
**Die Liste möglicher Schadsoftware (Malware) ist lang:**

### Cyber-Vertrauensschaden

Der Mitarbeiter eines Unternehmens hat Zugang zu mehreren Konten seines Arbeitgebers. Dies nutzt er aus, um sich über einen längeren Zeitraum kleine Beträge auf sein Privatkonto zu überweisen. Der über ein Jahr entstandene Schaden beträgt insgesamt 34.000 €.

### Cyber-Haftpflicht

Ein Online-Buchhändler stellt kostenlose Leseproben zum Download zur Verfügung. Trotz aller Sicherheitsmaßnahmen wird eine infizierte Datei zum Download angeboten. Die IT-Systeme mehrerer Kunden werden dadurch infiziert. Der entstandene Gesamtschaden beläuft sich auf 40.000 €.

## Haben wir Ihr Interesse geweckt?

Gerne stehen wir Ihnen zur Analyse Ihres individuellen Bedarfs zur Verfügung und finden mit Ihnen gemeinsam aus einer Vielzahl von Produktlösungen und Anbietern, die passende Absicherung für Ihr Unternehmen – sprechen Sie uns an!

LEDERBAUER GmbH & Co. KG
MAKLER FÜR FINANZEN + VERSICHERUNGEN

Marktler Str. 1 d · 84489 Burghausen
Telefon 08677 2362 · Makler@Lederbauer.de
www.Lederbauer.de

Stand: 12/2021

QUALITÄTSURTEIL Maklerverbund 01/2021 exzellent

vfm wurde von ASSEKURATA im Maklerverbund-Rating mit der Bestnote „exzellent“ beurteilt.

vfm® Versicherungs- & Finanzmanagement

LEDERBAUER GmbH & Co. KG
MAKLER FÜR FINANZEN + VERSICHERUNGEN

# Cyber-Versicherung

Schützen Sie Ihr Unternehmen vor den Folgen von Cyberattacken und Virenangriffen

Partner im vfm-Verbund

vfm® Versicherungs- & Finanzmanagement

## Schadenbeispiele

Als Unternehmen können Sie von Cyber-Risiken wie Hacker-Angriffen, Cyber-Einbrüchen oder Infektionen mit Viren bedroht werden. Gefährdet werden dadurch sowohl Ihre IT-Systeme (Computer, Server, Netzwerke, Mobiltelefone, Tablets, Videokonferenzsysteme, Datenleitungen und Intra-und Extranets) und Programme (Betriebssysteme, Datenbanken und Verwaltungssoftware) als auch Ihre elektronischen Daten (z. B. Auftragsdaten, Kundendaten, Personendaten).

### Cyber-Eigenschaden

Der Mitarbeiter einer Steuerkanzlei öffnet den Anhang einer E-Mail, welcher einen Verschlüsselungstrojaner beinhaltet. Alle Daten auf den Systemen der Kanzlei werden somit unlesbar gemacht. Die Kosten für die IT-Forensik sowie die Entfernung der Schadsoftware und Installation neuer Sicherheitssoftware betragen 28.000 €.

### Cyber-Betriebsunterbrechung

Ein Unternehmen wird mit einer Denial-of-Service-Attacke (DDOS) angegriffen. Die Plattform und alle damit verbundenen Dienste sind zwei Tage für Kunden nicht erreichbar. Die Kosten für die Anmietung zusätzlicher Serverkapazitäten sowie die Kosten der Betriebsunterbrechung und Wiederherstellung der ursprünglichen Homepage belaufen sich auf 75.000 €.

### Cyber-Forderung

Ein Hacker verschafft sich Zugriff auf die IT-Systeme eines Rechtsanwaltkanzlei und verschlüsselt wichtige Mandanten-Daten. Kurze Zeit später erhält der Jurist eine E-Mail mit der Forderung, den Betrag in Höhe von 5.000 € in Form von Bitcoins zu zahlen.

### Cyber-Zahlungsmittelschaden

Ein Online-Shop wird Opfer eines Hackerangriffes. Der Hacker hat sich eine „Backdoor“ installiert, mit welcher er sich Zugang zu Kreditkartendaten der Plattform verschafft. Dies wird bekannt und die Kreditkartenhersteller müssen alle Kreditkarten austauschen. Die Kosten für den Austausch belaufen sich auf 250.000 €.


