easyPRO Cyber pour fiducières

1. Pourquoi les fiduciaires sont-elles prises pour cible ?

Les fiduciaires sont des cibles de choix pour les cybercriminels. Elles concentrent un volume considérable de données financières sensibles : bilans comptables, déclarations fiscales, données sociales, IBAN, informations patrimoniales et personnelles de leurs clients. Leur rôle de tiers de confiance entre les entreprises et les administrations les rend particulièrement attractives, pirater une fiduciaire, c'est accéder en une seule attaque aux données de dizaines ou centaines d'entreprises clientes.

Les fiduciaires dépendent fortement de leurs hébergeurs et logiciels métier (ERP comptables, plateformes cloud partagées), ce qui crée un risque d'effet domino en cas d'attaque sur un prestataire commun. L'autorité nationale alerte sur le fait que les cybercriminels ciblent désormais les sous-traitants critiques des grandes entreprises, les fiduciaires en font partie. En cas de violation, les obligations RGPD et les risques de sanctions de la CNPD peuvent être considérables.

4 120 attaques/semaine

Moyenne d'attaques par semaine pour le secteur des services aux entreprises en Europe en 2025, soit environ 2,5 fois plus que la moyenne européenne globale de 1 673 attaques. [1]

49 %

Taux d'entreprises européennes victimes d'une cyberattaque significative en 2023, le secteur comptable étant une cible privilégiée en raison de ses données financières sensibles. [2]

2. Exemple concret de cyberattaque

Une fiduciaire a été infectée par un logiciel malveillant qui a exfiltré les données financières sensibles de ses clients, compromettant leur confidentialité. Bien que l'intrusion ait été détectée, les données volées ont été mises en vente sur le dark web, obligeant la fiduciaire à informer ses clients de la situation, gérer la crise de confiance et renforcer ses systèmes de sécurité pour éviter de futurs incidents. Plusieurs clients ont envisagé des poursuites judiciaires pour manquement à la confidentialité.

Qu'aurait pris en charge l'assureur ?

L'assurance easyPRO Cyber aurait pris en charge l'assistance d'urgence pour 720 €, la notification pour 5 000 €, la reconstitution des données exfiltrées pour 20 000 €, la responsabilité civile pour 80 000 €, et le monitoring des données pour 10 000 €.

(1) Cyberattaque Coaxis, décembre 2023, Adnov.fr / Lefebvre Dalloz 2025
(2) CYBER SECURITY REPORT 2026, Check Point 2026

3. Les principales conséquences d'une cyberattaque

Les cyberattaques réussies paralysent les fiduciaires, pouvant entraîner une interruption d'activité, une perte de revenus ou encore avoir un impact négatif sur l'image de marque, dans un métier fondé sur la confiance et la rigueur.

- Systèmes comptables bloqués : les attaques peuvent chiffrer ou compromettre les logiciels de gestion, les outils de déclarations fiscales ou les dossiers clients. Cela entraîne des retards dans les obligations comptables et fiscales avec des conséquences directes pour les clients.
- Effet domino sur les clients : une attaque sur la fiduciaire se propage aux données de dizaines d'entreprises clientes, les exposant à leur tour à des fraudes, des retards de TVA, de DSN et des poursuites.
- Vol de données financières ultra-sensibles : bilans, IBAN, données fiscales et patrimoniales peuvent être revendus sur le dark web ou exploités pour des fraudes financières ciblées contre les clients.
- Perte de confiance des clients : la fuite d'informations confidentielles peut altérer durablement la relation avec les clients et engager la responsabilité civile professionnelle de la fiduciaire.
- Conséquences réglementaires et juridiques : en cas de violation de données, la fiduciaire peut être exposée à des plaintes, des sanctions de la CNIL ou à des contentieux clients.

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 fiduciaire 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 fiduciaire 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 fiduciaire 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 fiduciaire 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 fiduciaire 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 fiduciaire 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 fiduciaire 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 fiduciaire 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