Liberty Specialty Markets

Cyberrisques

La cybercriminalité, un secteur florissant

Les méthodes de cybercriminalité sont diverses: de l'espionnage et du sabotage à la manipulation des marchés et à l'hameçonnage en passant par le chantage et les fuites de données. Les cas pour lesquels le point de départ se trouve dans l'entreprise sont également en augmentation, en d'autres termes, les actes d'individus internes à l'entreprise ou les comportements involontaires du personnel. Par ailleurs, on externalise toujours davantage des processus commerciaux IT complets. Les risques auxquels les entreprises sont exposées évoluent ainsi en conséquence.

Liberty protège les biens immatériels de ses clients grâce à une approche innovante et créative et propose des solutions d'assurance rapides et flexibles. Notre Cyber Suite est une assurance sur mesure pour tous les défis auxquels les entreprises sont confrontées compte tenu de leur dépendance croissante aux réseaux informatiques, aux structures informatiques de prestataires tiers, aux ressources numériques et aux données personnelles stockées.

Toute entreprise est exposée à des cyberrisques

Toute personne qui stocke des données concernant des tiers ou des collaborateurs doit se demander jusqu'à quel point leur sécurité est garantie. Plus les données sont volumineuses et confidentielles, plus une éventuelle responsabilité vis-à-vis de tiers ou de collaborateurs sera coûteuse.

Conformément à la législation et aux ordonnances des autorités de surveillance, les demandes de dommages-intérêts, les amendes (qui ne sont pas toujours assurables aux termes de la loi) et les frais relatifs à la notification aux clients ou la surveillance des cartes de crédit peuvent prendre des proportions considérables. De plus en plus de pays imposent une obligation légale d'information vis-à-vis des personnes dont les droits relatifs à la protection des données ont été violés. Si des données confidentielles de citoyens de l'Union européenne sont concernées, le Règlement général sur la protection des données de l'UE (RGPD) s'applique également pour les entreprises suisses. Et en l'absence de législation pertinente, cette obligation d'information est souvent intégrée aux dispositions contractuelles ou aux directives de branches.

Chaque entreprise court au demeurant le risque d'une défaillance réseau susceptible de provoquer une interruption de l'activité et donc un manque à gagner. À titre d'exemple, si les collaborateurs ne peuvent accéder aux listes de vente ou de marketing, aux systèmes de CRM ou d'approvisionnement de la chaîne logistique, le travail cesse rapidement. Les bâtiments, les usines et les entrepôts sont aussi souvent contrôlés par l'intermédiaire de réseaux. Leur défaillance peut également perturber sensiblement le processus de fabrication.

Attribution	Capacité
Cyberrisques	jusqu'à 10 CHF/EUR/USD millions

Exemples de cybercriminalité

Jusqu'à présent, les actes frauduleux visaient principalement les institutions financières. Désormais, les cabinets d'avocats, les sociétés de conseil et en particulier les PME des secteurs les plus divers sont de plus en plus les cibles d'attaques professionnelles. Trois exemples:

Chantage avec dommages indirects

Une société commerciale suisse subit une attaque subite de pirates informatiques. Sous-estimée tout d'abord, elle frappe violemment l'entreprise: plus d'accès à l'intranet, perturbation de nombreuses applications, suppression de banques de données, disparition ou réinitialisation aux paramètres d'usine du serveur, le système informatique est neutralisé. Les interfaces permettant aux clients importants de passer automatiquement leurs commandes ont été supprimées, le travail est totalement impossible et l'entreprise est contrainte de se déconnecter. Cette situation peut provoquer des départs de clients ou des pénalités conventionnelles. Arrivent alors des demandes de rançon s'élevant à plusieurs centaines de milliers de francs. L'entreprise ne retrouve son exploitation normale qu'après plus de trois semaines de travaux extrêmement coûteux pour se défendre contre l'attaque et reconstituer ce qui a été détruit.

Le facteur humain: un point faible

Toute l'infrastructure IT d'une entreprise de construction suisse a été paralysée: des collaborateurs ont autorisé l'accès suite à un e-mail de phishing. L'attaque a concerné le système ERP central et le système de stockage, le site Web, l'ensemble des adresses électroniques et la téléphonie fixe.

La logistique des stocks et des livraisons a été très fortement touchée, plus aucune marchandise n'est livrée. Des spécialistes informatiques appelés à la rescousse ont été chargés d'établir un bilan. Tous les sites suisses de l'entreprise (plus de 1000 employés) ont été concernés.

Attaques ciblées

La journée commence mal chez un fournisseur d'accès employant quelque 50 collaborateurs: une cyberattaque a totalement neutralisé le service Cloud. Si l'on est parvenu à bloquer la plupart des rançongiciels, il a fallu restaurer progressivement le serveur d'applications et les données. Mais après plusieurs semaines encore, l'entreprise a dû demander à de nombreux clients de patienter car les systèmes concernés ne pouvaient être remis en service que progressivement en raison notamment de très importantes quantités de données. Ce qui est remarquable dans ce cas, c'est le cyberchantage ciblé. En effet, toujours plus de tentatives de chantage ciblées s'ajoutent désormais aux rançongiciels propagés dans le cadre d'attaques de masse. Ces attaques ont un point caractéristique: les auteurs peuvent réclamer des sommes beaucoup plus importantes car ils connaissent leurs victimes et peuvent estimer approximativement le montant qu'elles sont disposées à payer.

Que recouvrent précisément les cyberrisques?

