KESSLER

Cyber Message 2024

Risk and Insurance

EN AVANT, SEREINEMENT.

En 2024, les entreprises ont été confrontées à des défis liés aux cybermenaces de plus en plus complexes. Au-delà des formes d'attaques déjà connues, les dépendances qui existent, notamment vis-à-vis des prestataires externes, deviennent évidentes. Dans cette deuxième édition de notre Cyber Message, nous nous penchons sur l'évolution générale du marché cyber ces derniers mois, sur le rôle de chacun dans l'entreprise et sur la manière dont nous optimisons le processus d'évaluation des risques.

Changements juridiques

revLPD

L'évolution effrénée de la technologie nécessite en permanence des adaptations législatives. Depuis l'entrée en vigueur de la loi révisée sur la protection des données (revLPD) le 1er septembre 2023, les dispositions suisses en matière de protection des données sont en conformité avec le règlement général européen sur la protection des données (RGPD). Cette réforme vise à améliorer la protection des données à caractère personnel.

Les principales nouveautés concernent l'extension des obligations de renseignement, de notification et d'information. Les entreprises doivent fournir aux personnes concernées des informations complètes sur la collecte et le traitement de leurs données et notifier les violations de données au Préposé fédéral à la protection des données et à la transparence (PFPDT). Au 31 mars 2024, le PFPDT a reçu plus de 200 notifications en provenance de différents secteurs. La révision de la LPD implique une plus grande responsabilité, un besoin d'adaptation de la part des entreprises, ainsi qu'une augmentation des coûts de mise en conformité et de possibles changements dans les pratiques commerciales.

Le 14 août 2024, un nouveau cadre pour la protection des données a été défini afin de permettre un échange sécurisé de données personnelles entre la Suisse et des entreprises américaines certifiées, sans garanties supplémentaires. Le « Swiss–U.S. Data Privacy Framework » vise à garantir que les mesures de protection des données sont respectées. Les entreprises certifiées sont répertoriées sur la liste officielle https://www.dataprivacyframework.gov/list.

LÉGISLATION SUR LES PAIEMENTS DE RANÇONS

Alors que Le Conseil fédéral et d'autres gouvernements cherchent des moyens efficaces pour faire face au problème des ransomwares, le cadre légal offre déjà des règlementations applicables pertinentes. Même en l'absence d'une interdiction spécifique, les organisations payant des rançons sont confrontées à des risques juridiques importants. Un paiement pourrait enfreindre l'article 260ter, paragraphe 1, lettre b du Code pénal s'il est effectué en faveur d'une organisation criminelle.

Il est donc essentiel de prendre la décision de payer une rançon avec précaution et en connaissance de cause. En Suisse, la pratique montre que les dispositions légales sont favorables aux victimes. Les entreprises qui ont tenté de s'en sortir en payant une rançon n'ont pas été confrontées à ce jour à des sanctions supplémentaires de la part des autorités.

INTELLIGENCE ARTIFICIELLE

Les menaces que recèlent les formes d'attaques générées par l'IA sont toujours bien présentes. L'entrée en vigueur, le 1er août 2024, de l'EU AI Act, un règlement de l'Union européenne visant à préserver les valeurs éthiques et les droits fondamentaux, prouve qu'une protection réglementaire supplémentaire est nécessaire et vise à créer un environnement sûr, tant pour les utilisateurs que pour les entreprises.

Risques actuels

FACTEUR HUMAIN

Les cybercriminels ciblent souvent les collaborateurs pour contourner les mesures de sécurité des entreprises et infiltrer les systèmes informatiques, avec des répercussions considérables. Le comportement des employés a une influence directe sur la cybersécurité et sur la limitation des conséquences d'une attaque. La protection et la prévention sont des éléments clés de la cyberrésilience.

Les récentes études indiquent que l'attitude des employés face aux cyberrisques est décisive. Si les collaborateurs comprennent qu'ils travaillent quotidiennement avec des informations à caractère sensible, cela renforce leur degré de vigilance et accroît leur sécurité. Il est important de mettre en évidence la portée de chaque individu sur la cyberrésilience. Des exemples concrets, des références spécifiques au secteur et des formations régulières favorisent une prise de conscience durable et conduisent à une approche axée sur la protection et la sécurité.

RISQUES EN MATIÈRE DE RESPONSABILITÉ CIVILE PROFESSIONNELLE POUR LES ENTREPRISES TECHNOLOGIQUES

Les entreprises technologiques sont largement tributaires de systèmes informatiques complexes et, en parallèle, les risques techniques ne cessent d'augmenter. Ceux-ci peuvent avoir de graves conséquences selon le type d'entreprise et les services proposés. Les manquements aux obligations, les omissions, les pannes de système et les erreurs de logiciel entraînent des problèmes et des responsabilités accrues. Une assurance responsabilité civile professionnelle (PI) est donc une excellente mesure pour se couvrir contre les risques professionnels.

Le risque lié aux cyberincidents augmente pour les entreprises technologiques, qui sont de plus en plus exposées à des attaques externes. Si l'« assurance PI Tech » couvre les risques liés à des erreurs ou des omissions dans la fourniture de services ou de produits techniques, la « cyberassurance » protège quant à elle contre les menaces externes telles que le piratage, les fuites de données ou les interruptions d'activité. La combinaison des deux offre une protection globale aux entreprises technologiques.

