
# Entscheider-News zur Cyber-Versicherung

**Das Thema Cyber-Risiken ist gerade auf allen Ebenen präsent. Aber was bedeutet es für Sie als Leitungskraft und Ihre Unternehmung? Wir wollen Ihnen mit dieser Entscheider-News einen Einblick geben, in die Chancen und Hürden einer Cyber-Versicherung.**

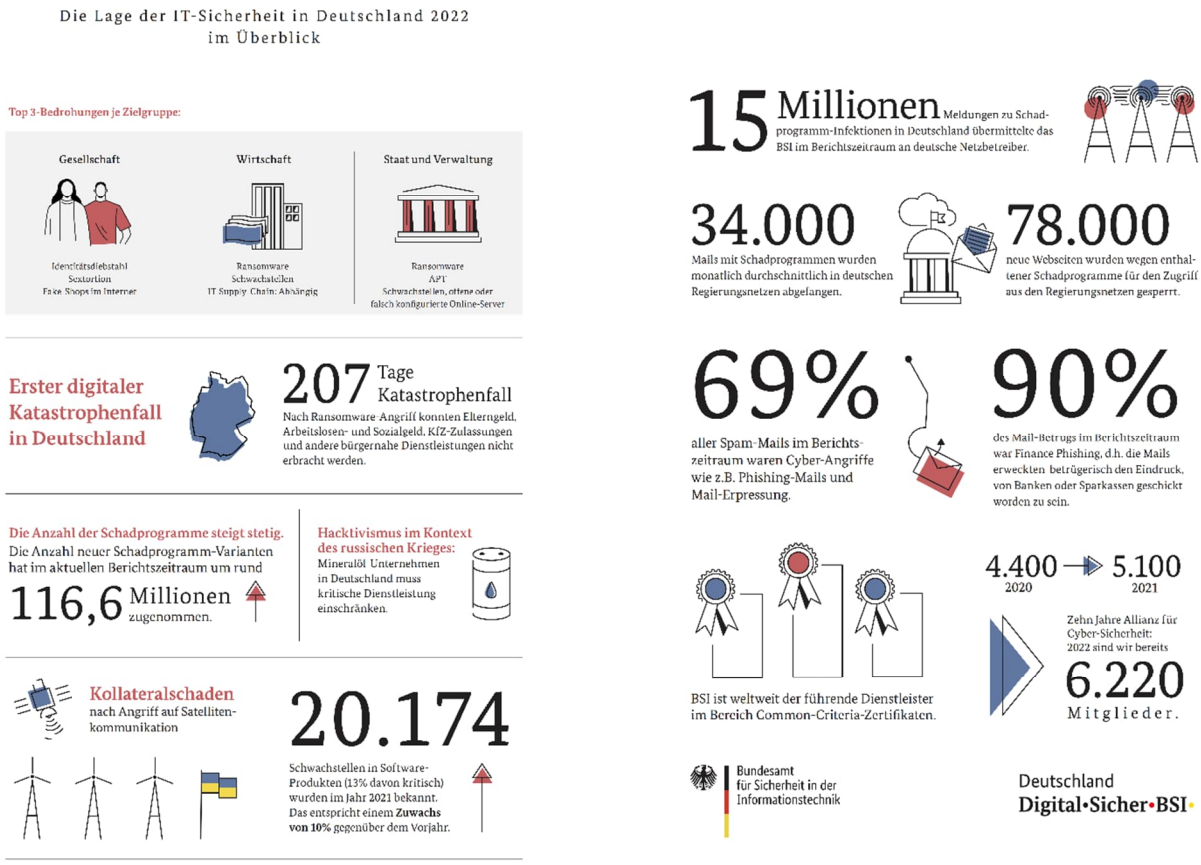
## Was Sie als Unternehmen über Cyber-Sicherheit im Jahr 2023 wissen sollten.

