DAS PLUS AN DIGITALER SICHERHEIT.

Damit Sie im Schadensfall handlungsfähig bleiben.

IT-Sicherheit - für Risiken sensibilisieren:

Wie greifen Sie auf Ihre Kundendaten zu, wenn Ihre IT durch einen Cyber-Angriff blockiert ist?
Wie schützen Sie sich vor der Manipulation Ihrer Daten durch Dritte?
Wie viele befreundete Unternehmer kennen Sie, die bereits von einer Cyber-Attacke betroffen waren?

Cyberkriminalität

Cyber-Angriffe können weitreichende Folgen haben: Lahmgelegte Systeme können dazu führen, dass der Geschäftsbetrieb nur noch eingeschränkt fortgeführt werden kann oder zeitweise unterbrochen werden muss. Hinzu kommen Wettbewerbsnachteile durch den Verlust eigener sensibler Daten oder Reputationsschäden durch den Verlust von Kundendaten. Das Cyber-Risiko stellt eines der Top-3-Risiken für Unternehmen dar.

82.649 Fälle von Cybercrime im engeren Sinne (+80,5 %)

253.290 Fälle mit dem Tatmittel Internet unter allen in der PKS erfassten Straftaten (+3,6 %)

972 Fälle von Ransomware (+94,4 %)

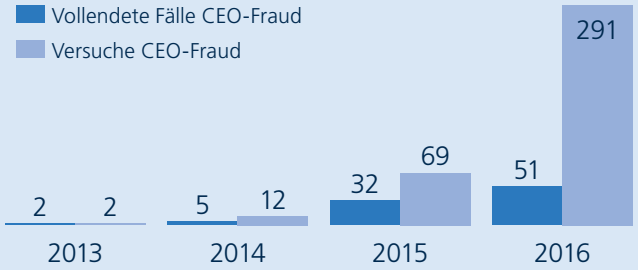
2.175 Fälle von Phishing im Onlinebanking (–51,4 %)

Quelle: Bundeskriminalamt, Cybercrime Bundeslagebild 2016

Wirtschaftskriminalität

Nicht nur Hacker bedrohen Unternehmen – auch kriminelle Dritte versuchen, unter anderem über das Internet, ihre Opfer zu manipulieren. Beim CEO-Fraud (auch Fake President Fraud genannt) nehmen die Täter Kontakt zu Mitarbeitern eines Unternehmens auf. Dabei geben sie sich beispielsweise als Geschäftsführer (CEO), leitender Angestellter oder Handelspartner des Unternehmens aus. Ziel der Kontaktaufnahme ist der Transfer eines größeren Geldbetrages ins Ausland.

Fallentwicklung CEO-Fraud



Quelle: Bundeskriminalamt, Sondererhebung

Geschäftsführerhaftung

IT-Sicherheit ist immer Chefsache!

Die Unternehmensleitung hat die Pflicht, geeignete Maßnahmen zu treffen, um den Fortbestand des Unternehmens sicherzustellen. Hierzu zählt beispielsweise die Einrichtung von Überwachungssystemen zu einer frühzeitigen Risikoerkennung.

Wer als Geschäftsführer keine geeigneten Mittel zur Gefahrenabwehr veranlasst, handelt grob fahrlässig und steht damit gegenüber dem eigenen Unternehmen und Dritten in der Haftung.

Die Einrichtung geeigneter Schutzmaßnahmen ist für den Fortbestand eines Unternehmens essenziell. Deshalb wirft der Eintritt eines IT-Schadens stets die Frage nach einem Organisations- oder Überwachungsverschulden seitens der Geschäftsleitung auf.

Ihre Ansprechpartner in der Volksbank Gronau-Ahaus eG:

Andreas Huesmann, R+V Firmenkundenberater Tel. 02561 / 696-828
Frank Nienhues, R+V Firmenkundenberater Tel. 02562 / 914-122
Corina Rotterdam. R+V Vertriebsassistenz Tel. 02562 / 914-283

R+V DIE VERSICHERUNG MIT DEM PLUS.

DAS PLUS AN DIGITALER SICHERHEIT.

Damit Sie im Schadensfall handlungsfähig bleiben.

CyberRisk Versicherung

> **„echte Schadenbehebung“** über eine **Direktverbindung** des Versicherungsnehmers mit unserem **Dienstleister** (nicht nur Vermittlung eines Dienstleisters oder Erstattung von Kosten) – **24 Std. / 7 Tage die Woche.**

> grundsätzlich Ersatz von **Betriebsunterbrechungsschäden** ohne Sublimit

> Übernahme der Kosten der **Wiederherstellung von Daten und Programmen**

> Deckung bei **internen und externen Handelnden**

> **„Bring your own Device“:** Versicherung von Unternehmensdaten auf dienstlich genutzten Privatgeräten

Versicherung gegen Wirtschaftskriminalität

> Schutz vor den Folgen zunehmender **Wirtschaftskriminalität** im Rahmen der Internet- und WirtschaftskriminalitätsPolice

- aufgrund **interner** Straftaten (Diebstahl, Untreue, Unterschlagung) oder
- **externer** Straftaten von Dritten, z. B. durch
  - Vorspiegelung einer falschen Identität (Fake President)
  - Nutzung einer fremden Identität (Fake Identity) oder
  - Umleitung von Zahlungsströmen (Payment Diversion)

> Absicherung von finanziellen Folgen wissentlicher Pflichtverletzungen Ihrer Mitarbeiter

D&O-Versicherung

> Absicherung der Geschäftsleitung, u. a. bei **organisatorischen Mängeln,** bei **Lücken in der Überwachung** des Geschäftsbetriebs oder der **Auswahl ungeeigneter Mitarbeiter,** z. B. durch

- unzureichende Regelungen bei der Vergabe von Administrator- und Zugriffsrechten, beim Passwortschutz oder der Datensicherung
- nicht vorhandene Vorkehrungen gegen **menschliches Fehlverhalten** (Übertragung falscher/geheimer Daten etc.), z. B. durch 4-Augen-Prinzip
- fehlenden Schutz gegen **technisches Versagen** (Notstromversorgung, redundante Systeme, Versicherungen etc.)

> Abwehrschutz bei **Vorsatz**vorwurf, z. B. Verstößen gegen Datenschutzvorschriften

> Unbegrenzte Rückwärtsdeckung

R+V DIE VERSICHERUNG MIT DEM PLUS.

00 234 70 0436 001 0 02.18