après les cyberattaques grâce à des mesures appropriées.

Selon la circulaire, la direction devrait également vérifier régulièrement l'efficacité du concept et des mesures au moyen d'analyses de vulnérabilité et de tests d'intrusion.

2.2 MESURES

L'arsenal de mesures visant à prévenir les cyberrisques est vaste. Tout d'abord, chaque entreprise devrait mettre en place **un programme de cyber sécurité**. Ce programme définit les responsabilités de base, telles que la désignation d'un *Chief Information Security Officer* (CISO). L'implication de la direction est essentielle à cet égard. Le programme établit également des lignes directrices en matière de sécurité et prévoit des systèmes de surveillance permettant de détecter rapidement les cyberattaques. Dans le cadre des systèmes de surveillance, de nouvelles solutions, basées sur les mécanismes de l'intelligence artificielle, ont récemment conquis le marché et permis d'obtenir des résultats fiables. L'efficacité des processus et systèmes mis en place devrait être testée régulièrement, par exemple au moyen de cyberattaques simulées.

"Il existe des règles explicites pour la prévention des cyberrisques dans certains secteurs de l'économie, en particulier dans le secteur bancaire et financier."

Chaque entreprise doit prendre conscience des risques auxquels elle est exposée. Un inventaire des données et infrastructures sensibles doit être dressé dans le cadre d'une telle **évaluation des risques**. Les menaces et attaques potentielles doivent être identifiées, le facteur humain et la possibilité d'une attaque interne ne devant pas être sous-estimés. L'analyse des risques sert ensuite à combler les lacunes et points faibles du système de protection et de défense en place et à les éliminer par des mesures techniques ou organisationnelles appropriées. Une couverture d'assurance doit être envisagée pour les risques restants (voir ci-dessous).

L'évaluation des risques ne devrait pas porter uniquement sur l'entreprise de manière isolée, mais également sur les **tiers** avec lesquels l'entreprise interagit. Les contrats conclus avec des fournisseurs de services essentiels (par exemple l'hébergement de données) doivent être examinés en profondeur pour vérifier si l'aspect de la sécurité des données et de l'information est suffisamment pris en compte. Les fournisseurs de services essentiels devraient faire l'objet d'une *due diligence* en lien avec la cyber-sécurité.

La formation du personnel est un élément essentiel des mesures préventives. D'une part, il convient de sensibiliser le personnel à la menace potentielle que représentent les cyber-risques; d'autre part, il faut lui fournir les outils les plus importants pour prévenir les cyberattaques puis pour adopter un comportement correct en cas de cyberattaque réussie, au moyen par exemple d'un entraînement fictif (*mock training*) dans des conditions réalistes.

Finalement, les mesures préparatoires comprennent la mise en place d'un plan pour répondre aux cyber-incidents, qui décrit comment procéder en cas d'urgence (voir ci-après).

3 ACTION

Chaque entreprise doit être préparée à l'éventualité dans laquelle une cyberattaque atteindrait sa cible malgré la mise en place de mesures de défense préventives. Outre **la détection rapide** d'une attaque réussie, l'adoption d'un **comportement correct en cas d'urgence** est essentiel. A cette fin, les responsabilités doivent être clairement définies et les tâches assignées.

3.1 ÉQUIPE

En cas d'urgence, l'équipe d'intervention de l'entreprise doit intervenir immédiatement. Cette équipe est composée de représentants des domaines de l'informatique, du droit/ *compliance*, des ressources humaines, de la communication, du domaine spécifique concerné par l'attaque et de la direction. L'équipe peut également comprendre des spécialistes externes (par exemple des experts en cybercriminalité ou des avocats).

3.2 TÂCHES

Les premières tâches de l'équipe consistent notamment à **évaluer l'ampleur du cyberincident** et à **prendre des mesures immédiates pour minimiser les dommages** (par exemple, séparer tous les terminaux du réseau afin d'empêcher la propagation des logiciels malveillants). La continuité des opérations commerciale doit alors être assurée dans une configuration d'urgence à court terme. A moyen et long terme, le retour à des opérations commerciales normales doit être planifié puis mis en place.

L'équipe d'intervention doit également vérifier si et comment l'incident est **communiqué** à l'interne et à l'externe et si des notifications officielles sont nécessaires (voir ci-après). Elle doit également se demander dans quelle mesure **une enquête interne** sur l'incident doit être ouverte et si d'autres mesures (par exemple dépôt de plainte pénale ou mesures disciplinaires) sont nécessaires. Enfin, l'équipe doit réfléchir à la manière dont des incidents similaires peuvent être évités à l'avenir.

> "Outre la détection rapide d'une cyberattaque réussie, l'adoption d'un comportement correct en cas d'urgence est essentiel."

4 RÉACTION

4.1 NOTIFICATION

Dès lors qu'une cyberattaque réussie a lieu, il convient de déterminer rapidement si l'incident doit être signalé et à qui. Premièrement, une telle obligation de notification peut découler de **la loi sur protection des données**. La LPD en vigueur ne prévoit pas expressément d'obligation de signaler les incidents liés à la sécurité. En revanche, le projet de révision de la LDP stipule que, à certaines conditions, le Préposé fédéral à la protection des données et à la transparence et, si nécessaire, les personnes concernées, doivent être informés "dès que possible" d'un cyberincident (art. 22 du projet). La même obligation prévaut dans le cadre du règlement général sur la protection des données de l'UE (voir art. 33 et suivant RGPD). En sus, certaines lois spéciales prévoient des **obligations de notification dans des secteurs spécifiques** (par exemple pour les fournisseurs de services de télécommunications, pour les institutions financières soumises à une surveillance ou dans le secteur de la santé).