Marché de la cyberassurance

POINT DE SITUATION DU MARCHÉ

Depuis fin 2023, le marché de la cyberassurance se caractérise par son dynamisme et sa compétitivité. Il est stimulé par de nouveaux prestataires. L'assouplissement des politiques de souscription, l'augmentation des montants assurés et, bien souvent, la baisse des primes pour une couverture inchangée sont des tendances qui se poursuivent. Parallèlement, des exigences minimales strictes en matière de maturité informatique des assurés, telles que les « 12 contrôles clés », restent une réalité constante. Ces exigences sont déterminantes pour la souscription d'une cyberassurance. L'évolution du marché montre que les assureurs suisses sont de plus en plus enclins à souscrire des risques, tout en recherchant un équilibre entre la prudence et le goût de l'innovation.

ÉVOLUTION GÉNÉRALE DU CONTEXTE DES SINISTRES

Les attaques de ransomware restent le risque le plus élevé et causent les dommages financiers les plus lourds. Souvent, les nombreux éléments de préjudice propre sont sous-estimés. Les coûts de gestion de crise, de restauration des systèmes et les conséquences d'une interruption de l'activité peuvent rapidement augmenter.

Les demandes de rançon posent toujours un sérieux problème. En cas d'extorsion, il est recommandé d'entamer des négociations afin de recueillir des informations et de gagner du temps. Les statistiques de Kessler montrent que cela permet de réduire les demandes de rançon de 59% en moyenne.

INTERRUPTION D'ACTIVITÉ LIÉE AUX CYBERATTAQUES

Le calcul de la perte de chiffre d'affaires résultant d'un cyberincident est un défi, car il est influencé par les variations saisonnières et conjoncturelles. Il faut donc comparer les chiffres d'affaires avec les prévisions budgétaires et les données de l'année précédente. Les approches telles que l'analyse d'impact sur l'activité sont chronophages et onéreuses. La consignation des coûts supplémentaires est également problématique. Kessler recommande de documenter les heures supplémentaires et les mesures connexes afin d'améliorer la traça-

bilité et la gestion de crise. Outre les heures de travail, les activités effectuées pendant cette période devraient être enregistrées afin de pouvoir retracer ultérieurement ce qui a été fait.

INCIDENT CROWDSTRIKE

L'incident CrowdStrike de juillet 2024 a mis en évidence le caractère critique que peut avoir une panne lors de la mise à jour d'un logiciel fourni par un tiers. Un bug dans la mise à jour du contenu Falcon a provoqué des pannes mondiales et paralysé les utilisateurs de Windows pendant quelques heures, parfois plusieurs jours. Un tel événement peut compromettre l'intégrité de toute la chaîne d'approvisionnement. L'audit des fournisseurs ne doit donc pas être mis en œuvre une seule fois, mais dans le cadre d'un processus continu. Dans les contrats avec des fournisseurs tiers, il faut des normes de sécurité claires, ainsi que des audits réguliers. Ces mesures permettent de protéger l'intégrité des données et de minimiser l'impact de tels incidents.

CYBER SELF-ASSESSMENT TOOL (CSA)

Depuis début 2024, Kessler propose à ses clients le Cyber Self-Assessment Tool (CSA) développé par son partenaire de réseau Marsh. Le questionnaire en ligne facilite la collecte d'informations sur les risques, l'étendue des questions étant adaptée à la taille et à l'activité de l'entreprise. La possibilité de réutiliser les données pour les années suivantes et leur large acceptation par les assureurs simplifient considérablement le processus d'appel d'offres et de renouvellement.

L'outil CSA présente encore d'autres avantages : il fournit des rapports montrant l'évaluation par les assureurs de la maturité informatique de l'entreprise, indique comment les contrôles se situent par rapport aux référentiels internationaux et comment l'entreprise se positionne par rapport à ses pairs. En plus, l'outil d'analyse Blue[i] modélise les scénarios de sinistres possibles, y compris les probabilités de survenance et l'ampleur des dommages attendus. Ces informations aident à évaluer le transfert du risque et à affiner la stratégie de souscription. Elles indiquent également quelles mesures peuvent être prises pour améliorer la cybersécurité de manière ciblée.

CYBER BLUE LINE

Nous tirons un bilan très positif du lancement de la Cyber blue line en 2023. La Cyber blue line simplifie considérablement le processus de souscription d'une cyberassurance. Une fois les 12 exigences minimales remplies (12 contrôles clés), plus de 98% de nos clients optent pour cette solution. De plus, par le biais du contrat-cadre, nos clients bénéficient de services tels que des simulations de phishing ou des formations pour le personnel.

THREEMA

Pour garantir une communication sécurisée même en cas de crise, nous collaborons avec la société Threema. En 2024, le cabinet d'études de marché « Forrester » a classé Threema en tête des solutions de communication sécurisée. Souvent, les entreprises ne maîtrisent pas la manière dont les échanges d'informations devraient avoir lieu en cas de crise – nous aidons nos clients à en prendre conscience et leur conseillons d'utiliser la communication sécurisée de Threema.

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 350 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. Actif 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
Avenue de la Gare 44
Case postale 950
CH-1001 Lausanne
T +41 21 321 60 30
www.kessler.ch

Marsh Network