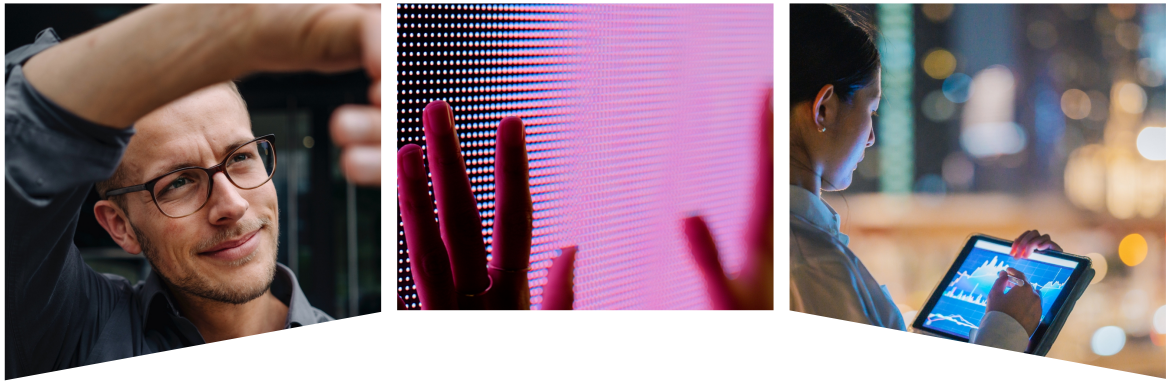




Numérisation

Cybercriminalité: *augmentation des attaques de ransomware*

17.10.2025

D'un coup d'oeil

Une vague d'attaques par ransomware orchestrée par un groupe de pirates informatiques déferle sur la Suisse. Les autorités fédérales tirent la sonnette d'alarme, d'autant plus que les attaques ciblant des entreprises sont en augmentation.

- Plus de 200 entreprises touchées depuis 2023, les dommages se chiffrent en millions
- On compte actuellement 4 ou 5 attaques par semaine, un triste record pour la Suisse
- Aucune entreprise n'est trop petite: les cybercriminels ciblent les failles

Les autorités fédérales tirent la sonnette d'alarme: un groupe de pirates informatiques intensifie actuellement ses activités en Suisse – les autorités enregistrent 4 ou 5 signalements relatifs à des attaques par semaine en ce moment. Jusqu'à présent, quelque 200 entreprises suisses ont déjà été victimes de ces attaques par ransomware. Les dommages s'élèvent à plusieurs millions de francs suisses – et à plusieurs centaines de millions au niveau mondial.

Protégez-vous: personne n'est trop petit ou trop grand pour se trouver dans le viseur

Cette mise en garde nous concerne toutes et tous. Les dernières évolutions montrent clairement qu'aucune entreprise n'est trop petite pour se trouver dans le viseur. Les cybercriminels ne font en effet pas de différence entre les grands groupes et les PME. Ils recherchent les points faibles – et les trouvent là où les mesures de protection font défaut ou sont inappropriées.

Depuis 2023, plus de 200 entreprises suisses, petites et grandes, ont été victimes de telles attaques. Les ransomware, aussi appelés rançongiciels, ne sont plus, depuis longtemps, un phénomène marginal. Une seule attaque peut paralyser l'ensemble des activités d'une entreprise en à peine quelques heures: interruptions de la production, perte de données critiques pour l'entreprise, mise en danger de la chaîne d'approvisionnement – les conséquences vont bien au-delà du domaine informatique. La cybercriminalité n'est donc pas seulement un risque technologique, mais également un risque commercial et stratégique à ne surtout pas négliger.

Il incombe aux entreprises de bien se préparer

Pour les milieux économiques, il est clair que la prévention commence dans l'entreprise elle-même. Une entreprise qui ne protège pas ses infrastructures numériques est exposée à des risques croissants. Il n'est pas nécessaire de disposer d'un service ad hoc pour prendre des mesures de base, mais il faut, en revanche, absolument une prise de conscience claire au niveau de la direction.

Les éléments essentiels de la cyber-résilience sont:

- l'entretien des systèmes et les mises à jour – des accès obsolètes sont l'une des portes d'entrée les plus fréquentes;
- des sauvegarde et des plans d'urgence – sauvegardés hors ligne, testés et accessibles en cas d'urgence;
- une authentification multi-factorielle – une mesure simple qui pourtant produit un grand effet;
- la sensibilisation des collaborateurs – l'humain reste souvent le maillon faible.

La cybercriminalité n'est pas un problème technologique: il incombe à la direction de s'en prémunir

Investir dans la sécurité numérique aujourd'hui permet de protéger demain les clients, les chaînes d'approvisionnement et la réputation de l'entreprise et, in fine, la place économique suisse dans son ensemble.

Pour de plus amples informations sur les incidents impliquant des ransomwares et sur la manière de se protéger, l'Association Suisse d'Assurances a publié un [guide destiné aux entreprises](#).

Pour de plus amples informations de la part de la Confédération, nous vous proposons ce [lien](#).



Angela Anthamatten

Responsable suppléante du Département Concurrence et Réglementation



David Stauffacher

Responsable de projet infrastructures et numérisation



Basile Dacorogna

Suppléant de la direction romande, Responsable de projet Concurrence et régulation

© economiesuisse | www.economiesuisse.ch