

Assurance cyber : ce qu'elle couvre vraiment

Un filet de sécurité précieux — à condition de remplir les exigences du contrat et de savoir lire les exclusions.

9 min de lecture · Niveau Intermédiaire · cyberionis.fr/ressources/assurance-cyber

L'assurance cyber n'empêche aucune attaque, mais elle peut faire la différence entre un mauvais trimestre et un dépôt de bilan. Encore faut-il comprendre ce qu'elle couvre, ce qu'elle exclut, et surtout ce qu'elle exige de vous — car un questionnaire rempli avec optimisme peut annuler la garantie le jour du sinistre.

1. Ce qu'un contrat couvre typiquement

- L'assistance à la gestion de crise : experts techniques, juristes, communication — souvent la partie la plus précieuse pour une PME
- Les frais de restauration des systèmes et des données
- Les pertes d'exploitation pendant l'interruption
- Les frais juridiques et les notifications RGPD (CNIL, personnes concernées)
- La responsabilité civile si des données de tiers sont compromises

2. Ce qu'il faut vérifier de près

- Les exigences de sécurité conditionnant la garantie : MFA, sauvegardes, EDR, mises à jour — non respectées, elles peuvent justifier un refus d'indemnisation
- Le questionnaire de souscription : chaque réponse vous engage ; répondre « oui » à « avez-vous la MFA partout ? » sans l'avoir est le piège classique
- Les exclusions : fraude au virement (parfois couverte séparément), actes de guerre, systèmes obsolètes non maintenus
- Les plafonds et franchises par type de sinistre — pas seulement le plafond global
- Le délai et la procédure de déclaration : appeler l'assureur fait partie des premiers gestes de la réponse à incident

3. L'assurance vient après la prévention

Les assureurs ont durci leurs conditions : sans MFA, sans sauvegardes testées et sans protection des postes, beaucoup refusent désormais d'assurer — ou à des tarifs dissuasifs. La démarche vertueuse est donc la même que pour la sécurité : mettre en place les fondamentaux d'abord. Bonus : un bon niveau de sécurité démontrable se traduit directement en prime réduite.

4. Le jour du sinistre : bien utiliser son contrat

- Appeler la hotline de crise de l'assureur dès les premières heures — pas après avoir tout tenté seul : l'assistance fait partie du contrat et intervenir tôt limite les dégâts (et les discussions sur le préjudice)
- Respecter scrupuleusement le délai de déclaration du contrat (souvent 48 h à quelques jours)
- Documenter tout : chronologie, captures, factures des frais engagés, temps passé — le dossier d'indemnisation se construit pendant la crise, pas après
- Déposer plainte rapidement : c'est une condition quasi systématique, et la loi l'impose sous 72 h pour l'indemnisation d'une rançon
- Ne rien signer ni payer (prestataires d'urgence, négociateurs) sans accord de l'assureur si vous voulez être remboursé

CAS CONCRET

Cas vécu par de nombreuses PME : le questionnaire de souscription indiquait « MFA déployée sur tous les accès distants ». Après le sinistre, l'expert constate qu'un accès VPN d'un prestataire n'en avait pas — c'est justement la porte d'entrée. Résultat : indemnisation refusée pour déclaration inexacte. Le questionnaire n'est pas une formalité commerciale, c'est une pièce contractuelle.

L'essentiel à retenir

- 01 Faire l'inventaire exact de vos mesures avant de remplir le questionnaire
- 02 Vérifier que les exigences du contrat (MFA, sauvegardes...) sont réellement en place
- 03 Lire les exclusions et les plafonds par type de sinistre
- 04 Vérifier si la fraude au virement est couverte (souvent une option séparée)
- 05 Intégrer le numéro de l'assureur à votre fiche réflexe incident
- 06 Revoir le contrat chaque année, à mesure que votre système évolue

Questions fréquentes

Combien coûte une assurance cyber pour une PME ?

De quelques centaines à quelques milliers d'euros par an selon le chiffre d'affaires, le secteur, les plafonds choisis et surtout votre niveau de sécurité démontrable : MFA, sauvegardes testées et EDR font baisser la prime, parfois de moitié. Un courtier spécialisé cyber aide à comparer des contrats devenus très hétérogènes.

Nous avons déjà une multirisque professionnelle. Ne couvre-t-elle pas déjà le cyber ?

Rarement au-delà du symbolique : les multirisques classiques excluent généralement les dommages immatériels d'origine cyber, ou les plafonnent très bas. Vérifiez noir sur blanc ce que couvre votre contrat actuel — la découverte du trou de garantie le jour du ransomware est un classique douloureux.

L'assurance rembourse-t-elle la rançon ?

Certains contrats le prévoient, dans un cadre légal strict (dépôt de plainte sous 72 h, destinataire non soumis aux sanctions internationales). Mais toutes les autorités déconseillent le paiement, et les assureurs restreignent de plus en plus cette garantie. Le vrai enjeu du contrat est ailleurs : l'assistance de crise, la reconstruction et les pertes d'exploitation.

Que vérifie l'assureur avant d'indemniser ?

La conformité entre vos déclarations de souscription et la réalité au jour du sinistre : l'expertise post-incident reconstitue comment l'attaque est entrée. Si la porte d'entrée est précisément une mesure que vous déclariez avoir (MFA, sauvegardes, mises à jour), le refus ou la réduction d'indemnité est probable. D'où la règle : déclarer exactement, et maintenir dans le temps ce qu'on a déclaré.

Pour aller plus loin

Cybermalveillance.gouv.fr — l'assurance du risque cyber — www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/assurance-cyber-risques

AMRAE — LUCY, rapport annuel sur l'assurance cyber — www.amrae.fr

Structurer sans vous noyer dans la paperasse ?

Audit, mise en conformité, chartes et sensibilisation des équipes : un accompagnement à la taille de votre entreprise.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr