Cyber-assurance.

Assurances Techniques Suisse.

Claude-Alain Bossens

Ingénieur HES - Ingénieur de sécurité

Senior Underwriter

simple. clair. helvetia

Votre assureur suisse

Cyber-risques?
Exemples de cyber-risques pour les entreprises

Attaque Denial of Service (DoS = déni de service)

- Paralysie de l'entreprise ➔ les systèmes ne peuvent plus assurer la communication par Internet
- Site web devenu inaccessible/surchargé

Sabotage interne par le personnel

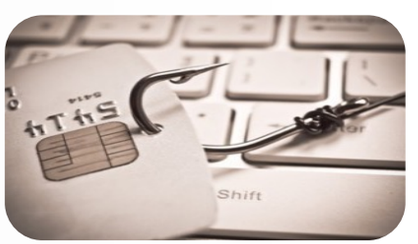
- Vol ou suppression de données
- Installation de logiciel malveillant

Chevaux de Troie / rançongiciel / logiciel malveillant

- Cryptage de données
- Espionnage de données confidentielles
- ➔ Violation de la protection des données
- Utilisation abusive du système

Hameçonnage

- Espionnage des mots de passe ➔ Accès à la banque en ligne
- Manipulation du site web



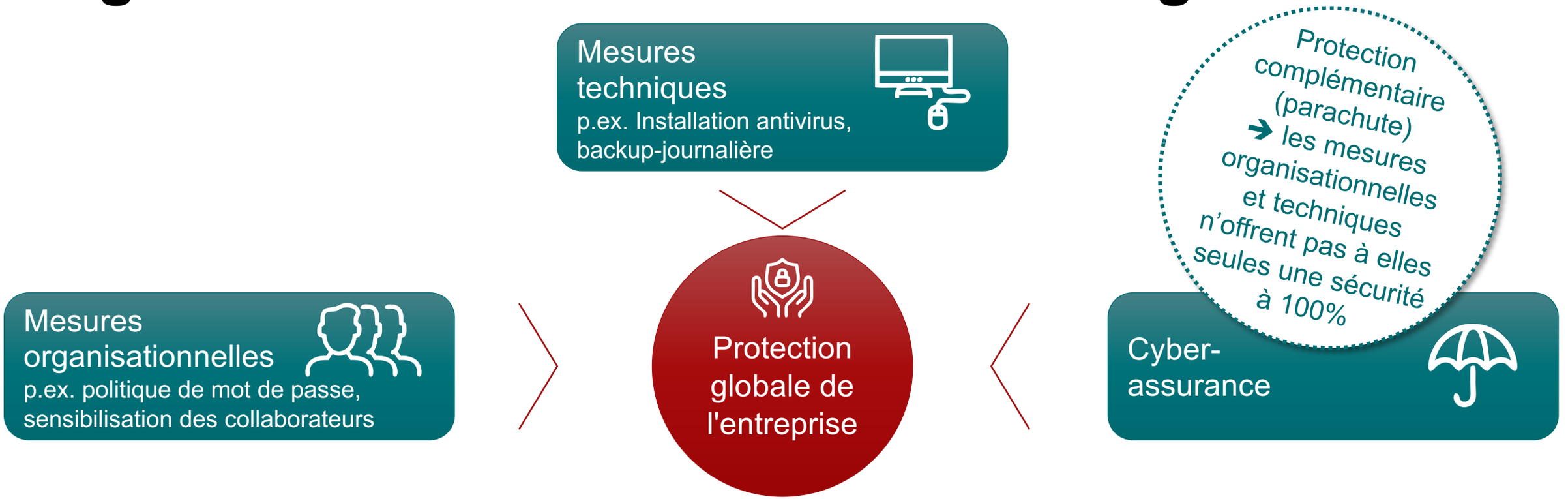
Collaborateur qui fait acte de négligence