Cette notion recouvre une série de risques conduisant à des dommages propres et à des dommages à des tiers dans le cadre de l'utilisation des technologies de l'information. La Cyber Suite de Liberty propose les types de garantie suivants:

Dommages propres

- **Perte ou endommagement de données ou de programmes**
  Prise en charge des frais de réparation, d'actualisation, de restauration ou de remplacement des données et/ou des programmes endommagés afin de rétablir l'état du système avant le sinistre.
- **Interruption de l'activité**
  Couverture des manques à gagner en raison d'une interruption, d'une dégradation ou d'une panne de votre réseau; y compris les dépenses de réduction et d'investigation du sinistre liées à l'interruption.
- **Cyberchantage**
  En cas de chantage sous la menace de paralyser ou de perturber votre réseau, de publier des données de votre réseau sans autorisation ou de communiquer avec vos clients sous de faux prétextes, traitement de la tentative de chantage et paiement de la rançon.
- **Préjudice de réputation**
  En cas de préjudice de réputation suite à la divulgation d'une atteinte à la protection de données suivi d'un manque à gagner engendré par la perte de clients, remboursement du manque à gagner ainsi que des éventuels surcoûts de travail et les dépenses liées à l'effort de relations publiques.

Dommages aux tiers

- **Cyberresponsabilité civile**
  Couverture des dépenses de responsabilité et de défense en justice pouvant découler de revendications d'un acte illicite réel ou prétendu.
- **Procédures d'autorités de surveillance**
  Prise en charge des frais d'investigation, d'avocat et également, pour autant que celles-ci soient assurables compte tenu du droit applicable, y compris des amendes et sanctions pécuniaires.
- **Frais d'information et gestion de crise**
  Prise en charge des frais juridiques ainsi que frais pour soutenir les personnes touchées par les manquements aux dispositions de protection des données, par exemple liés à la surveillance des cartes de crédit et/ou aux conseils en cas d'usurpation d'identité, également pour le rétablissement de la réputation.
- **Responsabilité civile multimédia**
  Si vous violez des droits de propriété immatérielle ou des droits de protection de données de tiers, si on vous reproche des propos diffamatoires ou si vous publiez ou imprimez des contenus électroniques par négligence, prise en charge des frais d'investigation et d'avocat ainsi que les actions en dommages-intérêts.

Bonne question: la perte de données est-elle déjà couverte par d'autres polices d'assurance?

Responsabilité civile professionnelle

Si vous disposez d'une assurance de responsabilité civile professionnelle, celle-ci couvre déjà éventuellement les dommages à des tiers en raison de pertes de données – mais en règle générale uniquement si le sinistre survient dans l'exercice de l'activité professionnelle.

La plupart du temps, une assurance de responsabilité civile professionnelle ne couvre pas non plus les prétentions des employés. L'assuré n'est pas non plus couvert en cas d'utilisation malveillante ou non autorisée de son réseau provoquant l'endommagement, l'abus ou la destruction de données de clients ou déclenchant des attaques par refus de service.

Les dommages engendrés par la transmission de virus informatiques sont en outre souvent exclus et la garantie se limite aux prétentions des clients de l'assuré alors que les procédures de surveillance réglementaire sont exclues. La plupart des assurances de responsabilité civile professionnelle ne fournissent en outre aucune garantie en cas de dommages propres tels que les manques à gagner, la perte ou l'endommagement de données/programmes, le cyberchantage ou le préjudice de réputation.

Responsabilité civile générale

Une assurance de responsabilité civile générale ne couvre que les dommages aux personnes et aux biens. Comme les tribunaux considèrent les données comme des biens immatériels, les manquements aux obligations de protection des données ne sont habituellement pas garantis.

Assurance de biens

Une assurance de biens ne couvre en règle générale que les dommages subis par des biens physiques. Les tribunaux considèrent les données comme des biens immatériels. C'est pourquoi les pertes ou les détériorations de données/programmes ne sont la plupart du temps pas prises en charge. Même si vous disposez d'une assurance en cas d'interruption de l'exploitation résultant de dommages matériels, il n'existe probablement aucune couverture en cas d'interruption de l'exploitation résultant de dommages immatériels sur votre réseau. Les virus informatiques et les risques réseaux sont souvent des exclusions pour les assurances de biens.

Assurance informatique tous risques

L'assurance informatique tous risques couvre les frais de réparation du matériel endommagé (biens physiques) de manière différente à une assurance Cyber Suite sans pour autant faire naître de revendication dans le cadre de la perte de données ou de dommages indirects.

Une approche de long terme

Notre collaboration avec les clients est placée sous le signe de l'innovation et de la détermination. Nous sommes rapides et réactifs. Dans le même temps, nous aspirons surtout à une évolution durable de notre relation avec nos clients mais aussi de votre entreprise.

Car votre prospérité est la condition de notre progression. C'est pourquoi, nous visons toujours le long terme: avec notre compétence en matière de souscription et notre connaissance des marchés locaux et internationaux, nos relations solides avec les divers partenaires ou encore la simplicité avec laquelle nous assurons le traitement des sinistres. Nous établissons ainsi confiance et fiabilité en des temps mouvementés. Aussi sur la durée.

Vous souhaitez plus d'informations sur Liberty en Suisse et sur nos produits d'assurance?

Contact:

Liberty Specialty Markets
Lintheschergasse 19, 8001 Zurich

+41 44 285 10 00
lsmzurich@libertyglobalgroup.com
www.libertyspecialtymarkets.com

Liberty Specialty Markets

For Mutual Advantage