easyPRO Cyber pour administrations communales

1. Pourquoi les administrations communales sont prises pour cibles ?

Les administrations communales, en raison de la nature sensible des données qu'elles détiennent (état civil, données fiscales, informations administratives), constituent des cibles privilégiées pour les cybercriminels. Leur niveau de maturité en cybersécurité reste encore hétérogène, ce qui en fait des organisations vulnérables face à des attaques de plus en plus industrialisées et accessibles. Aujourd'hui, les attaquants ne ciblent plus uniquement les grandes entreprises : les collectivités locales sont devenues un point d'entrée stratégique pour perturber les services publics et accéder à des données sensibles.

24 %

des incidents traités par l'ANSSI en 2025 concernent les ministères et les collectivités territoriales. [1]

4 mois

Un cas concret de durée de rétablissement observée après une cyberattaque grave dans une administration communale.[1]

2. Exemple concret de cyberattaque

Une administration communale est victime d'une attaque par ransomware après l'ouverture d'un email frauduleux. L'ensemble du système d'information est chiffré : état civil, services administratifs et outils métiers deviennent inaccessibles. Cette paralysie entraîne l'interruption de plusieurs services publics essentiels pendant plusieurs jours. Les cybercriminels exigent le paiement d'une rançon et menacent de publier les données sensibles de la collectivité.

Qu'aurait pris en charge l'assureur ?

easyPRO Cyber aurait pris en charge l'assistance d'urgence pour la gestion du sinistre à hauteur de 720 €, les frais d'experts pour la reconstitution du système informatique et des données estimés à 20 000 €, ainsi que la perte d'exploitation liée à l'interruption des services pouvant atteindre 60 000 €.

(1) ANSSI - CERT-FR, Panorama de la cybermenace 2025, Réf. CERTFR-2026-CTI-002, publié le 11 mars 2026.

3. Les principales conséquences d'une cyberattaque

Si la cyberattaque est fructueuse, l'attaquant peut paralyser l'activité de l'administration communale, mais aussi celle de ses clients.

- 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 services sont interrompus, les cyberattaques peuvent perturber les systèmes informatiques de la mairie et entrainer l'interruption des services essentiels tels que la collecte des déchets, l'eau potable, l'éclairage public...
- Des vols de fonds publics ou de la manipulation de comptes bancaires de la municipalité peut être commise.
- L'image et la réputation de la collectivité peuvent être fortement impactées. Les résidents et les entreprises locales peuvent connaître un sentiment d'insécurité.

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 administration communale 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 administration communale 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 résidents fuitent et parmi ces données se trouvent des informations sensibles et/ ou des informations permettant d'identifier directement ou indirectement un résident. 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 administration communale 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 administration communale 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 administration communale 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 administration communale 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 administration communale 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 administration communale 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