- Envoi de données confidentielles au mauvais destinataire

- **Dommages économiques**
- **Préjudice de réputation / Perte de confiance des clients et fournisseurs**
- **Chantages**
- **Prétentions de tiers en responsabilité civile**

helvetia
Votre assureur suisse

Comment se protéger des cyber-risques? Exigences minimales concrètes et tangibles

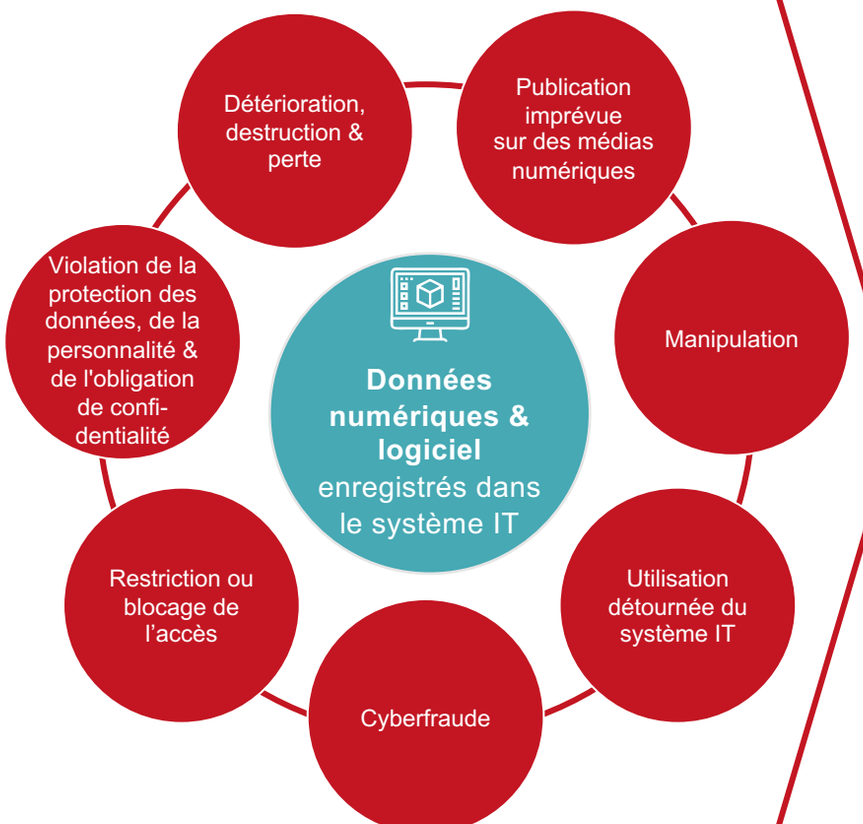


- Catalogue de mesures de sécurité élaboré sur la base de MELANI (Centrale d'enregistrement et d'analyse pour la sûreté de l'information) pour les PME
- Dans son propre intérêt, le client doit respecter les mesures de sécurité figurant dans le catalogue

helvetia
Votre assureur suisse

Helvetia Cyber-assurance – explications en un coup d'œil

Assurés sont les cyber-risques...



...qui sont la conséquence de:

causes criminelles comme

- le sabotage interne par les propres collaborateurs
- l'abus d'une faille du système technique ou de sécurité
- installation/exécution intentionnelle ou non de logiciels corrompus
- installation/utilisation de matériel (hardware) non autorisé
- usage de données d'accès volées
- DoS (déni de service)

causes non criminelles comme

- négligence imputable au personnel
- perturbations de courte durée

avec prestations orientées vers le client pour:

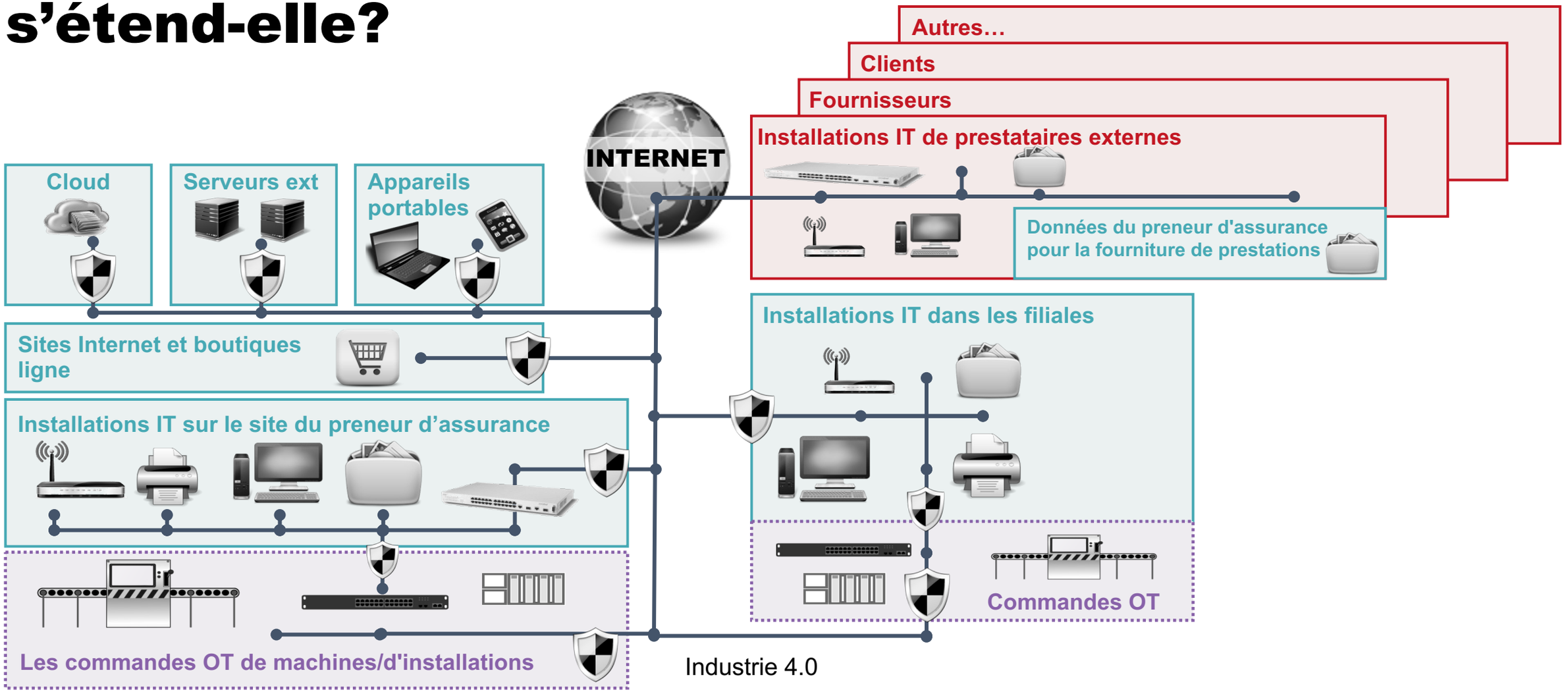
Dommages propres

Sinistres en responsabilité civile

Protection juridique

helvetia
Votre assureur suisse

Base de l’assurance – jusqu’où l’assurance s’étend-elle?



Système IT du preneur d’assurance (base)

Elargissement du système IT avec des commandes OT (optionnel)

Ne sont pas considérés comme des systèmes IT du preneur d’assurance

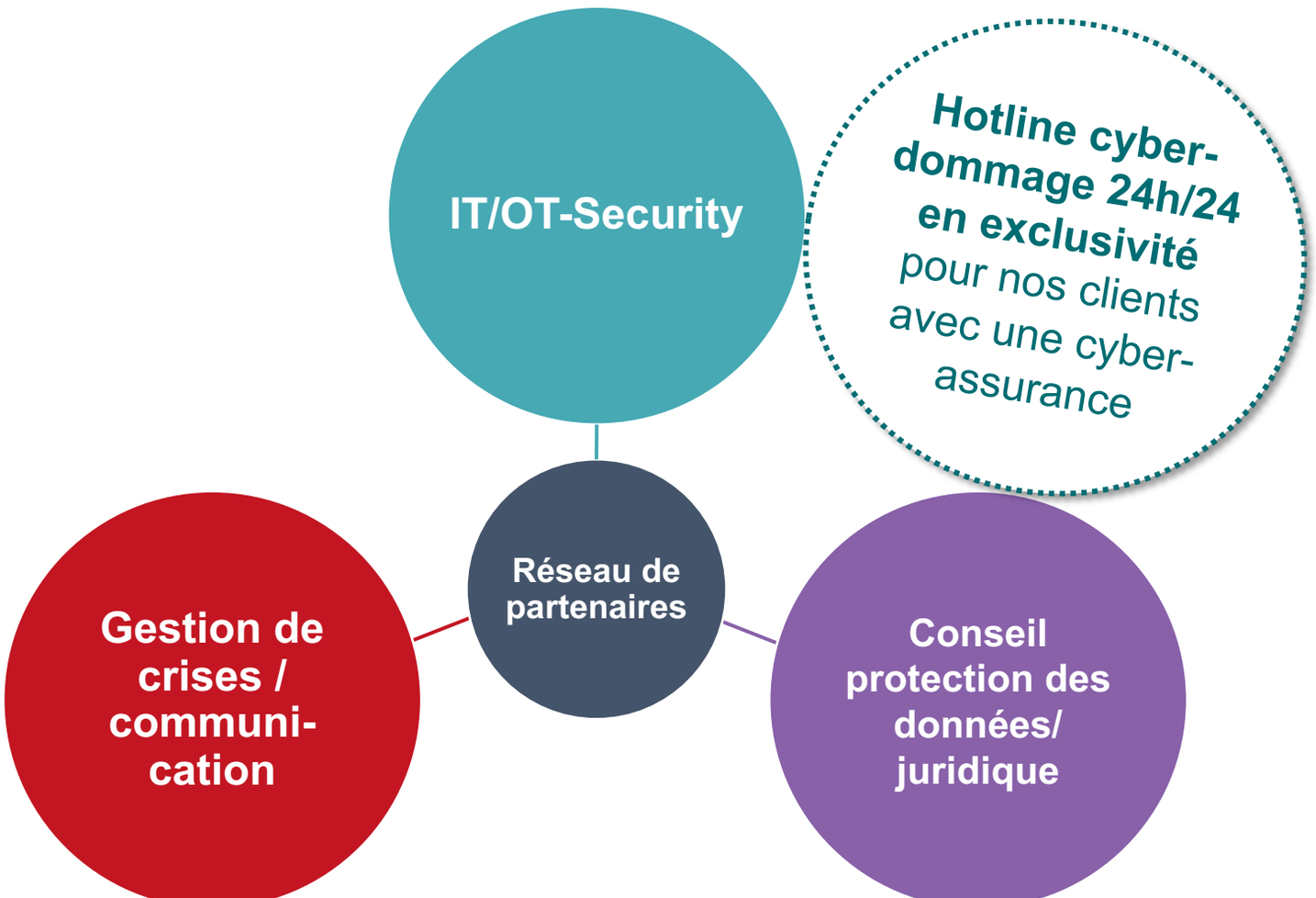
helvetia
Votre assureur suisse

Vue d’ensemble des prestations – à chaque besoin sa solution

Dommages propres (max. SA CHF 5 Mio/durée de prestation 12 mois)	PREMIUM	Sous-limite
Restauration du système	✓	
Reconstruction des données	✓	30% de la SA, max. CHF 50'000 (augmentation de limite possible)
Frais supplémentaires pour la poursuite du traitement des données	✓	
Perte de revenu liée à l’interruption d’exploitation	✓	
Analyse du sinistre / forensique	✓	
Gestion de notification	✓	250'000 pour procédure disciplinaire, de surveillance, administrative ou pénale (non augmentable)
Gestion de la réputation (préjudice de réputation)	✓	
Défense contre le chantage	✓	30'000 pour le paiement de rançon (augmentation de limite possible)
Compensation de patrimoine en raison d’une cyberfraude / d’une manipulation	✓	30'000 pour les transactions financières et commandes de marchandises (augmentation de limite possible)
Production de mauvaise qualité	(✓)	
