



easyPRO Cyber pour crèches

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

Les crèches numérisent massivement leurs processus : cahiers de transmissions numériques, portails familles, logiciels de facturation, dossiers médicaux des enfants. Cette digitalisation accélérée les rend particulièrement vulnérables aux cyberattaques. Elles stockent des données extrêmement sensibles : informations médicales (allergies, vaccinations), données d'identité des enfants et des familles, coordonnées bancaires, photos, autant d'éléments précieux pour les cybercriminels.

Les données concernant des mineurs bénéficient d'une protection renforcée sous le RGPD, exposant les crèches à des sanctions importantes en cas de fuite. De plus, les crèches sont souvent des petites structures peu dotées en ressources informatiques, avec des mots de passe peu sécurisés et des réseaux Wi-Fi non protégés. Leur dépendance à des prestataires numériques partagés (logiciels SaaS) multiplie les points d'entrée pour les hackers, qui savent que la pression est maximale pour rouvrir rapidement.

+264 %

hausse des cyberattaques entre 2021 et 2022 pour les entreprises de moins de 10 salariés, catégorie regroupant la quasi-totalité des crèches. ^[1]

88 %

Risque de ransomware sur les PME (vs 39 % grandes entreprises), paralysant l'accès aux dossiers enfants et à la facturation. ^[2]

2. Exemple concret de cyberattaque



Une crèche a été victime de cyberfraude, avec des criminels usurpant l'identité d'un fournisseur de logiciel de gestion pour demander un changement de RIB. La structure a transféré 50 000 euros vers un compte frauduleux, entraînant une perte financière significative et la nécessité de renforcer les procédures de vérification pour prévenir de futures fraudes. En parallèle, plusieurs crèches utilisant le même prestataire de cahier de transmissions numérique ont simultanément perdu l'accès à leurs données à la suite d'une cyberattaque visant leur prestataire.

Qu'aurait pris en charge l'assureur ?

L'assurance easyPRO Cyber aurait pris en charge l'assistance d'urgence de 720 € pour la gestion du sinistre ainsi que le remboursement total du virement frauduleux de 12 000 €.

[1] Chambre de Commerce Luxembourg, Eco News Flash 2023/15

[2] Verizon Data Breach Investigations Report 2025

3. Les principales conséquences d'une cyberattaque

Les cyberattaques réussies paralysent les crèches, pouvant entraîner une interruption d'activité, une perte de revenus ou encore avoir un impact négatif sur l'image de la structure auprès des familles.

- Paralyse du fonctionnement quotidien : accès aux dossiers des enfants, plannings, cahiers de transmission et outils de facturation bloqués. Le personnel ne peut plus travailler normalement.
- Fuite de données ultra-sensibles : informations médicales, photos d'enfants, coordonnées des familles, des données de mineurs soumises à une protection renforcée sous le RGPD, pouvant entraîner des sanctions importantes de la CNPD. une perte de chiffre d'affaires immédiate et une perte de confiance de la clientèle.
- Cyberfraude et détournement de fonds : usurpation d'identité de fournisseurs pour changer des RIB et détourner des virements, une menace très répandue dans les petites structures.
- Impact sur la confiance des familles : la perte de données personnelles d'enfants nuit durablement à la réputation de la structure et peut engager sa responsabilité civile.
- Responsabilité juridique renforcée : les données de mineurs bénéficient d'une protection spéciale sous le RGPD. Les amendes et litiges légaux peuvent être lourds de conséquences.

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 crèche 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 crèche 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 crèche 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 crèche 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 crèche 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 crèche 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 crèche 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 crèche est victime d'une cyberattaque et les malfaiteurs utilisent vos lignes téléphoniques pour appeler des numéros surtaxés. Nous prenons alors en charge le surcoût.

