



easyPRO Cyber pour agences immobilières

1. Pourquoi les agences immobilières sont prises pour cibles ?

Historiquement préservé des cyberattaques, le secteur immobilier doit aujourd'hui faire face à des risques de plus en plus élevés. Agences immobilières, promoteurs et bailleurs traitent un volume de données personnelles important et traitent des transactions d'un montant élevé. Autant d'éléments attractifs pour les hackers. En cas d'attaque fructueuse, l'activité est paralysée temporairement. Cela représente un coût financier conséquent, ainsi qu'un risque pour la réputation de l'entreprise.

74 %

du secteur n'est pas prêt à une cyberattaque, pourtant il est dans le top 5 des cibles. ⁽¹⁾

54 %

C'est la part des entreprises qui ont subi au moins une cyberattaque en 2021. ⁽²⁾

2. Exemple concret de cyberattaque



Une agence immobilière a été victime d'une attaque de phishing après qu'un employé ait ouvert un email frauduleux se faisant passer pour un client. Les cybercriminels ont ainsi accédé aux systèmes de l'agence et volé des informations sensibles, incluant des détails bancaires et des contrats immobiliers.

Qu'aurait pris en charge l'assureur ?

easyPRO Cyber aurait pris en charge l'assistance d'urgence de 720 €, les frais de notification aux autorités de 2 000 €, les frais de reconstitution des données à hauteur de 2 000 €, les frais de responsabilité civile car c'est une atteinte aux données de 10 000 € et enfin, la perte d'exploitation de 30 000 €.

3. Les principales conséquences d'une cyberattaque

Les cyberattaques qui atteignent leurs objectifs paralysent l'activité des agences immobilières, des promoteurs et des bailleurs. Cela entraîne une perte de revenus et nuit à la réputation de l'agence.

- Un ransomware peut être déposé, les données, chiffrées, et une demande de rançon, formulée.
- Les données personnelles peuvent fuir et être revendues sur internet. L'agence peut se retrouver en non conformité sur le RGPD et s'exposer à des sanctions.
- Les ordinateurs ne peuvent plus être utilisés, les collaborateurs de l'agence ne peuvent plus accéder aux dossiers des clients, ni à leur historique. Les clients n'ont plus accès à leur espace personnel en ligne. Il existe un risque d'endommagement des systèmes et de corruption des fichiers de données.
- L'image et la crédibilité de l'agence immobilière sont fortement impactées. L'accès au site est souvent suspendu pendant quelque temps (entre 1h à plusieurs semaines) et l'agence doit prévenir ses contacts, dont ses clients, suite à la découverte de l'attaque. 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 agence 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 agence est victime d'une cyberattaque et les données personnelles de l'un de vos clients fuient 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 fuient 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 agence 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 agence 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 rencontre 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 fuient et la CNPD lance une enquête à votre rencontre. 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 agence 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 agence 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 agence 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 agence est victime d'une cyberattaque et les malfaiteurs utilisent vos lignes téléphoniques pour appeler des numéros surtaxés. Nous prenons alors en charge le surcoût.

