easyPRO Cyber pour les notaires

1. Pourquoi les études notariales sont-elles prises pour cible ?

Les études notariales gèrent des flux d'informations confidentielles par e-mail et sont vulnérables au phishing. Ils détiennent des données personnelles et financières sensibles sur leurs clients, comme les numéros de sécurité sociale et les détails bancaires. Certains études manquent de protections informatiques adéquates, exposant ainsi leurs clients à des risques de violation de la confidentialité.

54 %

Des entreprises ont subi au moins une cyberattaque en 2021. [1]

41 %

Des victimes de ransomware n'ont pas réussi à récupérer leurs données malgré le paiement de la rançon.[2]

2. Exemple concret de cyberattaque

Une étude notariale a été victime d'une fraude au RIB résultant d'une intrusion via le vol d'un mot de passe d'un collaborateur. Cette fraude a entraîné un virement de 12 000 € sur un compte frauduleux.

Qu'aurait pris en charge l'assureur ?
Dans ce cas, easyPRO Cyber aurait pris en charge l'assistance d'urgence de 720 € ainsi que le remboursement total du virement de 12 000 €.

(1) CCESIN - 7ème édition du baromètre annuel - Janvier 2022
(2) Hiscox Assurances - Rapport Hiscox 2022 sur la gestion des cyber-risques - Mai 2022

3. Les principales conséquences d'une cyberattaque

Les cyberattaques réussies paralysent l'activité des études notariales, entraînant une perte de revenus et un impact négatif sur leur réputation.

- En cas d'attaque, tout le système peut être touché et les données chiffrées, une rançon peut être exigée par le hacker. Les données confidentielles (personnelles, bancaires...) peuvent être volées et revendues sur le dark web.
- Les études notariales sont des cibles privilégiées pour les cyberattaques en raison de la sensibilité de leurs données telles que les informations sur les transactions immobilières et les testaments.
- Les conséquences des cyberattaques peuvent être dévastatrices, allant de la paralysie des systèmes informatiques à la corruption des archives client, perturbant ainsi gravement les opérations essentielles.
- L'image et la crédibilité de l'étude peuvent être sérieusement impactées, compromettant la confiance des clients et nécessitant une communication proactive pour restaurer cette confiance.

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 étude 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 étude 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 étude 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 étude 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 étude 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 étude 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 étude 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 étude 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