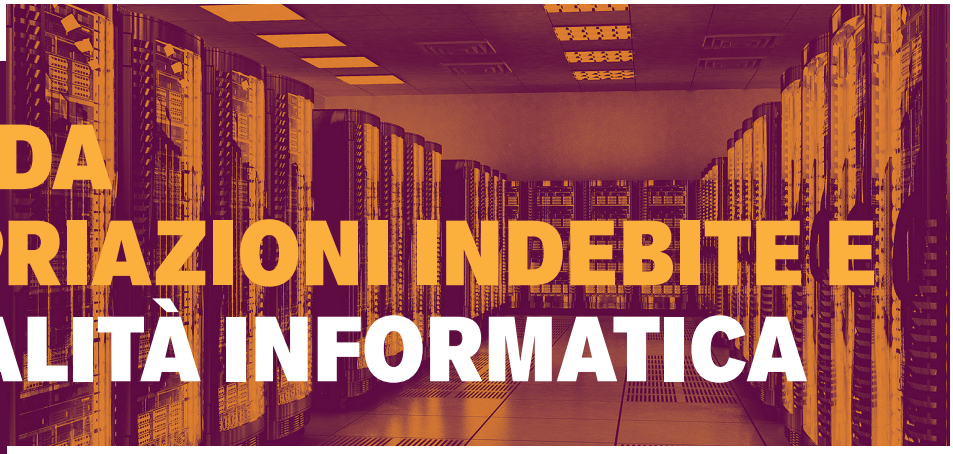


TUTELA DA APPROPRIAZIONI INDEBITE E CRIMINALITÀ INFORMATICA

Sempre più aziende in Svizzera sono minacciate da criminalità informatica e attacchi di hacker. Chi si affida solo alla sicurezza dei propri sistemi informatici e dei software antivirus può avere brutte sorprese: lo spionaggio o il furto di dati aziendali, il sabotaggio mirato o l'installazione dolosa di software dannosi possono avere infatti conseguenze pesanti in termini di costi. Gli attacchi di social engineering, come il furto d'identità di dipendenti o partner commerciali, per esempio, o la disposizione di operazioni finanziarie, sono sempre più diffusi. Anche la fiducia verso i propri collaboratori, a volte, può essere mal riposta: purtroppo non si può escludere la presenza di pecore nere tra i dipendenti o personale esterno, pronti a rovinare il datore di lavoro o il committente con frodi, appropriazioni indebite o manipolazione dei dati.

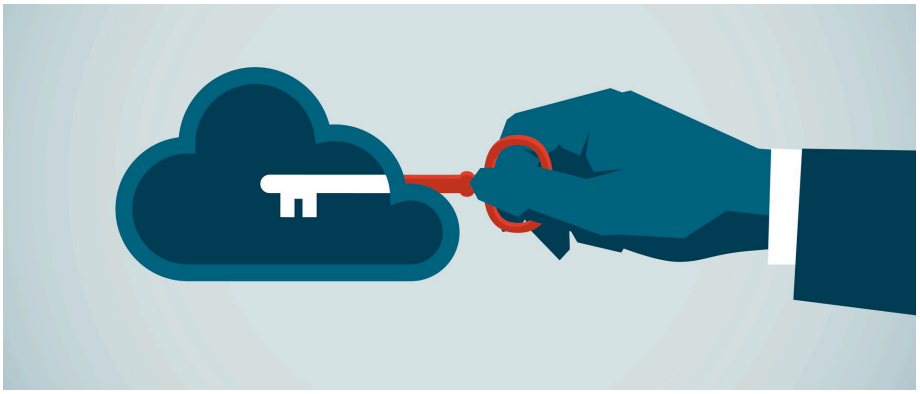
A CHI SI ADDICE LA SOLUZIONE:
Qualsiasi azienda con dipendenti che utilizzi sistemi informatici e Internet.