Dommages en responsabilité civile (max. SA CHF 5 Mio)	PREMIUM	Sous-limite
Dommages économiques purs et dommages immatériels	✓	100'000 pour les prétentions résultant de l'exécution de contrats d'origine criminelle (augmentation de limite possible)
Protection juridique (Coop protection juridique) (SA CHF 20'000)	PREMIUM	Sous-limite
Conseil juridique et première intervention	✓	

helvetia
Votre assureur suisse

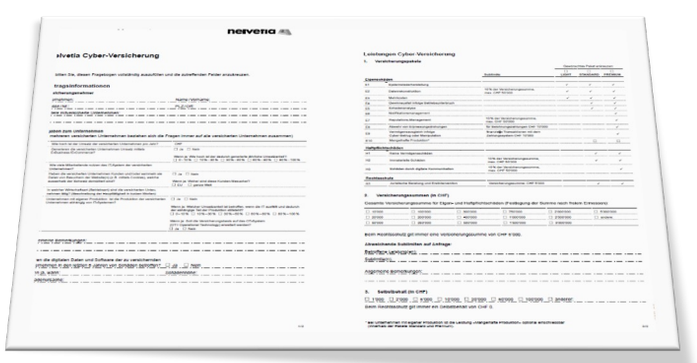
Quel est le réseau d'Helvetia?
Pour les sinistres et conseils en matière de risque



helvetia
Votre assureur suisse

Avec un minimum de données pour l'offre - informations sur les risques pour une offre

- Chiffre d’affaires annuel
- Chiffre d’affaires réalisé en e-commerce (commerce en ligne)
- Nombre de collaborateurs qui utilisent le système IT (utilisateurs de l’informatique)
- Origine de la clientèle et des données (pays)
- Secteur économique (type d’activité)
- Pour les entreprises industrielles: dépendance de l’informatique



helvetia
Votre assureur suisse

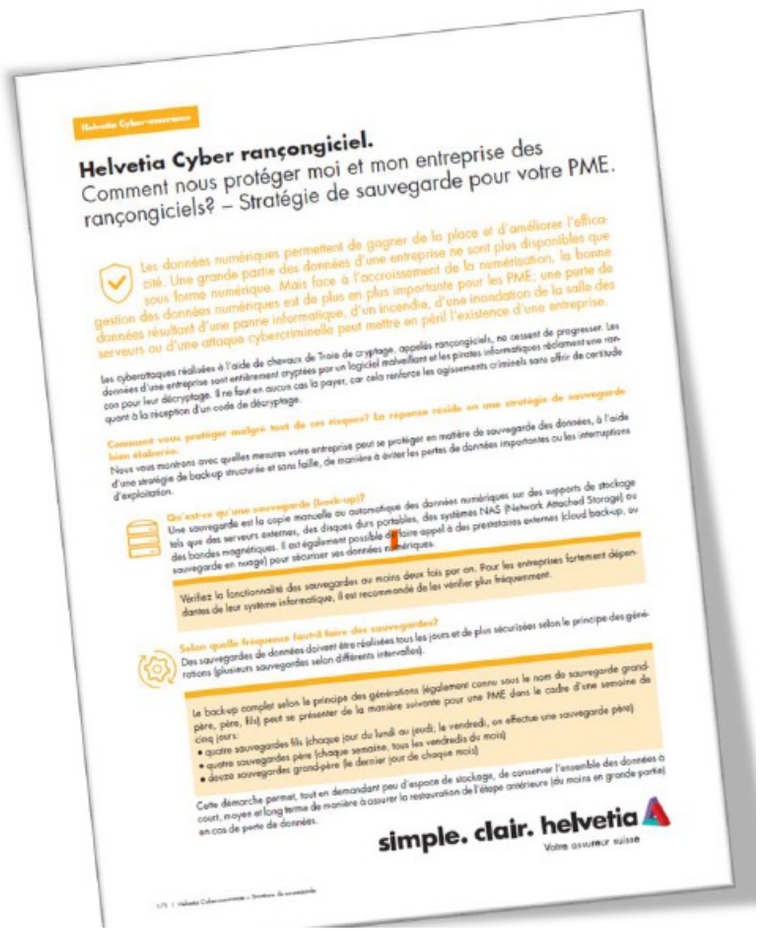
Merci pour votre attention.