Dans le cas des sociétés cotées, l'obligation de divulguer un cyberincident peut également découler de l'obligation de **publicité ad hoc**. Ainsi, toute information susceptible d'avoir une influence notable sur le cours de bourse des actions d'une société doit être communiquée.

Même en l'absence d'obligation légale de notification, il peut être recommandé de communiquer l'existence d'un indicent, par exemple pour des raisons de réputation, de bonne gestion ou pour minimiser les dommages potentiels.

4.2 TRAITEMENT JURIDIQUE

Une fois qu'un cyberincident s'est produit, l'entreprise doit déterminer quelles actions en justice elle va entreprendre à l'encontre des auteurs de l'attaque. Des mesures de droit civil et pénal ainsi que des mesures spéciales sont envisageables.

En vertu du **droit civil**, les actions conservatoires, les actions en cessation ou les actions en dommages-intérêts peuvent être fondées sur des violations de contrat (par exemple par des clients ou des fournisseurs) ou sur des actes illicites; dans ce cas, l'illicéité est généralement due à la commission d'une infraction pénale, à une violation du droit à la marque ou du droit d'auteur, à une atteinte à la personnalité, à une violation de la protection des données ou à la concurrence déloyale. En matière de **droit pénal**, la palette comprend, d'une part, les délits spécifiques de cybercriminalité (p. ex. accès indu à un système informatique, vol ou détérioration de données, utilisation frauduleuse d'un ordinateur) et, d'autre part, les délits "classiques" (p. ex. escroquerie, chantage, contrainte, faux dans les titres ou violation de secrets), souvent combinés.

L'ordonnance sur les domaines Internet (**ODI**), qui a été révisée le 1er novembre 2017, offre un nouvel instrument pour **bloquer les noms de domaine des sites Web illégaux**. Le règlement s'applique aux sites Internet des *Top-Level Domains* .ch et .swiss, par lesquels des *phishings* sont réalisés ou des logiciels malveillants distribués ou qui soutiennent de tels actes illicites.

Il est également possible de signaler tout type de cyberincident à la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI (www.melani.admin.ch) ou au Service national de Coordination de la lutte contre la Criminalité sur Internet SCOCI (www.kobik.ch). Toutefois, en raison du grand nombre d'incidents signalés et des ressources limitées dont elles disposent, ces institutions ne seront souvent pas en mesure de mener une enquête approfondie.

Comme indiqué précédemment, il existe un vaste arsenal d'actions juridiques, mais les circonstances et défis particuliers inhérents à la cybercriminalité, en particulier l'anonymat et la virtualité des auteurs, la dimension internationale et le facteur temps, laissent présager que la mise en œuvre de telles actions sera parfois compromise.

4.3 ASSURANCE

Même avec des mesures préventives complètes, la survenance d'un cyberincident ne peut être totalement exclue, ce qui soulève la question de l'assurabilité des cyberrisques. Le **marché de la cyber assurance** est encore relativement jeune en Suisse, mais il se développe. Les modèles d'assurance disponibles à ce jour couvrent les pertes subies par des tiers (par exemple, les cas de responsabilité civile) et/ou les "dommages propres" de l'entreprise concernée (par exemple, les coûts de gestion de crise, les coûts de récupération des données ou les conséquences d'une interruption de l'activité commerciale).

Dans le cas de la cyber assurance, il est conseillé **d'examiner en détail** quels risques sont couverts, quel niveau de diligence est attendu du preneur d'assurance (notamment les mesures techniques et organisationnelles préventives) et quelles obligations lui incombent en cas de dommages (par exemple les obligations de déclaration ou de notification).

5 PERSPECTIVES ET RÉSUMÉ

En Suisse, de nombreuses **actions politiques** dans le domaine de la cybercriminalité sont actuellement en cours. Celles-ci vont de la création de centres de compétences spécifiques et de points centraux de contact et de coordination à l'introduction de nouvelles exigences en matière de déclaration (par exemple pour les exploitants d'infrastructures critiques). La nécessité d'agir a donc également été reconnue par le législateur et les autorités.

Les entreprises suisses sont de plus en plus conscientes des cyberrisques. Cependant, la **mise en œuvre de mesures appropriées reste souvent insuffisante**. La gestion proactive des cyberrisques devient progressivement un pilier central de la gouvernance d'entreprise et du *compliance*.

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:

Benjamin Borsodi
Associé
benjamin.borsodi@swlegal.ch

Louis Burrus
Associé
louis.burrus@swlegal.ch

A Zurich:

Roland Mathys
Associé
roland.mathys@swlegal.ch

Peter Burckhardt
Associé
peter.burckhardt@swlegal.ch

CHAMBERS EUROPE AWARDS 2014 WINNER SCHELLENBERG WITTMER Switzerland Law Firm of the Year

WWL AWARDS Switzerland FIRM OF THE YEAR 2015

WWL AWARDS Switzerland FIRM OF THE YEAR 2016

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.