Eine Unternehmung ohne digitale Prozesse, CRM-Systeme oder vernetze Maschinen ist kaum noch vorstellbar. Wo der Fortschritt in den letzten Jahren eine schnelle Entwicklung und Digitalisierung gefördert hat, dort sind leider auch Prozesse zum sicheren Umgang mit den neuen Technologien auf der Strecke geblieben. Viele Unternehmen nutzen vernetzte Systeme und das Internet, aber sind nur rudimentär gegen die neuen Gefahren der Technologie geschützt. Häufig fehlt es am Verständnis oder an der Expertise. Dies gilt jedoch nicht für die neuen Generation von Kriminellen, welche anstatt mit einem Brecheisen mit einer Phishing-E-Mail Ihr Unternehmen angreifen, um nur eine der bekanntesten Arten zu nennen.

### Die aktuelle Bedrohungslage in aller Kürze!

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) geht bereits seit vielen Monaten von einer „erhöhten Bedrohungslage“ aus. Tatsächlich werden im Moment so viele System-Angriffe wie noch nie registriert. Die Anzahl der erfolgreichen Angriffe auf IT-Systeme, von denen die Medien berichten, ist kaum mehr überschaubar. Hierzu gehören bekannte Unternehmen wie PayPal, Sky Deutschland, die Industrie- und Handelskammer (IHK), die Universität Duisburg, diverse Stadtverwaltungen und Energieversorger. Diese Liste wird täglich umfangreicher und ist sicher noch

lange nicht abgeschlossen. Besonders die Auswahl der bekannten Ziele zeigt, dass die IT-Infrastruktur anfällig ist. Auffällig ist, dass die Wiederinstandsetzung von Systemen nach einem Cyber-Angriff keine Frage von Tagen ist, sondern ggf. Monate dauert. Als bekanntestes Beispiel mag hier die IHK dienen. Diese wurde am 03.08.2022 Ziel einer starken Cyber-Attacke. Zwar trennte die IHK sehr schnell betroffene System vom Netz, aber auf der Seite der IHK berichtete die IHK noch im Dezember, dass die IT-Struktur nur schrittweise wieder in Betrieb genommen werden kann. Ein großes Unternehmen in Deutschland war für mehrere Wochen nur eingeschränkt handlungsfähig.




## Das sagt der Gesetzgeber!

Aus den Reihen der Gesetzgebung gab es bereits vor der DSGVO deutliche Aussagen zum Thema der Datensicherheit in Unternehmen. Hat der Gesetzgeber viele Jahre das Thema des vertraulichen Umgangs mit Daten nur begrenzt reguliert, ist dies seit der DSGVO in den Fokus gerückt.

Im Rahmen seiner Abhandlung zum Thema Cyber-Versicherung führt Prof. Dr. Michael Fortmann aus, dass die Nichtbeschäftigung mit dem Thema Datenrisiken eine Pflichtverletzung der Geschäftsführung darstellen kann. Dies umfasst darüber hinaus auch die mangelnde laufende Überwachung, fehlerhafte Entscheidungen im Rahmen der Business Judgment Rule (BJR) und die mangelnde Qualifizierung von Mitarbeitern und IT-Sicherheit. Quelle: R+S 2019/668

Diese Haftung ist in Deutschland nicht in einem zentralen Gesetz geregelt, sondern verteilt sich über viele verschiedene Regelwerke und ist daher schwer zu definieren. Für die Verarbeitung von Daten hat die Datenschutzgrundverordnung, gemäß Art. 5 Abs. 1 f) DSGVO eine zentrale Bedeutung. Gemäß DSGVO müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der Daten gewährleistet. Dazu sind geeignete technische und organisatorische Maßnahmen zu treffen, um ein angemessenes Schutzniveau herzustellen.

