PROTECTION CONTRE LA FRAUDE ET LA CYBERCRIMINALITÉ

De plus en plus d'entreprises en Suisse sont menacées par la cybercriminalité et la piraterie informatique. Celles qui s'en remettent exclusivement à la sécurité de leur système informatique et aux logiciels antivirus risquent gros: les dommages causés par l'espionnage, le vol de données, le sabotage ou des maliciels ciblés peuvent se chiffrer en milliers, voire en millions de francs. Quant aux incidents relevant de l'ingénierie sociale, c'est-à-dire l'usurpation de l'identité d'un collaborateur ou d'un partenaire commercial afin de passer des transactions financières indues, ils sont de plus en plus courants. Même les collaborateurs abusent parfois de la confiance de l'employeur. Certains n'hésitent pas à commettre des fraudes ou des détournements, ou à manipuler des données.

LA SOLUTION POUR:

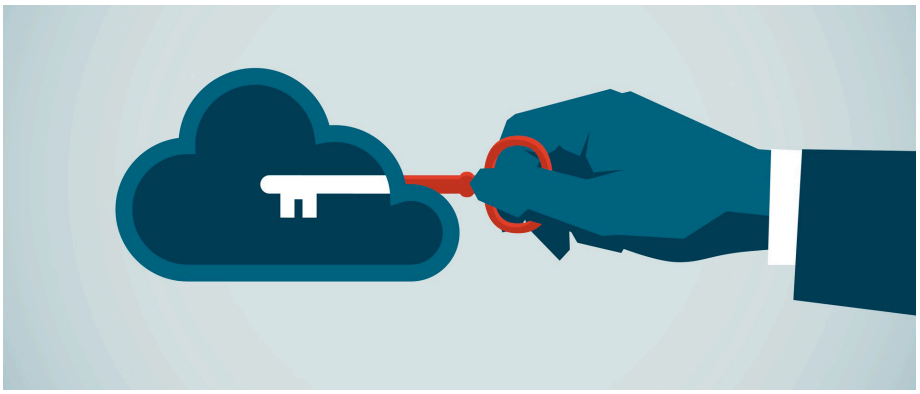
- Toutes les entreprises dont le personnel utilise Internet et les systèmes de données numériques.

POURQUOI UNE ASSURANCE POUR LES DOMMAGES D'ABUS DE CONFIANCE?

- **Compléter idéalement votre cyberassurance** en bénéficiant d'une couverture supplémentaire contre les actes de cybercriminalité et d'ingénierie sociale.
- Vous **protéger financièrement contre les dommages de piratage** et l'utilisation abusive de données.
- Vous **protéger contre les fraudes** de collaborateurs ou de tiers (fournisseurs externes de services informatiques, experts comptables, agents d'entretien).
- Vous **défendre en cas d'attaque d'ingénierie sociale:** hameçonnage, dévoiement, utilisation de logiciels espions.
- **Limiter durablement les risques commerciaux pour votre entreprise.**

VOS AVANTAGES

- **Protection contre les dommages de l'ingénierie sociale** (fraude liée à l'utilisation d'une fausse identité, comme l'«arnaque au faux président»).
- **Protection contre les dommages causés par les collaborateurs internes à l'entreprise,** le personnel étranger à l'entreprise, les intérimaires, ainsi que les avocats, les conseillers fiscaux et les experts-comptables qui travaillent pour votre entreprise.
- **Couverture contre les dommages de piratage** résultant d'intrusions dans vos systèmes informatiques.
- **Protection contre les dommages causés par des tiers** en cas de détroussement, de vol et d'escroquerie.



RISQUES ASSURÉS:

- **Pertes financières** découlant d'actes criminels commis par des personnes de confiance, p.ex. vol, fraude, abus de confiance, détournement de fonds ou dommage matériel, désignés par dommages résultant d'abus de confiance.
- **Dommages par usurpation d'identité,** tels que l'«arnaque au faux président» ou le détournement de flux financiers par des tiers se faisant passer pour des partenaires commerciaux («détournement de paiements»).
- **Dommages causés par des tiers** sous la forme d'un détroussement, d'un vol ou d'une escroquerie.
- **Dommages occasionnés par la divulgation de secrets** et peines contractuelles.
- Prise en charge destinée à **réduire les dommages de réputation.**
- **Couverture des peines contractuelles.**
- Prise en charge des frais internes et externes **d'évaluation du dommage et de poursuites judiciaires.**
- Protection contre les dommages découlant d'intrusions intentionnelles, illégales et ciblées de tiers dans votre système informatique, avec ou sans enrichissement (dommages de piratage).
- Protection contre les dommages découlant de l'obtention illégale et non autorisée et de l'utilisation frauduleuse de mots de passe et données d'accès, par hameçonnage, dévoiement ou par le biais d'un logiciel espion, d'un enregistreur de frappe ou d'autres moyens criminels.

FAQ

- **Je n'ai rien à reprocher à mes collaborateurs, pourquoi ne pourrais-je pas leur faire confiance?**
  De nombreuses entreprises font pleinement confiance à leurs collaborateurs. À juste titre, dans la majorité des cas. Mais les statistiques révèlent un tout autre tableau. Chaque année, les dommages liés aux infractions comme les abus de confiance et les escroqueries s'élèvent à plusieurs millions de francs. Bien souvent, ces actes sont le fait de collaborateurs qui se retrouvent dans des situations financières difficiles, qui veulent par exemple financer un train de vie dispendieux ou rembourser les dettes qu'ils ont contractées. Certains financent ainsi une addiction aux jeux. Sans que «l'occasion fait le larron».

- **Notre système informatique bénéficie des moyens de protection les plus avancés, qui réussirait à le pirater?**
  Les cybercriminels eux aussi mettent constamment à jour leur équipement et trouvent toujours de nouvelles façons de pirater les systèmes informatiques des entreprises. L'envoi ciblé d'e-mails d'hameçonnage (phishing) est une méthode particulièrement populaire. Les collaborateurs sont incités à communiquer leurs données utilisateur via un lien intégré dans l'e-mail, ce qui permet aux fraudeurs d'accéder à leur système informatique sans être dérangés. Même un système informatique doté des normes de sécurité les plus strictes ne se révèle pas d'une grande utilité dans ces cas.

- **Admettons que nous subissions un vol, nous pourrions nous en remettre, non?**
  Ici, il n'est pas question de petits délits comme le vol de matériel de bureau, mais du détournement de sommes pouvant atteindre plusieurs millions de francs, souvent pendant des années, comme les médias en relatent régulièrement. Et même lorsque l'on parvient à attraper le coupable, la plupart du temps l'argent s'est envolé. Par ailleurs, si un tel acte s'est produit dans votre entreprise et que vous ne le découvrez qu'après coup, la couverture rétroactive de la protection Euler Hermes contre la fraude vous garantit une protection optimale.

Euler Hermes Switzerland Richtiplatz 1 8304 Wallisellen T +41 44 283 65 65 info.ch@eulerhermes.com www.eulerhermes.ch
Office Lausanne Avenue Gratta-Paille 2 1018 Lausanne T +41 21 643 74 20
Office Lugano Via Antonio Adamini 10A 6900 Lugano T +41 91 922 73 64