

Cyber Plan

Assurance des risques cybernétiques

En Belgique, les cyber attaques font 36 victimes déclarées par jour. Selon les spécialistes, ce nombre ne peut que croître dans les prochaines années. Pour protéger vos clients contre ces menaces, Allianz lance Cyber Plan : une assurance hybride qui combine responsabilité, pertes d'exploitation, dommages propres et assistance informatique.

Points forts de Cyber Plan

Cyber Plan couvre les dommages immatériels d'origine cybernétiques. Principaux atouts :

- 4 volets de garantie pour une couverture optimale (responsabilité, perte d'exploitation, frais de gestion de crise, pertes subies)
- Un capital assuré à partir de 250.000 euros par sinistre et par année d'assurance
- Des montants supérieurs ou sur mesure sont possibles sur demande
- Une assistance 24 heures sur 24, 7 jours sur 7, d'un bureau d'avocats spécialisés et d'experts en IT pour permettre une réaction rapide à un évènement assuré
- Une franchise unique à partir de 2.500 euros
- Des conditions générales claires et transparentes.
- Intervention en cas de notification dans le cadre de GDPR.
- Une assistance sans franchise pendant les 72 premières heures.

Cible

Cyber Plan s'adresse à toute société :

- établie en Belgique, sans limite inférieure de taille
- désirant couvrir les dommages immatériels purs auxquels elle pourrait être exposée
- pour quasi toute activité professionnelle et lui propose :
- une solution standard de souscription rapide si elle développe un chiffre d'affaires allant jusqu'à 100.000.000 euros
- une solution sur mesure si elle présente un chiffre d'affaires entre 100.000.000 et 250.000.000 euros.

Preneur d'assurance

La société, personne morale.



Garanties dans le détail

Garanties de responsabilité

Atteinte aux données personnelles et les atteintes aux données informatiques

Couverture :

- des atteintes aux données personnelles (accès, utilisation ou divulgation non autorisée de données personnelles stockées dans le système informatique du preneur d'assurance ou d'une filiale)
- des atteintes aux données informatiques (notamment la communication et/ou divulgation non-intentionnelle de données clients par l'assuré ou le prestataire de services externalisés).

Atteinte frauduleuse au réseau

Prise en charge :

- du montant des dommages-intérêts
- des frais de défense suite à une réclamation contre un ou plusieurs assurés et consécutive à une atteinte frauduleuse (exemple : une cyber-attaque suite à un acte, une erreur ou une omission d'un assuré).

Atteinte par publication/diffusion

Prise en charge :

- du montant des dommages-intérêts
- des frais de défense suite à une réclamation contre un ou plusieurs assurés et consécutive à une atteinte par publication/diffusion.

Sont notamment couverts, les publications ou diffusions par l'assuré de données numériques causant :

- une atteinte non intentionnelle aux droits de propriété intellectuelle
- un dénigrement
- une atteinte au droit au respect de la vie privée d'un individu
- la divulgation d'informations personnelles ou l'appropriation à des fins commerciales du nom, de l'image ou de l'apparence d'une personne
- une situation de concurrence déloyale, etc.

Sanctions administratives

Prise en charge :

- du montant des frais de défense
- des sanctions administratives telles que les amendes et pénalités financières imposées à un assuré à la suite d'une réclamation formulée par un régulateur.

Réclamations des prestataires de services de paiement électronique

Couverture :

- des dommages-intérêts
- des pénalités contractuelles
- des frais de défense

résultant d'une réclamation introduite par un prestataire de services de paiement électronique, fondée sur la violation non-intentionnelle de toute Norme de Sécurité des Données PCI.

Garantie pertes d'exploitation

Couverture des pertes d'exploitation à la suite d'une interruption d'activité due à l'inaccessibilité totale ou partielle du système informatique.

Garanties frais de gestion de crise

Frais du consultant chargé du chiffrage des pertes

Couverture des honoraires de tout expert informatique pour déterminer l'étendue et le montant des pertes.



Sont toujours exclus, les frais engagés pour déterminer si un sinistre, une réclamation ou une perte est oui ou non couverte.

Frais des consultants en communication de crise

Prise en charge des honoraires d'un consultant en communication de crise afin d'atténuer les effets négatifs sur la réputation de l'assuré.

Frais d'investigation numérique

Couverture des honoraires de tout expert informatique en vue d'établir l'existence ou non et l'étendue :

- d'une atteinte aux données personnelles
- d'une atteinte aux données informatiques
- d'un évènement perte d'exploitation.



Ces frais ne sont couverts que si l'assuré dispose d'éléments permettant de suspecter l'existence des atteintes reprises ci-dessus.