Nach der Einführung der DSGVO sind Datenschutzpannen zu einem erheblichen Kostenfaktor für Unternehmen geworden. Die Strafen liegen bei bis zu 4 % des Jahresumsatzes der Unternehmung. Im Durchschnitt liegt die Strafe bei einem mittelständischen Unternehmen bei 20.000 bis 100.000 Euro. Hier sind noch nicht etwaige Reputationsschäden und Wiederherstellung der IT-Struktur beinhaltet.

## Risikofaktoren in der IT-Sicherheit

Der größte Risikofaktor für die Datensicherheit in einem Unternehmen ist der Mensch. Hier wollen wir noch nicht einmal von der Vielzahl unzufriedener Mitarbeiter sprechen, welche Daten zum Mitbewerber transferieren oder für eigene Zwecke missbrauchen. Die Mitarbeitenden sind immer noch das größte Sicherheitsrisiko für jedes Unternehmen. Gezielt und geschult richten sich Cyber-Angriffe durch Phishing-E-Mails, manipulierte Anrufe und Dokumente an den Faktor Mensch. Hinzu kommen benutzerfreundliche, aber schwache Passwortregelungen und technische Lücken in der genutzten Software.

Viele dieser Faktoren lassen sich durch regelmäßige Schulungen, starke Sicherheitskonzepte für Passwörter, im Umgang mit privater und beruflicher Hardware und einen vertrauensvollen Umgang stark abmindern. Dies bedeutet aber die Auseinandersetzung mit diesen Themen und zu Anfang auch den Verlust gefühlter Komfortzonen beim täglichen Umgang mit den Systemen.

Wichtige Maßnahmen zum Schutz Ihres Unternehmens können daher sein:

- IT-Sicherheitsprüfung
- Schulung der Mitarbeitenden und die Sensibilisierung der Mitarbeitenden
- Regelmäßiges Anlegen von Backups
- Regelmäßiges Update der Firewall und Endgeräte-Schutz
- eine aktuelle Antivirus-Software
- Multi-Faktor-Authentifizierung und eine Passwort-Hygiene
- Regelmäßige Software-Updates
- Finanzielle Absicherung gegenüber Cyberrisiken

Die IT-Systeme und Abläufe im Unternehmen sollten, genauso wie die Feuerlöscher, regelmäßig überprüft werden. Analog zu den Brandschutzplänen sollte ein Unternehmen, unabhängig von der Größe, einen Notfall-Plan erarbeiten, um im Falle von Störungen schnell und sicher zu handeln. Besonders bei kleinen und mittelständigen Unternehmen sind diese Präventionsbausteine und Notfall-Pläne die Brücke zur Cyber-Versicherung. Diese bietet in der Vielzahl der Produkte diese Dienstleistung an. Dadurch erhalten Unternehmen ohne eigene IT-Abteilung und große Dienstleister den Zugang zu einer hochwertigen Unterstützung und Schadenminderung.

## Die Cyber-Versicherung als Bestandteil Ihrer IT-Sicherheit

Existenzbedrohende Risiken bedürfen hohen Rücklagen oder einer Versicherungslösung. Durch eine Versicherungslösung erhalten Unternehmen die Möglichkeit mit kalkulierbaren Kosten diese Risiken abzusichern oder abzumildern. Dies gilt besonders für die Absicherung durch eine Cyber-Versicherung, welche neben der Übernahme der Kosten im Schadenfall auch noch präventive Bausteine umfasst. Dadurch können auch die Kosten für IT-Dienstleitung optimiert werden.

## Bausteine einer Cyber-Versicherung

Die Produkte der Gesellschaften unterscheiden sich stark im Umfang der Leistungsbausteine, welche neben den Versicherungssummen und Selbstbehalten den Grundstein für die Cyber-Versicherung darstellen. Die nachfolgende Auflistung fasst die gängigsten Bausteine zusammen.

