# Pourquoi faut-il une protection contre les ransomwares?

Personne n'est à l'abri des dangers des cybercriminels, pas même les PME. Infecté, données cryptées et victime de chantage, on ne peut plus accéder à ses données que contre une rançon.

**Thomas Liechti**
CEO de Mount10

Toute entreprise qui cède à un tel chantage finance les agissements des pirates. Payer une rançon est aussi utile que d'essayer d'éteindre un incendie avec de l'essence. Celui qui ne répond pas aux exigences doit toutefois s'attendre à perdre des données ou même à devoir lutter pour sa survie.

### Pourquoi aujourd'hui plus que hier?

La perte de données est aujourd'hui nettement plus grave qu'il y a dix ans. À l'époque déjà, il était possible de perdre ses données, que ce soit parce qu'on les avait effacées par erreur, que le disque dur présentait un défaut technique ou qu'une copie de sauvegarde n'était plus lisible. Comme on pouvait encore s'appuyer sur des processus analogiques ainsi que sur du papier et des classeurs, les pertes étaient la plupart du temps supportables. Avec la numérisation très avancée d'aujourd'hui, ce n'est toutefois plus le cas. Une attaque de virus est donc un événement très grave. «Aujourd'hui, une perte de données peut menacer l'existence d'une entreprise», avertit Thomas Liechti, CEO de Mount10.

### Que peuvent faire les entreprises?

Les dangers des virus ransomware pouvant être massivement endigués avec des moyens adéquats mais relativement simples, l'initiative «Swiss Cyber Defence – DNA» a été lancée. Il s'agit d'un guide simple comprenant six mesures que les entreprises peuvent appliquer seules ou avec l'aide de partenaires de mise en œuvre. Le catalogue de mesures est facile à comprendre et tient compte des domaines de responsabilité que sont l'organisation et la technologie.

### Qu'est-ce qui distingue ce guide des check-lists en ligne?

«Swiss Cyber Defence – DNA» renonce à exiger des entreprises qu'elles s'inscrivent pour avoir accès aux informations. L'initiative est entièrement à but non lucratif.

Les initiateurs sont également conscients que les entreprises souhaitent, le cas échéant, traiter le sujet à l'aide d'une check-list physique afin de conserver la vue d'ensemble nécessaire. C'est pourquoi les informations sur le site www.kmuschutz.ch sont entièrement transparentes.

Les partenaires de mise en œuvre mettent également à disposition les dépliants physiques.

Toutes les informations sont disponibles en allemand, français, italien et anglais. En cas de questions supplémentaires, les partenaires de mise en œuvre dans les régions sont à disposition.

L'initiative doit être bénéfique pour vous et votre entreprise, c'est ce que nous défendons au sein de l'organisme responsable. «Nous» signifie: Mount10, La Poste, Helvetia, Microsoft, Swisscom, HP, Cisco, Sophos, TrendMicro ainsi que l'entreprise de conseil atrete et le spécialiste de la sécurité informatique Compass Security.

Pour que les obstacles soient élevés pour les cybercriminels et que les entreprises soient moins vulnérables au chantage!