easyPRO Cyber pour les commerces

1. Pourquoi les commerces sont pris pour cible ?

Les commerces sont des cibles attrayantes pour les hackers en raison de leur dépendance aux systèmes informatiques pour la gestion des stocks et des transactions. Ils conservent également des données personnelles et financières des clients, ce qui en fait des cibles potentielles pour le vol d'identité et les fraudes. Leur structure souvent indépendante peut limiter leurs ressources pour mettre en place des protections adéquates, augmentant ainsi leur vulnérabilité aux cyberattaques.

+102 %

La hausse du pourcentage de cyberattaques au Luxembourg entre 2023 et 2024, soit 1 173 par semaine. (1)

23 %

des organisations ont constaté une augmentation des cyberattaques réussies en 2023.(2)

2. Exemple concret de cyberattaque

Une librairie en ligne a été attaquée par une injection SQL, permettant aux cybercriminels d'accéder à la base de données clients, y compris les informations de paiement. Bien que la faille ait été sécurisée et des mesures de protection mises en place, la librairie a dû informer ses clients de la violation, entraînant une perte de confiance et une baisse des ventes.

Qu'aurait pris en charge l'assureur ?

Qu'aurait pris en charge l'assureur ? easyPRO Cyber aurait pris en charge l'assistance d'urgence de 720 € pour la gestion du sinistre ainsi que les frais de perte d'exploitation estimés à 4 000 €.

(1) Check Point Software Technologies - 2024
(2) CESIN - 7ème édition du baromètre annuel - Janvier 2022

3. Les principales conséquences d'une cyberattaque

Les cyberattaques réussies paralysent les commerces, pouvant entraîner une interruption d'activité, une perte de revenus ou encore avoir un impact négatif sur l'image de marque.

- Systèmes de caisse et de stock bloqués : les logiciels de gestion des ventes, des stocks et des commandes peuvent être paralysés. Les données clients peuvent être chiffrées ou revendues sur le dark web, avec rançon à la clé.
- Activité quotidienne interrompue : sans outils numériques, les équipes ne peuvent plus encaisser, gérer les stocks ni commander de nouveaux produits, provoquant désorganisation et perte de chiffre d'affaires.
- Perte de confiance des clients : la fuite de données personnelles nuit à la réputation du commerce, fragilisant la relation de proximité si importante dans ce secteur.
- Risques juridiques : des procédures peuvent être engagées en cas de violation de données, entraînant enquêtes, amendes ou sanctions réglementaires.

4. Ce qui est couvert par l'assurance easyPRO Cyber

ASSISTANCE ET EXPERTISE

Hotline d'urgence 24/7

Nous mettons à votre disposition un numéro d'appel d'urgence (+352 4761-4444) 24h/24 et 7j/7 pour missionner un expert de notre partenaire Dattak qui coordonnera la gestion de votre incident (sans franchise). Dattak déploie son réseau de plus de 50 experts cyber, juridiques et en gestion de crise qui interviennent pour sécuriser vos systèmes, gérer l'attaque et limiter les impacts sur votre entreprise.

Interventions d'experts

Nos meilleurs experts vous accompagnent : ingénieurs, experts en cybersécurité, experts juridiques, gestion de crise, etc.

Exemple : Votre commerce est victime d'une cyberattaque et votre réputation est fortement impactée. Nos experts en communication de crise vous assisteront dans la gestion des relations publiques et dans votre communication interne et externe.

RESPONSABILITÉ CIVILE

Responsabilité Civile Cyber & Média

Nous prenons en charge le coût et les frais de défense résultant de toute réclamation introduite par un tiers suite à une fuite de données et/ou une transmission de virus.

Exemple : Votre commerce est victime d'une cyberattaque et les données personnelles de l'un de vos clients fuitent ou vous transmettez un virus à un tiers. Il vous poursuit en justice pour obtenir un dédommagement. Nous prenons alors en charge tous les coûts et les frais de défense (gestion des réclamations, frais d'enquêtes, frais d'avocats, etc.)

DOMMAGES ET PERTES

Frais de monitoring et de surveillance

Nous prenons en charge les frais engagés pour détecter l'utilisation non conforme de données personnelles.

Exemple : Les données de vos clients fuitent et parmi ces données se trouvent des informations sensibles et/ ou des informations permettant d'identifier directement ou indirectement un client. Nous engageons alors des frais pour nous assurer que ces données ne sont pas utilisées à des fins malveillantes.

Frais de notification

Nous prenons en charge les frais de notification aux autorités et aux personnes concernées en cas de vol de données personnelles.

Exemple : Votre commerce est victime d'une cyberattaque, vous êtes alors dans l'obligation de notifier tous vos clients impactés par l'attaque ainsi que la CNPD.

DOMMAGES ET PERTES

Frais de reconstitution de vos données et de votre système informatique

Nous prenons en charge les frais de reconstitution des données présentes sur vos sauvegardes exploitables ainsi que les frais engagés pour remettre votre système informatique en bon état de marche.

Exemple : Suite à une cyberattaque, le système informatique de votre commerce est impacté. Nous prenons en charge tous les frais nécessaires à sa restauration dans le même état de fonctionnement que celui existant avant l'attaque.

Frais d'enquêtes et sanctions administratives

Nous prenons en charge les frais d'enquêtes diligentées à votre encontre par une autorité administrative ou gouvernementale compétente au titre de la violation des données personnelles ou suite à un manquement aux règles de sécurité PCI DSS (pour les cartes bancaires). Ainsi que les éventuelles amendes et pénalités dès lors qu'elles sont légalement assurables.

Exemple : Suite à une cyberattaque, des données personnelles de vos clients fuitent et la CNPD lance une enquête à votre encontre. Nous prendrons en charge les frais de défense dans le cadre de cette enquête.

Pertes d'exploitation

Nous prenons en charge vos pertes de marge brute d'exploitation consécutives à l'interruption totale ou partielle de votre système informatique.

Exemple : Votre commerce est victime d'une cyberattaque, vous êtes dans l'obligation d'interrompre totalement ou partiellement votre système informatique pour limiter les dégâts. Nous prenons alors en charge vos pertes de marge brute d'exploitation. C'est à dire la marge brute que vous auriez dû réaliser sur la période d'interruption.

Frais de négociation de la rançon

Nous prenons en charge les frais de la négociation de la rançon.

Exemple : Votre commerce est victime d'une cyberattaque. Les malfaiteurs prennent le contrôle de vos données et exigent une rançon, tout en menaçant de publier des informations sensibles. Nous prenons en charge les frais de négociation de la rançon, notamment l'intervention d'experts spécialisés, et vous accompagnons à chaque étape pour gérer la situation et limiter les impacts.

Cyber-fraude

Nous prenons en charge les conséquences pécuniaires faisant suite à une cyber-fraude.

Exemple : Votre commerce est victime d'une cyberattaque, les malfaiteurs s'introduisent dans votre système informatique et envoient un mail à votre responsable financier pour qu'il émette un virement. Nous prenons alors en charge le montant des fonds détournés.

Surfacturation téléphonique

Nous prenons en charge les surcoûts dus à une utilisation frauduleuse de vos lignes téléphoniques.

Exemple : Votre commerce est victime d'une cyberattaque et les malfaiteurs utilisent vos lignes téléphoniques pour appeler des numéros surtaxés. Nous prenons alors en charge le surcoût.

Document non contractuel à caractère publicitaire

DON'T WORRY *be happy*

lalux ASSURANCES