## Schutz vor Cyberrisiken

Digitale Risiken wie Hackerangriffe und Datenverluste sind allgegenwärtig und unabhängig von der Größe des Unternehmens kann jeder davon betroffen sein. Wie umfangreich drohende Folgen sein können ist vielen nicht bewusst. Für kleine und mittelständische Unternehmen kann es überlebenswichtig sein, ein funktionierendes Cyber Risk Management zur Absicherung zu haben.


Fast jeder Betrieb hat eine Anbindung an das Internet und setzt sich dadurch den Cyber-Risiken aus. Je mehr Wertschöpfung Sie im Internet generieren, um so höher ist die Gefahr für Ihren Betrieb (Online-Shops, Internetportale). Kein IT-Dienstleister kann für ein 100 % sichereres Netzwerk garantieren. Jeden Monat kommen etwa 1.000.000 neue Schadprogramme wie Viren und Trojaner hinzu. Ein häufig unterschätztes Cyber-Risiko sind Mitarbeiter: sie öffnen infizierte E-Mail-Anhänge, benutzen zu einfache Passwörter oder vergessen sich vom System abzumelden.

## Stellen Sie sich bitte folgende Fragen:

- Wer trägt die Kosten, wenn Ihr Unternehmen Opfer eines Hackerangriffs wird?
- Wissen Sie, wer bei Datenrechtsverletzungen durch Datenverlust haftet und den entstandenen Schaden bezahlt?
- Wie handeln Sie, wenn Ihr Unternehmen nach Datenverlust erpresst wird?
- Wer sichert Sie ab, wenn z. B. Internetseiten vorübergehend offline sind und Sie finanzielle Einbußen haben?

## Die Fakten

- Die Zahl der Schadprogramme ist in 2016 auf knapp über 500 Mio. Viren, Trojaner und sonstige Malware gestiegen
- E-Mails mit Viren-Anhängen haben von 2014 auf 2015 um 36 % zugenommen
- Es gab 32.000 DDoS-Hacker-Angriffe (Denial-of-Service-Attacke)
- Über 60.000 Cyber-Straftaten wurden begangen

## Das deckt eine Cyber-Versicherung ab

### EIGENSCHÄDEN

**Risiko:** **Wirtschaftliche Schäden durch Betriebsunterbrechung**

**Regulierung:** **Zahlung eines Tagessatzes**

**Risiko:** **Kosten der Datenwiederherstellung und System-Rekonstruktion**

**Regulierung:** **Übernahme der Kosten**

### DRITTSCHÄDEN

**Schadensersatzforderungen von Kunden wegen Datenmissbrauch und/oder Lieferverzug**

**Regulierung:** **Entschädigung berechtigter und Abwehr unberechtigter Forderungen**

### SERVICE-LEISTUNGEN

**Risiko:** **IT-Forensik-Experten zur Analyse, Beweissicherung und Schadenbegrenzung**

**Risiko:** **Anwälte für IT- und Datenschutzrecht zur Erfüllung der Informationspflichten**

**Risiko:** **PR-Spezialisten für Krisenkommunikation zur Eindämmung des Imageschadens**

**Regulierung:** **Jeweils Übernahme von Service & Kosten**

## Sichern Sie sich daher gegen diese drei Hauptrisiken ab

### Cyber-Angriff

Hierunter versteht man einen unbefugten Hacker-Angriff Dritter mit dem Ziel, Ihre Systeme zu unterbrechen oder zu blockieren. Hierzu belasten Hacker meist Internetleitungen oder die Server durch eine Vielzahl von Anfragen, die dann zum Absturz oder Blackout der Systeme führen.

### Cyber-Eingriff

Darunter versteht man einen unbefugten Hacker-Eingriff Dritter um Daten oder Programme zu stehlen, zu verändern, zu blockieren oder zu zerstören. Der Hacker sucht eine Schwachstelle in Ihrem System, z. B. eine ungeschützte oder offene Netzwerkverbindung, um z. B. mit einem Trojaner dort anzugreifen. So kann er Daten absaugen, verändern oder verschlüsseln.

### Cyber-Infektionen mit Schadsoftware

Der Angreifer infiziert Ihre IT-Systeme mit Schadsoftware, insbesondere Viren und Trojaner. Hierdurch werden Cyber-Eingriffe auf die eigenen IT Systeme (Trojaner) oder auch Cyber-Angriffe auf Dritte durch die eigenen IT Systeme (kompromittierte IT Systeme) ermöglicht. Viele Infektionen führen zu Straftaten, manche sind jedoch willkürlich, um einfach nur Schaden zu verursachen.