easyPRO Cyber pour cabinets médicaux

1. Pourquoi les cabinets médicaux sont-ils pris pour cible ?

Le secteur de la santé est le secteur le plus touché par les cyberattaques au niveau mondial. Les données médicales figurent en tête des données les plus sensibles, qui se revendent plus cher sur le darkweb. Avec la fragilité de ses systèmes informatiques, ce secteur est une cible privilégiée pour les hackers. Les cabinets médicaux n'y font pas exception. En cas d'attaque, l'activité du cabinet est paralysée temporairement et ses données subtilisées. Cela représente un coût financier conséquent, ainsi qu'un risque pour sa réputation.

1er

Le secteur de la santé est le plus touché par les cyberattaques au niveau mondial. [1]

x 2

Les cyberattaques contre les établissements de santé ont doublé en 2021.[2]

2. Exemple concret de cyberattaque

Suite à une attaque phishing accompagnée d'une demande de rançon, le système de gestion de chambres d'une clinique est paralysé.

Qu'aurait pris en charge l'assureur ?

L'assurance easyPRO Cyber prend en charge l'assistance d'urgence pour la gestion du sinistre de 720 €, le travail des experts informatique pour l'identification de la faille à hauteur de 1 800 €, ainsi que les frais de reconstitution du système informatique 10 000 €.

(1) Oodrive - Le coût des failles de sécurité : les secteurs qui sont les plus touchés et ceux qui s'en sortent le mieux
(2) Tech et Web - Les cyberattaques contre les établissements de santé ont doublé en 2021 - Février 2022

3. Les principales conséquences d'une cyberattaque

Les cyberattaques qui atteignent leurs objectifs paralysent l'activité du cabinet médical. Cela entraîne une perte de revenus et nuit à la réputation du cabinet.

- En cas d'attaque ransomware, tout le système d'information et les données sont chiffrées. Une rançon peut également être exigée par le hacker. Les données confidentielles (personnelles, bancaires...) touchées sont le plus souvent volées et revendues sur le dark web.
- Les données personnelles peuvent fuiter et être revendues sur internet. Les données médicales se revendent cher sur le darkweb. Le cabinet peut se retrouver en non conformité sur le RGPD et s'exposer à des sanctions.
- Les ordinateurs ne peuvent plus être utilisés, les collaborateurs du cabinet ne peuvent plus accéder aux dossiers des patients, ni à leur historique. Il existe un risque d'endommagement des systèmes et de corruption des fichiers de données.
- L'image et la crédibilité du cabinet sont fortement impactées. Le cabinet médical doit prévenir ses contacts suite à la découverte de l'attaque. Cela mène à une perte de confiance de la part de la patientèle.

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 cabinet 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 cabinet 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 cabinet 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 cabinet 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 cabinet est victime d'une cyberattaque, vous êtes dans l'obligation d'interrompre totalement ou partiellement votre système informatique pour limiter les dégats. 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 cabinet 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 cabinet 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 cabinet est victime d'une cyberattaque et les malfaiteurs utilisent vos lignes téléphoniques pour appeler des numéros surtaxés. Nous prenons alors en charge le surcoût.

DON'T WORRY *be happy*

lalux ASSURANCES