I MOTIVI PER STIPULARE UN'ASSICURAZIONE CONTRO I DANNI DA ABUSO DI FIDUCIA:

- **Riduzione del rischio di responsabilità personale** della direzione aziendale e del consiglio di amministrazione.
- **Integrazione ottimale di un'assicurazione cyber** per tutelarsi anche da criminalità informatica.
- **Tutela economica in caso di danni provocati da attacchi di hacker** e uso fraudolento di dati.
- **Protezione da appropriazione indebita** da parte di dipendenti o terzi (fornitori IT esterni, esperti contabili, personale addetto alle pulizie ecc.).
- **Protezione da attacchi di social engineering** tramite phishing, pharming e spyware.
- **Riduzione duratura del rischio d'impresa.**

VANTAGGI

- **Tutela dai danni causati dal social engineering** (frode mediante simulazione di un'identità falsa come ad es. «Fake President Fraud»).
- **Tutela dai danni causati da dipendenti,** personale esterno, collaboratori temporanei, avvocati, consulenti fiscali ed esperti contabili incaricati dall'impresa.
- **Protezione contro i danni causati da hacker** tramite attacchi ai sistemi informatici dell'azienda.
- **Tutela dai danni causati da terzi** in caso di rapina, furto e frode.



RISCHI ASSICURATI:

- **Perdite finanziarie** conseguenti ad attività criminali commesse da persone di fiducia tramite furto, infedeltà, frode, appropriazione indebita o danni materiali, ossia i cosiddetti danni da abuso di fiducia.
- **Danni da frodi commessi sotto falsa identità** (ad es. «Fake President Fraud») o la deviazione di flussi di pagamento da parte di terzi che si spacciano per partner commerciali («Payment Diversion»).
- **Danni causati da terzi** sotto forma di rapina, furto o frode.
- **Danni dovuti a violazione dell'obbligo di segretezza** e penali contrattuali.
- Assunzione dei costi per la **limitazione dei danni d'immagine.**
- **Copertura di penali contrattuali.**
- Assunzione dei costi interni ed esterni legati all'**accertamento dei danni e al procedimento giudiziario.**
- Tutela dai danni causati da attacchi intenzionali, illeciti e mirati di terzi ai sistemi informatici dell'azienda, con o senza scopo di arricchimento (danni da hacker).
- Tutela dai danni causati dall'utilizzo illecito e non autorizzato di password o dati di accesso ottenuti tramite pratiche di phishing, pharming, spyware, keylogger o altre tecniche criminali.

ANCORA DOMANDE? DI SEGUITO LE RISPOSTE AD ALCUNE DELLE DOMANDE PIÙ FREQUENTI:

- **Non permetto che si parli male del mio personale, perché non dovrei fidarmi?**
  Molti imprenditori si fidano ciecamente dei propri dipendenti, e nella maggior parte dei casi con ragione. I numeri, però, mostrano anche un'altra realtà. Ogni anno i reati collegati a infedeltà e frodi arrecano milioni di danni. Spesso le cause sono da ricondursi alle difficoltà economiche in cui incorrono i dipendenti, ad esempio per permettersi uno stile di vita costoso o estinguere i debiti contratti. Anche la dipendenza dal gioco può essere un fattore scatenante. Infine, non bisogna dimenticare che l'occasione fa l'uomo ladro.

- **Il nostro sistema informatico è protetto secondo i più rigidi standard di sicurezza, chi potrebbe attaccarlo?**
  Anche i criminali informatici si aggiornano e trovano sempre nuove tecniche per attaccare con successo i sistemi informatici delle aziende. Una delle tecniche preferite consiste nell'invio mirato di e-mail di phishing, che invitano l'ignaro collaboratore a cliccare su un link e ad inserire i suoi dati utente, con i quali i criminali informatici otterranno facile accesso al suo computer. Contro questi attacchi anche i più moderni sistemi di sicurezza possono fare poco.

- **Anche se qualcuno dovesse rubare qualcosa non sarebbe poi una perdita così grave, o no?**
  Il problema non riguarda la piccola criminalità come il furto di apparecchiature per ufficio ma l'appropriazione indebita di somme milionarie, che può continuare anche per anni, come si legge regolarmente sui giornali. E anche se si riesce ad identificare il colpevole, nella maggior parte dei casi è impossibile recuperare qualcosa perché i soldi sono già spariti. Inoltre, la copertura retroattiva illimitata della protezione di Euler Hermes contro l'appropriazione indebita protegge anche nel caso in cui l'impresa fosse già vittima di un simile caso senza saperlo.

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