easyPRO Cyber pour les syndics de copropriété

1. Pourquoi les syndics de copropriété sont-ils pris pour cible ?

L'immobilier est le secteur le plus touché par les cyberattaques au niveau mondial. La vulnérabilité générale des systèmes informatiques en fait une cible de choix pour les hackers. Les syndics de copropriété n'y font pas exception. En cas d'attaque réussie, l'activité de l'administrateur de biens est paralysée temporairement. Cela représente un coût financier conséquent, ainsi qu'un risque pour sa réputation.

50 %

Les attaques par mail dans le secteur de l'immobilier ont augmenté de 50% en 2023 par rapport à 2022. (1)

74 %

Le pourcentage des entreprises dans l'immobilier qui ne sont pas préparées aux cyberattaques en 2022.(2)

2. Exemple concret de cyberattaque

Décembre 2023, un syndic de copropriété fait fuiter des informations sensibles de locataires suite à une attaque de type phishing. Une rançon de 100 000 euros avait été demandée, mais nous avons récupéré les données sans payer.

Qu'aurait pris en charge l'assureur ?

L'assurance easyPRO Cyber a indemnisé les frais de gestion du sinistre de 720 €, l'intervention de l'expert informatique, 1 800 €, les frais de reconstitution du système informatique, 10 000 €, les frais de notification aux autorités et aux personnes concernées 20 000 €.

(1) Proofpoint - Le rapport 2022- Février 2022
(2) Tehtris - Le cyber risque dans le secteur le l'immobilier -Octobre 2022

3. Les principales conséquences d'une cyberattaque

Si la cyberattaque est fructueuse, l'attaquant peut paralyser l'activité de la société de gestion et d'administration, mais aussi celle de ses clients :

- 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. L'établissement peut se retrouver en non conformité sur le RGPD et s'exposer à des sanctions.
- Les ordinateurs ne peuvent plus être utilisés, les collaborateurs ne peuvent plus accéder aux dossiers des clients, ni à leur historique.
- L'image et la crédibilité de l'établissement sont fortement impactées. Le professionnel doit prévenir ses contacts suite à la découverte de l'attaque. Cela mène à une perte de confiance de la part des usagers.
- Une fuite de données peut exposer les informations confidentielles des usagers, risquant l'usurpation d'identité et une atteinte à la confidentialité, nuisant ainsi à la confiance envers l'établissement.

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 syndic 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 syndic 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 syndic 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 syndic 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 syndic 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 syndic 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 syndic 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 syndic 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