6.7. Se prémunir contre la cybercriminalité : une nécessité absolue !

Suite à la récente attaque terroriste contre le journal satirique français « Charlie Hebdo » le 7 janvier 2015 et l'action anti-terroriste menée à Verviers le 15 janvier 2015, il est plus que jamais évident que personne n'est à l'abri de la criminalité et du terrorisme.

Le Ministre de la Justice, Koen Geens, veut des lors intercepter les communications téléphoniques de toute personne qui encourage le terrorisme. Cependant, les inspecteurs belges demandent de pouvoir intercepter les conversations en ligne et d'avoir l'autorisation de les (re)pirater. En effet, les terroristes et les criminels n'utilisent plus un téléphone fixe, mais plutôt des applications en ligne comme Skype et WhatsApp, ou bien ils correspondent par des jeux en ligne.

De plus en plus d'entreprises doivent faire face aux pratiques d'hameçonnage («phishing »). Les cybercriminels ont même l'audace d'envoyer des courriels au nom et depuis l'adresse <<courriel>› personnelle du CEO d'une entreprise au sein de laquelle ils demandent aux collaborateurs internes d'exécuter des virements en faveur de consultants <<impliqués››, par exemple, dans un nouveau projet d'investissement. Ensuite, avec professionnalisme, les cybercriminels téléphonent aux personnes concernées afin d'avoir la certitude que les montants seront prochainement versés.

En tant que CEO, CFO ou dirigeant d'entreprise, nul doute que vous êtes également préoccupé par le fait que le cyberespace économique constitue, depuis un certain temps, une source d'inspirations et d'opportunités pour des hackers et que, de plus en plus d'acteurs, venant d'horizons divers, se livrent à des comportements criminels:

› Intrusion dans les systèmes informatiques en vue de s'emparer de ressources financières ou matérielles.
› Extorsion et vol de données personnelles.
› Blanchiment d'argent ou organisation de commerces illégaux.
› Concurrence déloyale par le biais de la vente en ligne de produits contrefaits.
› Destruction de sites internet ou de systèmes d'information.
› Toute organisation peut être la cible d'une cyberattaque:
› La chaîne de livraison de pizzas « Domino's » ainsi que la Banque Centrale Européenne ont été les victimes d'un vol de données personnelles de certains de leurs clients.
› Les données personnelles de 1,46 millions de voyageurs de la SNCB ont été disponibles sur Internet sans protection aucune et ce, durant des semaines.
› Suite à une erreur de communication, le Ministère de la Défense a publié les données personnelles de plus de 500 travailleurs sur le site Internet de la Défense.
› Des hackers ont proposé à la société AGO-Intérim d'échanger les données de 10.000 demandeurs, dont ils s'étaient appropriés frauduleusement, contre une rançon de 100.000 €.
› La société Elantis, filiale de Belfius, a elle aussi été victime d'un chantage portant sur la publication de données personnelles de 3.700 clients contre 150.000 €.
› L'organisation terroriste extrémiste Etat islamique (ES) a notamment hacké le canal de YouTube et le compte Twitter du Commandement Militaire Central Américain pour le Moyen-Orient (CentCom) et a publié en ligne les données personnelles de militaires américains.
› Sony de même que l'administrateur du réseau internet ICANN (Internet Corporation for Assigned Names and Numbers) furent les victimes d'un hameçonnage qui a permis à des hackers d'obtenir les données de connexion des membres du personnel afin d'accéder aux systèmes internes.

En 2013, 61% des attaques via «spear phishing» (un courriel émanant apparemment d'une personne ou d'une entreprise connue mais qui, en réalité, a été envoyé par un hacker qui tente d'accéder aux numéros de comptes et cartes de crédit, mots de passe et données financières) étaient dirigées contre des entreprises comptant jusqu'à 2.500 travailleurs. La moitié de ces attaques a été dirigée contre des sociétés de moins de 250 travailleurs.

Peu importe la grandeur ou la nature de votre entreprise, vos activités sont liées à un réseau IT, un site Web ou un magasin en ligne. Vous recevez des paiements, vous utilisez des systèmes hautement automatisés dans vos procédures et intégrez de ce fait parfois diverses plateformes IT. Par définition, il s'agit là de portes d'entrée vulnérables.

En 2013, quelques 800 millions de données ont été perdues suite à des cybervols ou des cyberattaques. Le dommage annuel mondial, suite à la cybercriminalité et le vol de la propriété intellectuelle, est estimé à 376 milliards € (1).

C'est la raison pour laquelle les entreprises doivent prendre conscience de ces risques réels et mettre dès lors en place les mesures nécessaires. En effet, elles sont responsables de la protection des données dont elles disposent. Le législateur belge prévoit des amendes pouvant aller jusqu'à 550.000 € en cas de publication non autorisée de données personnelles. Il est donc primordial pour les entreprises:

› De prendre conscience des risques.
› D'établir des priorités.
› D'adapter les technologies et les systèmes.
› D'assurer la continuité et d'anticiper une crise.
› De sensibiliser les collaborateurs: une gestion de risques se mesure à son maillon le plus faible.

Mais, malgré les mesures de prévention prises, |'éventualité d'un sinistre persiste. Les conséquences financières d'un incident peuvent être considérables: les frais pour avertir les personnes concernées du vol de leurs données, pour récupérer ces données, pour rétablir l'image de votre entreprise, etc. Viennent encore s'ajouter une éventuelle perte du chiffre d'affaires, des dommages potentiels aux tiers, des amendes administratives et la défense en justice. Une « cyberassurance›› vous permet de couvrir une partie de ces frais et de limiter l'impact sur votre entreprise.

En 2013, 5% des entreprises belges étaient assurées contre les conséquences d'une cyberattaque. En 2014, ce pourcentage est passé à près de 13%.

Aujourd'hui, un grand nombre d'assureurs offrent des produits spécifiques qui constituent une solution partielle à la prise en charge de risques liés à la cybercriminalité. Ces produits s'articulent majoritairement autour des principes suivants:

1. Les garanties

› Interruption de |'activité ou du réseau, consécutive à une attaque ou violation du système: couverture de la perte d'exploitation.
› Responsabilité en cas de violation frauduleuse.
› De l'information détenue: données de tiers, données de l'entreprise, données externalisées, sécurité réseau.
›Des moyens multimédias utilisés : dommages et frais de défense, propriété intellectuelle et contenu électronique.
›L'extorsion en matière de cyber-confidentialité : versement de rançons.
›Vol informatique

2. Les biens assurés

Toutes les données détenues, en ce compris les licences et autres droits d'usage

3. Les frais et dépenses

›Obligations administratives, amendes et enquêtes
›Gestion de crise, restauration d'image, coaching violation
›Les données électroniques, leur restauration, récupération et récréation

La gestion du risque de cybercriminalité est devenue un élément clé de la gestion des risques d'une entreprise. Ce sujet doit être évoqué lors des discussions avec les actionnaires et les collaborateurs doivent être conscients de leur responsabilité dans le traitement de l'information de l'entreprise.

Source: (1) « Net Losses: Estimating the Global Cost of Cybercrime »
Center for Strategic and International Studies (CSIS)

Annette Senn
Head of Major & International Accounts
Gras Savoye Belgium

AIHE-Revue nr. 198 avril-mai 2015