Questionnaire sur les risques cyber (standard)

Introduction

Le **questionnaire standard sur les risques cyber** doit être complété lorsque
- la somme d'assurance souhaitée pour propres dommages/somme d'assurance combinée est supérieure à CHF 500'000; ou
- la somme d'assurance souhaitée pour responsabilité civile est supérieure à CHF 1 Mio.

Si un ou plusieurs des critères suivants est/sont rempli(s), le **questionnaire étendu sur les risques cyber** doit être complété:
- la somme d'assurance souhaitée pour propres dommages/somme d'assurance combinée est supérieure à CHF 1 Mio;
- la somme d'assurance souhaitée pour la responsabilité civile est supérieure à CHF 2 Mio;
- le chiffre d'affaires cumulé de toutes les entreprises coassurées est supérieur à CHF 100 Mio.

Les questions relatives aux risques se rapportent au proposant/à la proposante, y compris à l'ensemble des entreprises coassurées. Veuillez mentionner, si les réponses aux questions ne s'appliquent qu'à une partie du proposant/de la proposante et des entreprises coassurées. En cas de divergences importantes, il est recommandé de remplir un questionnaire par entreprise.

1. Mesures de protection organisationnelles

1.1 Organisation informatique

Avez-vous désigné une personne interne ou externe responsable de l'informatique au sein de votre entreprise? ☐ Oui ☐ Non

Si oui: nom et fonction (pour une personne externe veuillez préciser le nom de l'entreprise pour laquelle elle travaille)

1.2 Gestion des utilisateurs, gestion des autorisations et directives concernant les mots de passe

Les utilisateurs ont-ils des niveaux d'autorisation/droits d'accès différents dans les systèmes informatiques selon leur fonction et les tâches qui leur sont assignées (y compris droits d'administrateur [accès lié à la fonction à des données financières, personnelles ou de clients, p. ex.])? ☐ Oui ☐ Non

Avez-vous défini et implémenté une politique de mots de passe permettant de garantir des mots de passe solides? ☐ Oui ☐ Non

1.3 Sensibilisation

L'ensemble des utilisateurs informatiques de l'entreprise assurée suivent-ils des formations/séminaires sur le thème de la sensibilisation aux cyber-risques?

☐ Oui, une fois (p. ex. au moment de l'entrée dans l'entreprise)

☐ Oui, les formations/séminaires ont lieu de manière irrégulière (moins d'une fois par an)

☐ Oui, les formations/séminaires ont lieu régulièrement (au moins une fois par an)

☐ Non

1.4 Vérification des transactions financières et des commandes de produits

Dans le cas de transactions financières d'envergure (factures ou ordres de paiement > CHF 30'000), vérifiez-vous l'authenticité de l'ordre de transaction lorsque les destinataires des virements et/ou les coordonnées bancaires ou de paiement sont nouvelles ou modifiées? ☐ Oui ☐ Non

Dans le cas de grosses commandes de produits (> CHF 30'000), en vérifiez-vous l'authenticité? ☐ Oui ☐ Non

2. Mesures de protection techniques

2.1 Sauvegarde des données et des systèmes (back-up)

Au sein de votre entreprise, procédez-vous à une sauvegarde quotidienne de vos données? ☐ Oui ☐ Non

Si non: à quelle fréquence et pourquoi pas quotidiennement?

Êtes-vous informé·e de la réussite ou de l'échec de vos sauvegardes (monitoring)? ☐ Oui ☐ Non

Vérifiez-vous la qualité des sauvegardes au minimum tous les 6 mois (volumétrie comparative ou échantillonnage des données aux fins de vérification de la fonctionnalité, p. ex.)? ☐ Oui ☐ Non

Si non: à quelle fréquence et pourquoi pas tous les 6 mois?

Conservez-vous la sauvegarde en lieu sûr, afin qu'elle ne puisse pas être manipulée, endommagée, détruite ou volée en même temps que les originaux (sauvegardes off site et offline, p. ex., ou autres copies de sécurité inaltérables)? ☐ Oui ☐ Non

2.2 Logiciels antimaliciels et protection d'accès

2.2.1 Pare-feu, antivirus et antivirus de nouvelle génération (NGAV)

Vos réseaux sont-ils protégés par un pare-feu mis à jour régulièrement? ☐ Oui ☐ Non

Avez-vous installé (dans la mesure du possible) sur l'ensemble des terminaux et des serveurs une solution antivirus mise à jour régulièrement?

☐ Oui ☐ Non

☐ En partie, les terminaux restants disposent d'une protection équivalente (isolement, p. ex.)

2.2.2 Accès à distance au réseau de l'entreprise

Est-il possible d'accéder à distance au réseau de l'entreprise? ☐ Oui ☐ Non

Si oui: comment ces accès sont-ils protégés? Il existe un accès à distance:

☐ sans protection d'accès

☐ protégé par un nom d'utilisateur et un mot de passe

☐ protégé par une authentification multifactorielle

2.2.3 Services en nuage

Utilisez-vous des services en nuage? ☐ Oui ☐ Non

Si oui: un ou plusieurs de ces services en nuage ont-ils une importance critique* pour votre entreprise? ☐ Oui ☐ Non

*Sont considérés comme services en nuage critiques pour l'entreprise, les services utilisés pour les processus commerciaux principaux et dont la disponibilité dépend de plus de 30 % du chiffre d'affaires annuel.

Si oui: lesquelles?

