KESSLER

Cyber Message 2023

Risk and Insurance

EN AVANT, SEREINEMENT.

Plus que jamais, les entreprises sont menacées par les cyberattaques. Pour la plupart d'entre elles, les cyberincidents font partie du top 3 des risques commerciaux encourus. En second lieu, les assureurs sont tout autant concernés par l'augmentation du nombre de sinistres subis par les entreprises. Notre message cyber vous livre notre expérience des sinistres et les enseignements que nous en avons tirés.

Changements juridiques

NOUVELLE LOI SUR LA PROTECTION DES DONNÉES

La nouvelle loi sur la protection des données (revLPD) est entrée en vigueur le 1er septembre 2023. Pourquoi avoir adapté la loi existante ? La version initiale fut instaurée en 1992. En 31 ans, les choses ont fortement évolué ; nous sommes entrés dans l'ère du numérique. Pour protéger les intérêts privés de chacun, il est donc indispensable de mettre également à jour la protection des données. La corrélation entre la sécurité de l'information et celle des données se manifeste dans les objectifs de protection bien connus que sont la confidentialité, l'intégrité et la disponibilité.

Quelles sont les adaptations à relever ?

- Les données des personnes physiques sont concernées, mais les données des personnes morales ne le sont plus
- Obligations en matière de documentation
- Renforcement des droits des personnes concernées
- Introduction de la notion de « privacy by design » ou de « privacy by default » (prise en compte du respect de la sphère privée dès la conception ou par défaut)
- Responsabilité pénale de la personne en charge de la protection des données

Il n'y a pas eu de période de transition. Que recommandons-nous à nos clients ? C'est très simple : toutes les tâches doivent être clairement attribuées et les responsables doivent être sensibilisés en conséquence.

NOTIFICATION OBLIGATOIRE DES INFRASTRUCTURES CRITIQUES

Une autre adaptation réglementaire aura lieu sous la forme de la révision de la loi sur la sécurité de l'information (LSI), qui définit de nouvelles normes, notamment pour les autorités et les organisations de la Confédération. Celles-ci doivent à l'avenir améliorer la sécurité de l'information et la cybersécurité. Toutes les autorités et organisations concernées devront par exemple mettre en place un système de gestion de la sécurité de l'information (SGSI) et disposer d'une gestion des risques adéquate.

En outre, les entreprises du secteur des infrastructures critiques sont tenues de signaler au National Cyber Security Centre (NCSC) toute cyberattaque ayant des conséquences graves dans les 24 heures suivant sa découverte. Le non-respect de cette obligation de notification peut être sanctionné par une amende pouvant aller jusqu'à CHF 100 000.

Sont notamment considérées comme des infrastructures critiques les hautes écoles, les autorités, les organisations de sécurité et de sauvetage, l'approvisionnement en eau potable et en eaux usées, l'élimination des déchets, l'approvisionnement en énergie, les banques, les assurances, les infrastructures sanitaires, les assurances sociales, la Société suisse de radiodiffusion et télévision, etc. L'entrée en vigueur de la nouvelle législation est attendue prochainement.

Risques actuels

DÉVELOPPEMENT DES ATTAQUES PAR RANSOMWARE

Les attaques par ransomware restent l'un des principaux risques pour la plupart de nos clients. De plus, les petites et moyennes entreprises deviennent plus attrayantes pour les cybercriminels. Elles n'ont généralement pas investi autant de moyens dans leur sécurité informatique que les grandes entreprises par exemple. De manière générale, on constate que les attaques par ransomware ciblent moins certains secteurs d'activité. Depuis la mi-2022, les attaques par ransomware sont à nouveau devenues nettement plus fréquentes.

