easyPRO Cyber
pour cabinets d'avocats

1. Pourquoi les cabinets d'avocats sont-ils pris pour cible ?

Si les avocats ne sont historiquement pas les cibles prioritaires des hackers, les incidents se multiplient ces dernières années. Les cabinets d'avocats hébergent de nombreuses données sensibles et sont soumis à une obligation de sécurisation de ces données. En cas de cyberattaque, ces dernières peuvent être diffusées en ligne, représentant un risque de notoriété important dans un secteur où la confidentialité est clé.

40 M €

La rançon demandée au cabinet d'avocats Grubman Shire Meiselas & Sacks en 2020. [1]

87 %

Le pourcentage de personnes prêtes à rompre leur contrat en cas de cyberattaque.[2]

2. Exemple concret de cyberattaque

Un cabinet d'avocats a subi une violation de données à la suite d'une base de données mal protégée. La base contenait des informations personnelles et sensibles, et l'incident a été largement médiatisé en raison de la nature des données compromises. Les pirates ont exigé une rançon initiale de 500 000 €, qui a été revue à la hausse en raison de la sensibilité des informations.

Qu'aurait pris en charge l'assureur ?

easyPRO Cyber aurait indemnisé l'assistance d'urgence, 1 800 € et pris en charge le travail des experts, 1 800 €, la gestion de la communication de crise, 30 000 €, les frais de notification à la CNPD et aux clients, 20 000 €, la reconstitution des données, 10 000 €, le monitoring des données compromises, 40 000 € et l'accompagnement juridique pour non-respect du RGPD, 5 000 €.

(1) Clubic - Un cabinet d'avocats défendant de grandes stars américaines, victime d'une cyberattaque - Mai 2020
(2) TechRepublic - Data privacy: What consumers want businesses to know - Février 2020

3. Les principales conséquences d'une cyberattaque

Le métier d'avocat repose sur la confidentialité des informations partagées entre le client et son avocat. En cas de cyberattaque fructueuse, le cabinet s'expose à la paralysie de son activité, une perte de revenus, mais aussi de crédibilité.

- 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 ordinateurs ne peuvent plus être utilisés, les collaborateurs n'ont plus accès aux données clients et à leur historique. Il existe un risque d'endommagement des systèmes et de corruption des fichiers de données.
- Les données personnelles peuvent fuiter et être revendues sur internet. Le cabinet se retrouve en non-conformité réglementaire et en violation du secret professionnel. Sa responsabilité pénale, civile et professionnelle peut être engagée.
- L'image et la crédibilité du cabinet sont fortement impactées. Cela mène à une perte de confiance de la part de la clientèle.

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