helvetia 20.20

simple. clair. helvetia

Votre assureur suisse

Mesure préventive :
Protection contre les rançongiciels



Helvetia Cyber rançongiciel.

Comment nous protéger moi et mon entreprise des rançongiciels? – Stratégie de sauvegarde pour votre PME.

simple. clair. helvetia

Votre assureur suisse

Guide "Stratégie de sauvegarde pour PME"

Pour plus d'informations : www.helvetia.ch/cyber-assurance

→ Rançongiciels : Comment les PME peuvent-elles se protéger?

→ Bénéficiez de recommandations et de conseils pour sauvegarder vos données à l'aide d'une stratégie de sauvegarde structurée et transparente.

→ Demander le soutien de nos partenaires dans ce domainre.

helvetia
Votre assureur suisse

Catalogue de sécurité (1/2)
Mesures organisationnelles

- Nomination d’un responsable informatique (interne ou externe)
- Définition et implémentation d’une gestion des autorisations avec différents niveaux de pouvoirs
- Définition et implémentation d’une password policy (politique de mots de passe)
- Sensibilisation régulière et formation à la sécurité des assurés en matière de cyber-risques

Catalogue de sécurité (2/2)
Mesures techniques

- Sauvegarde journalière des données (Backup). La sauvegarde ne peut pas être écrasée avant un délai d'une semaine. La qualité de la sauvegarde des données doit être vérifiée de manière hebdomadaire (p. ex. comparaison du volume de données, vérification de la fonctionnalité par échantillonnage de données). Les sauvegardes doivent être archivées de manière à ce qu'elles ne puissent pas être manipulées, endommagées, détruites ou volées avec les données originales;
- Installation de solutions de protection techniques fondamentales actuelles et conformes à l'état de la technique telles que des pare-feu, programmes antivirus, filtres anti-spam, logiciels de protection d'accès, programmes de cryptage de réseaux, accès à distance authentifiés (p. ex. VPN);
- Installation de dispositifs de protection contre un accès physique non autorisé aux serveurs du système IT du preneur d'assurance (p. ex. local verrouillé);
- Gestion des correctifs et de mises à jour en vue de garantir que les correctifs et les mises à jour de sécurité des logiciels/systèmes concernés soient rapidement installés (en tenant compte de la compatibilité du correctif avec le logiciel installé);
- Mise en œuvre technique d'une password policy (politique de mots de passe) définie et de la gestion des autorisations;
- Cryptage de données numériques considérées comme sensibles selon les lois sur la protection des données en vigueur;
- Lors de transactions par cartes de crédit ou de débit, les règles des normes PCI-DSS doivent être observées;
- Avant l'utilisation, le preneur d'assurance prend les mesures nécessaires pour éviter les dommages dus à des surtensions risquant d'affecter les serveurs et les autres éléments d'infrastructure essentiels (routeurs, systèmes de sauvegarde, etc.). Ces mesures consistent notamment à protéger les prises électriques de dispositifs de protection contre les surtensions appropriés ou d'une alimentation sans interruption (ASI).