

# CYBER-DIEBSTAHL VS. CYBER-BETRUG

## BEDEUTUNG UND UNTERSCHIED

Immer häufiger kommt es bei Netzwerksicherheitsverletzungen (z. B. ein Hacker-Angriff) zum Abfluss von Vermögenswerten. Im Klartext: Kriminelle verschaffen sich z.B. Zutritt zu Ihrem IT-System und überweisen sich selbst Geld (Cyber-Diebstahl) oder Ihre Mitarbeiter werden durch den Hacker derart getäuscht, dass sie eine Überweisung auf das Konto des Betrügers durchführen (Cyber-Betrug). Beide Risiken lassen sich über die Hiscox CyberClear Versicherung abdecken.

Der **Cyber-Diebstahl** – bereits in der Grunddeckung enthalten – sichert dabei den finanziellen Verlust durch Computer-Sabotage ab. Ein versicherter Schaden entsteht, wenn sich ein Krimineller ins IT-System des Unternehmens hackt, den Computer täuscht und sich dadurch selbst bereichert. Der Vermögensschaden entsteht unmittelbar durch die Kompromittierung des IT-Systems.

Beim **Cyber-Betrug** – optionaler Versicherungsbaustein – wird das IT-System des Unternehmens zur "Tatwaffe". Durch die Kompromittierung des IT-Systems wird ermöglicht, dass ein Mitarbeiter unmittelbar getäuscht wird und im guten Glauben unbewusst den Abfluss von Vermögenswerten herbeiführt. Der Vermögensschaden entsteht dabei nur mittelbar durch die Kompromittierung des IT-Systems.



## SCHADENFALL

Ein Krimineller hackt sich ins IT-System eines Versicherten und überweist sich selber Geld auf sein Konto.  
*Schadenhöhe oft mehrere zehntausend Euro.*

Ein Krimineller schaltet sich auf die Telefonanlage des Versicherten auf und routet seine Anrufe von dort auf teure Servicenummern oder ins Ausland.  
*Schaden durch erhöhte Telefonrechnungen regelmäßig € 5.000 - € 50.000.*

Ein Krimineller erlangt die Kontrolle über die Rechenleistung des versicherten IT-Systems und nutzt diese aus, um unbemerkt Kryptowährungen zu schürfen.  
*Schäden durch erhöhte Stromrechnungen oder erhöhte Nutzungsabrechnungen des Rechenzentrums führen schnell zu mehreren zehntausend Euro.*

Ein Krimineller verschafft sich Zugang zum Email-Account des Geschäftsführers, gibt sich gegenüber einem Mitarbeiter aus der Buchhaltung glaubhaft als dieser aus und weist eine hohe Summe wegen eines geheimen und dringenden Geschäfts an (Fake-President-Fall).  
*Schäden durch selbst angewiesene Überweisungen liegen häufig bei über € 10.000.*

Ein Krimineller hat Zugriff auf das IT-System eines Unternehmens und täuscht dadurch einen Mitarbeiter, sodass dieser die Kontodaten vom Rechnungssteller ändert und an ein falsches Konto bezahlt wird (Lieferantenbetrugsfall).  
*Schäden durch nicht bezahlte Rechnungen belaufen sich schnell auf fünfstelligen Eurobeträge.*

Ein Krimineller hat keinen Zugang zum IT-System des Unternehmens. Er täuscht einen Mitarbeiter in der Buchhaltung jedoch durch eine dem Unternehmen sehr ähnlich aussehende aber **externe Email-Adresse**. (Es handelt sich nicht um einen Hacker-Angriff auf das IT-System des Versicherten.)

Ein Krimineller hat Zugang auf das IT-System eines **Lieferanten** und manipuliert die Rechnung des Unternehmens oder den Zahlungsstrom so, dass nicht auf das Konto des Unternehmens, sondern auf das des Kriminellen gezahlt wird. (Es handelt sich nicht um einen Hacker-Angriff auf das IT-System des Versicherten.)

## MIT HISCOX CYBERCLEAR VERSICHERT?

✓ Ja, innerhalb von Cyber-Diebstahl versichert.

✓ Ja, innerhalb von Cyber-Diebstahl versichert.

✓ Ja, innerhalb von Cyber-Diebstahl versichert.

✓ Ja, innerhalb von Cyber-Betrug versichert.

✓ Ja, innerhalb von Cyber-Betrug versichert.

✗ Nein, nicht versichert, da keine Netzwerksicherheitsverletzung unmittelbar zur Täuschung geführt hat.

✗ Nein, nicht versichert, da keine Netzwerksicherheitsverletzung beim versicherten Unternehmen vorliegt.

Hiscox  
Arnulfstraße 31  
80636 München

Für Makler  
Tel.: +49 89 54 58 01 100  
hiscox.info@hiscox.de  
makler.hiscox.de

Für Endkunden  
Tel. +49 89 54 58 01 700  
myhiscox@hiscoxdirekt.de  
www.hiscox.de