Frais d'intervention

En cas d'atteinte aux données personnelles ou informatique, couverture des honoraires de tout expert informatique pour :

- l'analyse du système informatique en vue de déterminer :
 - l'existence, la cause et l'étendue de l'atteinte aux données personnelles ou informatiques
 - la manière dont il est possible d'en atténuer les conséquences.
- l'identification et la préservation des données informatiques pertinentes dans le système informatique de la société assurée
- les conseils à l'assuré sur son obligation légale d'informer toute victime, tout client, tout régulateur sur l'existence d'une atteinte aux données personnelles ou informatiques
- la notification de l'atteinte aux données personnelles ou informatiques à une personne victime, à un tiers ou à un régulateur, conformément aux obligations légales
- les conseils à l'assuré sur les obligations d'indemnisation dans tout contrat écrit signé entre l'assuré et tout prestataire de services tiers
- la mise en place d'une plateforme téléphonique d'information au profit des personnes victimes et des tiers
- l'établissement et la fourniture aux personnes victimes et aux clients :
 - de nouvelles références de compte bancaire
 - de services de contrôle des crédits (jusqu'à six mois après la date de ladite atteinte)
 - de conseils liés au sinistre afin de respecter toute autre exigence légale relative à l'atteinte aux données personnelles devant être remplie par l'assuré vis-à-vis des personnes victimes.



Uniquement lorsque ces pratiques sont autorisées légalement.

Frais de restauration

Couverture des frais de recours à un expert informatique suite à une atteinte aux données personnelles ou informatiques, ou d'un évènement perte d'exploitation afin de :

- restaurer le système informatique des assurés dans un état comparable à celui avant le sinistre.
- procéder à la restauration, la récupération ou la réinstallation technique des données informatiques ou des programmes informatiques des assurés (y compris le coût d'achat d'une licence de logiciel nécessaire pour reproduire ces données informatiques ou ces programmes informatiques).



Sont exclus :

- les frais pour respecter toute décision de remise en état par voie d'injonction de faire ou toute autre réparation en nature et/ou non pécuniaire, toute attribution d'une telle remise en état ou tout accord de mise en œuvre d'une telle remise en état
- les frais de défense et les dépenses de toute sorte
- les coûts engendrés en l'absence d'évènement perte d'exploitation
- le coût de conception, de mise à niveau, de maintenance ou d'amélioration du système informatique ou des programmes informatiques
- les frais internes de l'assuré, y compris les charges sociales et les frais généraux
- les coûts de restauration des données ou des programmes informatiques exclusivement stockés dans la mémoire vive ou la mémoire « RAM ».

Garanties des dommages propres

Cyber extorsion

Remboursement des pertes suite à une menace d'extorsion cybernétique.



Conditions de couverture :

L'assuré doit :

- prendre les mesures nécessaires pour ne pas communiquer l'existence de la présente garantie à moins que cette communication soit requise par la loi.
- informer et coopérer pleinement avec lesdits services de police ou toute autorité publique (dépôt de plainte pour une menace d'extorsion dans les 48h suivant la menace)
- limiter les pertes causées par la menace en faisant intervenir un conseil spécialisé en matière de sécurité (avec accord écrit d'Allianz).



Sous-limite à 25% du montant assuré, par sinistre et par année d'assurance.

Vol cybernétique

Remboursement de la monnaie scripturale virée ou transférée des comptes de la société assurée* vers un compte tiers, à la suite d'une cyber attaque.



Sous-limite de 50.000 € par sinistre et par année d'assurance.

Etendue de la garantie

Dans l'espace

La garantie s'étend au monde entier.

Dans le temps

Allianz couvre :

- les réclamations formulées pendant la période de validité du contrat
- pour des faits ou fautes survenus ou commis
 - pendant la période de validité du contrat
 - ou même avant le contrat (mais non connus à la souscription), et ce sans limite dans le temps
- les réclamations formulées dans les 36 mois après le contrat et se rapportant à des faits ou fautes survenus ou commis pendant la période de validité du contrat.

Montants assurés

Formules au choix à partir de 250.000 euros.

Souscription simplifiée

Le Cyber Plan peut être souscrit de façon standard et simplifiée, aux conditions suivantes :

1. Les activités du preneur d'assurance et/ou ses filiales et/ou ses produits ne sont pas liés à des pays/ régions ou localisations soumises à des sanctions et/ou embargos.