Comment sont protégés les accès aux services en nuage d'importance critique pour l'entreprise?
Il existe un accès en nuage:

☐ sans protection d'accès

☐ protégé par un nom d'utilisateur et un mot de passe

☐ protégé par une authentification multifactorielle

Le prestataire externe qui vous propose les services en nuage d'importance critique pour votre entreprise dispose-t-il d'un plan d'urgence et d'un plan de continuité d'activité (BCA, [Business Continuity Plan]) permettant une reprise rapide de vos activités en cas de cyber-incident affectant le prestataire externe?

☐ Oui ☐ Non

☐ Non connu

2.2.4 Autres services disponibles via Internet

Utilisez-vous d'autres services disponibles via Internet: banque en ligne, portail de messagerie, systèmes de billetterie, p. ex.? ☐ Oui ☐ Non

Si l'authentification multifactorielle est disponible pour ces services, est-elle utilisée?

☐ Oui ☐ Non

☐ En partie

2.2.5 Operation technology (OT)

Utilisez-vous operation technology* pour vos activités? ☐ Oui ☐ Non

*Operation Technology (OT) = contrôles de machines, installations et appareils, comme des installations industrielles reliées au réseau de l'entreprise pour la production ou la fabrication, un entrepôt grande hauteur ou des appareils médicaux, p. ex.).

Si oui: les deux réseaux (IT et OT) sont-ils clairement séparés (segmentation des réseaux) et les passerelles entre les réseaux (interfaces logiques ou physiques) sont-elles protégées par des dispositifs (pare-feu, p. ex.) à la pointe de la technologie? ☐ Oui ☐ Non

2.3 Gestion des correctifs

Existe-t-il une gestion des correctifs et des mises à jour garantissant que les derniers correctifs/dernières mises à jour de sécurité sont installés rapidement (c.-à-d. dans les 30 jours au plus tard, sauf si le processus de vérification de la compatibilité des correctifs nécessite davantage de temps)? ☐ Oui ☐ Non

Si oui: à l'exception des installations et des appareils qui sont «out of support»: ces installations et appareils (IT et/ou OT) qui ne bénéficient plus de correctifs/mises à jour de sécurité sont-ils rattachés à des réseaux isolés en conséquence et sans connexion avec les systèmes d'importance critique pour l'entreprise? ☐ Oui ☐ Non

3. Protection des données

Les données sensibles sont-elles cryptées lors de l'envoi (p. ex. en utilisant un VPN ou le protocole HTTPS, sous forme de courriel crypté, ou en utilisant des supports de données cryptés)? ☐ Oui ☐ Non

4. Comportement en cas de sinistre

4.1 Plan d'urgence

Avez-vous défini un plan d'urgence en cas de cyber-incident (Emergency Response Plan)? ☐ Oui ☐ Non

4.2 Gestion de la continuité des activités

Disposez-vous d'un plan écrit (Business Continuity Management Plan – BCM) pour maintenir l'activité de l'entreprise en cas de défaillance de votre informatique? ☐ Oui ☐ Non

Protection des données

Toutes les données à caractère personnel sont traitées conformément à la législation sur la protection des données en vigueur. Vous trouverez les dernières informations à ce sujet sur notre page Internet «Notice explicative sur la politique en matière de protection des données» disponible à l'adresse www.helvetia.ch/protectiondesdonnees.

Déclaration de consentement

Les réponses aux questions doivent être complètes et conformes à la vérité. Si cela est nécessaire à l'examen de la proposition ou de la prestation en raison de l'étendue du risque, les données sont transmises à des fins de traitement aux tiers participant au contrat en Suisse et à l'étranger, en particulier aux réassureurs ainsi qu'aux sociétés du Groupe Helvetia, dans le respect de la loi sur la protection des données suisse.

Le/la proposant·e autorise Helvetia, en vue d'atteindre les buts mentionnés dans la notice explicative sur la protection des données, à se procurer auprès des autorités, d'autres compagnies d'assurance et de tiers ainsi que de leurs auxiliaires toute information, donnée et copie de document pertinente le/la concernant (y compris des renseignements portant sur son état de santé antérieur) et, dans ce cadre, à transmettre à ces tiers les informations nécessaires. Le/la proposant·e délie par conséquent expressément ces tiers et Helvetia de leur secret de fonction et professionnel et de toute obligation de confidentialité, et il/elle autorise ces derniers à donner à Helvetia les renseignements nécessaires et à lui remettre tous les documents pertinents pour l'examen de la proposition, l'exécution du contrat et le règlement des cas de prestations.

Les données reçues peuvent être utilisées par les sociétés du Groupe Helvetia ainsi que par leurs sociétés partenaires pour soumettre des offres de prestations de service personnalisées.

Cette autorisation est valable indépendamment de la naissance du contrat et sans limitation dans le temps. Elle peut être révoquée à tout moment par une déclaration sous forme de texte (p. ex. par courriel) à l'attention d'Helvetia. Toute révocation s'applique uniquement pour le futur. Pour autant que l'autorisation soit nécessaire à la préparation ou à l'exécution du contrat, sa révocation n'est possible que par le biais du retrait de la proposition ou de la résiliation du contrat conformément aux dispositions applicables. Une révocation ultérieure peut entraîner l'impossibilité de fournir des prestations. Helvetia est autorisée à poursuivre le traitement des données même en cas de révocation dans la mesure où la loi l'y autorise ou en cas d'intérêt prépondérant.

Les obligations énoncées dans les conditions d'assurance s'appliquent indépendamment des réponses fournies par le/la proposant·e dans le présent questionnaire.

Le/la proposant·e

Nom du proposant/de la proposante:

Nom et fonction du signataire:

Lieu, date

Signature

120015767 09.23