Il est intéressant d'observer que dans certains cas, le mode opératoire des pirates a changé. Précisément parce que les entreprises ont investi davantage dans la détection et la réponse aux attaques, divers groupes de pirates mettent l'accent sur l'exfiltration de données, y compris la menace de les publier, et non plus sur leur cryptage. En cas d'attaque réussie, certains groupes entrent en contact avec les entreprises concernées et tentent d'obtenir les informations de couverture de leur police d'assurance cyber.

Dans un tel cas, il est fortement déconseillé de coopérer avec les cybercriminels sans l'accord préalable de l'assureur. Une telle coopération constitue une violation des obligations au sens de la police et peut entraîner des réductions de prestations en cas de sinistre.

ATTAQUES PAR INTELLIGENCE ARTIFICIELLE (IA)

Avec le développement rapide de l'IA, les possibilités de fraude et d'escroquerie numérique se sont considérablement étendues. On le voit en particulier dans les dernières méthodes d'utilisation de courriels d'hameçonnage et de « Social Engineering Fraud » (SEF). Entre-temps, « deep fake » offre des possibilités de manipuler des enregistrements audio et vidéo de telle sorte que les victimes sont convaincues, voire contraintes, de transférer de l'argent ou de divulguer des informations sur des plateformes de rencontres virtuelles. Souvent, les escrocs se font passer pour des cadres supérieurs qui incitent les collaborateurs à effectuer de telles opérations.

De la même manière, la plateforme WormGPT permet de créer un grand nombre de courriels de phishing sophistiqués, qui se résument à des Business Email Compromise (BEC) et des attaques de phishing. Il est important de mentionner que pour une fraude d'ingénierie sociale (Social Engineering Fraud – SEF) classique, où il n'y a pas de manipulation du système informatique de l'assuré, c'est généralement l'assurance contre les abus de confiance qui s'applique et non la cyberassurance.

Les assureurs sur le marché cyber

12 CONTRÔLES CLÉS

Les exigences minimales pour la conclusion d'une cyberassurance se résument en « 12 contrôles clés ». Le respect de ces 12 points a une influence déterminante sur la prévention des sinistres, selon une étude de notre partenaire de réseau Marsh. Toutefois, l'efficacité des différents contrôles clés peut varier considérablement selon les cas.

La comparaison des exigences minimales avec la base de données des sinistres enregistrés a montré que ce sont surtout les mesures dites de durcissement qui réduisent la probabilité d'une cyberattaque réussie. Les mesures de durcissement sont les configurations de sécurité installées et les mesures prises pour rendre les systèmes, réseaux ou logiciels plus résistants aux menaces et attaques potentielles.

À noter toutefois que la plupart des assureurs se sont concentrés jusqu'à présent sur trois contrôles clés, à savoir « l'authentification à facteurs multiples » (AMF), « la détection et réponse des terminaux » (Endpoint Détection and Response – EDR) et « la gestion des accès privilégiés » (Privileged Access Management – PAM). L'étude a également montré que l'AMF n'a un impact fort que si elle est pleinement déployée .

VIOLATION DES OBLIGATIONS

Les conditions générales d'assurance (CGA) prévoient de nombreuses obligations pour le preneur d'assurance, y compris, de plus en plus, pour la branche cyber. Des mesures de protection et des procédures techniques appropriées sont imposées. Elles vont jusqu'à obliger les preneurs d'assurance d'attester, par un contrôle professionnel, la conformité de leurs systèmes informatiques et de leurs processus IT. L'intégrité, la disponibilité et la confidentialité des données qui s'y rapportent doivent être garanties.

En cas de violation fautive des obligations par le preneur d'assurance, l'assureur est en droit de réduire l'indemnisation. C'est à l'assureur qu'il incombe de prouver qu'il y a eu violation des obligations. Il n'y a pas de préjudice pour le preneur d'assurance si, au vu des circonstances, la violation de l'obligation est considérée comme non fautive ou si la violation de l'obligation n'a eu aucune influence sur la survenance de l'événement et sur l'étendue des prestations dues par l'assureur (depuis la révision de la LCA). La revLCA apporte une amélioration du point de vue juridique en faveur du preneur d'assurance.