Ces pays en septembre 2017 sont :

Afghanistan, Arménie, Azerbaïdjan, Balkans occidentaux, Belarus, Birmanie (Myanmar), Burundi, République centrafricaine, Chine, Cuba, République Démocratique du Congo, Égypte, Érythrée, Guinée, Guinée-Bissau, Iran, Irak, Liban, Liberia, Libye, Corée du Nord, Russie, Somalie, Soudan (Sud), Soudan (Nord), Syrie, Tunisie, Ukraine, Est de l'Ukraine (Provinces de Donetsk, de Kharkiv, de Louhansk, de Zaporizhia et de Dnipropetrovsk), Crimée (en ce compris ses eaux territoriales et Sebastopol), Yémen, Venezuela, Zimbabwe.

Cette liste est évolutive dans le temps et nous sommes à votre disposition pour vous fournir une information actualisée sur le sujet.

2. Les activités du preneur d'assurance, de ses filiales et/ou co-assuré(s) et/ou leurs produits ne relèvent pas des secteurs suivants soumis à sanctions sectorielles :

- Armes, biens et technologies à usage militaire, en ce compris les logiciels destinés à un usage militaire
- Biens à double usage, produits et technologies pouvant avoir une application militaire
- Industrie gazière et pétrolière (y compris, notamment, le pétrole brut, le gaz ainsi que tout autre produit fini ou semi-fini)
- Technologies destinées à un usage dans le secteur du nucléaire, y compris les logiciels (tous types confondus)
- Exportation de graphite, de métaux finis et semi-finis, y compris le fer, l'acier, le cuivre, le nickel, l'aluminium, le plomb, le zinc, l'étain et tout autre métaux dérivé
- Equipements, technologies et logiciels susceptibles d'être utilisés pour la surveillance

Prime

A partir de 600 euros (hors taxes)

Franchise

- À partir de 2.500 euros
- pour la garantie « pertes d'exploitation » : période d'attente de 8 heures. Si cette période est dépassée, l'intervention couvre les pertes à partir de la première heure d'interruption, sous seule déduction de la franchise forfaitaire d'application.

Taxes

9,25%

- Equipements susceptibles d'être utilisés à des fins de répression interne
- Biens culturels et autres biens présentant une importance archéologique, historique, culturelle, scientifique rare ou religieuse
- Commerce des diamants
- Industrie du sexe
- Jeux de hasard et paris
- Production et utilisation d'amiante
- Centrales électriques au charbon / lignite

3. **Le preneur d'assurance et/ou ses filiales n'est(ne sont) pas actif(s) dans les domaines d'activité suivants : jeux de hasard, contrôle aérien, entités gouvernementales, institutions financières et industrie du sexe.**
4. **Le chiffre d'affaires consolidé du preneur d'assurance et de ses filiales est inférieur à € 100.000.000.**
5. **Le preneur d'assurance et/ou ses filiales réalise(nt) moins de 10% de son chiffre d'affaires aux USA/Canada.**
6. **Le preneur d'assurance et/ou ses filiales réalise(nt) moins de 50% de son chiffre d'affaires dans des activités de « e-commerce ».**
7. **Le preneur d'assurance et ses filiales possèdent moins de 1.000.000 de données à caractère personnel.**

Cela porte sur toute information qui concerne une personne physique identifiée ou identifiable (appelée « la personne concernée »). Il peut s'agir du nom d'une personne, d'une photographie, d'un numéro de téléphone (même professionnel), d'un code, d'un numéro de compte en banque, d'une adresse e-mail, d'une empreinte digitale, etc. Pour calculer l'estimation du nombre de données, veuillez établir le nombre de clients personnes physiques avec lesquelles vous travaillez dans le cadre de votre activité.
8. **Le preneur d'assurance et/ou ses filiales confirme(nt) qu'il y a des procédures de sécurité et de contrôle (comme des anti-virus) sur les systèmes IT et sur les hardwares.**
9. **Le preneur d'assurance et/ou ses filiales confirme(nt) qu'il existe des restrictions d'accès aux informations sensibles.**
10. **Le preneur d'assurance et/ou ses filiales confirme(nt) qu'il existe des procédures de back-up et de restauration des données en place.**
11. **Le preneur d'assurance est domicilié en Belgique.**
12. **Le preneur d'assurance n'est détenu par aucune autre personne morale (le preneur d'assurance n'est pas une filiale d'une autre entité juridique).**
13. **Le preneur d'assurance et/ou ses filiales n'ont pas de police d'assurance en place avec AGCS/Allianz Benelux qui couvre les risques « cybernétiques ».**
14. **Au cours des 3 dernières années, la société et/ou ses filiales et/ou leurs administrateurs n'ont pas connaissance d'actes, de faits ou de circonstances qui ont donné lieu ou qui pourraient donner lieu à une réclamation ou à une action contre eux en ce qui concerne les risques cybernétiques.**

L'entreprise ne répond pas aux critères ? Une offre sur mesure peut être proposée.