Marché de la cyberassurance

POINT DE SITUATION DU MARCHÉ

En 2023, le marché de la cyberassurance poursuit sa stabilisation. En règle générale, les assureurs maintiennent les capacités et les couvertures. Les primes ont enregistré une hausse moyenne à un chiffre, ce qui représente une amélioration significative par rapport aux années précédentes.

Pour les clients particulièrement exposés, comme les hôpitaux ou les prestataires de services dans le domaine des infrastructures critiques, des adaptations parfois plus importantes ont été nécessaires. La conclusion d'une cyberassurance doit être considérée comme un critère de qualité pour un haut degré de maturité en matière de sécurité informatique. C'est pourquoi les « 12 contrôles clés » sont systémaatiquement exigés. Leur efficacité ne s'est pas fait attendre : alors que depuis le milieu de l'année 2022, on enregistre dans le monde entier une nette augmentation des « cyberincidents », en particulier des attaques par ransomware, le nombre de cas enregistrés par Kessler et Marsh a diminué durant la même période.

KESSLER BLUE LINE

Nous avons voulu simplifier le processus de souscription d'une cyberassurance et proposons dès lors notre solution blue line pour les petites et moyennes entreprises. Dans la mesure où vous répondez aux critères requis, nous renonçons au processus de renouvellement annuel et vous bénéficiez d'un contrat négocié en exclusivité et d'une prime attrayante.

UNE CYBERATTAQUE ? COMMUNIQUER EN TOUTE SÉCURITÉ AVEC THREEMA

Dans le contexte cyber actuel et futur, la communication en cas de crise est essentielle. De nombreuses entreprises – qu'il s'agisse de grandes entreprises ou de PME – ne disposent pas d'une plate-forme de communication sécurisée leur permettant d'échanger rapidement et de manière fiable des informations avec les personnes faisant partie de la cellule de crise.

En collaboration avec Threema, Kessler a pu élaborer une solution pour faire face aux futures attaques. Au 1er janvier 2024, nous offrirons gratuitement l'application de communication Threema Work à la cellule de crise de nos clients, en plus de la cyberassurance. Nous pouvons ainsi mettre à la disposition de nos clients une plateforme sécurisée leur permettant de communiquer de manière efficace même en cas de crise.

KESSLER EN BREF

Kessler est l'entreprise leader dans le domaine du conseil en risques, assurances et prévoyance en Suisse. Nous nous occupons de plus de 1 500 moyennes et grandes entreprises suisses issues des services, du commerce et de l'industrie ainsi que du secteur public. Grâce à nos compétences dans les différents secteurs économiques, à nos collaborateurs qualifiés et à notre position de leader sur le marché, nous contribuons de manière significative au succès durable de nos clients. En tant que partenaire fiable, nous suscitons leur enthousiasme et leur ouvrons de nouvelles perspectives par notre gestion sûre des risques. Fondée en 1915, Kessler compte aujourd'hui 330 collaborateurs travaillant au siège à Zurich et sur les sites de Bâle, Berne, Genève, Lausanne, Lucerne, Neuchâtel, Saint-Gall, Sion et Vaduz. En tant que partenaire suisse de Marsh, nous faisons depuis 1998 partie d'un réseau de spécialistes issus de toutes les branches de gestion des risques et disposons d'une grande expérience dans le suivi des programmes d'assurances globaux. Active dans plus de 130 pays, Marsh est le principal courtier en assurances et conseiller en gestion des risques sur le plan mondial et fait partie de Marsh McLennan (NYSE : MMC).

Vous trouverez de plus amples informations, sous www.kessler.ch, www.marsh.com et www.mmc.com.

KESSLER & CO SA
Forchstrasse 95
Case Postale
CH-8032 Zurich
T +41 44 387 87 11
www.kessler.ch

Marsh Network