### Prävention

**Die aktiven Präventionsbausteine sind eine neue Art der Versicherungsleistung. Damit soll bereits im Vorfeld Umfang nach einem Schadeneintritt vermindert oder der Schadenfall abgemildert werden. Für das Unternehmen bedeutet es den Zugang zu hochwertigen Dienstleistern und Lösungen für die eigene IT-Sicherheit.**

- Erstellung eines Notfallplans und Überprüfung der vorhandenen Systeme gemeinsam mit der Versicherung
- Mitarbeiterschulung und Sensibilisierung für Angriffe und Abläufe durch die Versicherung
- umfassendes IT-Sicherheitsdienstleisternetz mit vergünstigten Konditionen
- Erstellung von rechtsicheren Vorlagen zur Auftragsdatenverabeitung und Datenschutzerklärung

## Deckung für Eigenschäden

**Die Eigenschadendeckung stellt, wie auch in der klassischen Feuerversicherung, den bekanntesten Baustein der Cyber-Versicherung da. Diese erstattet dem Unternehmen die Mehrkosten bei einem versicherten Schadenfall.**

- Erstattung von Kosten für Krisenmanagement, IT-Forensik oder begleitende PR-Maßnahmen
- Unterstützung durch externe IT-Spezialisten für die Abwehr und Behandlung von Cyber-Angriffen
- Unterstützung bei der Wiederherstellung der IT-Systeme des Kunden und Übernahme von Wiederherstellungskosten
- Zahlung von Betriebsunterbrechungsschäden bei System- und Cloud-Ausfall

## Schadenersatz und juristische Unterstützung

**Gerade im Schadenfall ist die rechtssichere Kommunikation mit den Behörden, Kunden und Partnern ein wichtiger Baustein, um weiteren Schaden vom Unternehmen abzuwenden. Hier stellt die Cyber-Versicherung dem Kunden spezialisierte Anwälte an die Seite, welche diese Aufgabe übernehmen.**

- Prüfung, Abwehr und Ausgleich von Schadenersatzansprüchen von Geschädigten
- Kommunikation mit Behörden und Anwälten
- Vertragsstrafen an E-Payment Service Provider
- Vertragsstrafen wegen der Verletzung von Geheimhaltungspflichten
- Bußgelder und Entschädigungen mit Strafcharakter im Ausland

## Reduzierung von Reputationsschäden

Im Schadenfall muss der Kunde über etwaige Datenverluste informiert werden. Dies sollte mit viel Fingerspitzengefühl passieren. Hierzu bieten die Cyber-Versicherung einen Baustein an, welcher diese Kosten übernimmt. Hierzu gehört die Einrichtung von Hotlines und die Beauftragung von Experten.

- Kosten für Krisenmanagement- und Public-Relations-Maßnahmen (etwa IT-Experten und PR-Berater)
- Erstattung der Kosten für gesetzliche Benachrichtigungspflicht des Dateninhabers

# Deckungssummen und Selbstbehalte

Neben der Auswahl der Bausteine ist die Auswahl der Deckungssummen und Selbstbehalte ein wichtiger Faktor.

### Deckungssummen

Die Cyber-Versicherung leistet nur bis zur ausgewählten Deckungssumme, ungeachtet vom tatsächlichen Schaden. Daher ist die Auswahl der Deckungssumme ein wichtiger Schritt und ist abhängig von vielen Faktoren wie zum Beispiel der Art des Unternehmens, der Anzahl gespeicherter Datensätze und der Komplexität der IT-Struktur. Die Ermittlung der Deckungssumme wird dadurch erschwert, dass die Erfahrungswerte fehlen. Um Ihnen hier eine Hilfestellung zu leisten, bedienen wir uns verschiedener Datenbanken und Softwarelösungen.

### Selbstbehalte und Eigenbeteiligung

Um den Versicherungsbeitrag zu reduzieren, gibt es die Möglichkeit verschiedene Selbstbehalte und Karenzzeiten zu vereinbaren. Dies bedeutet, bei einer Anpassung an das Unternehmen, keine merkliche Einschränkung, aber es kann eine deutliche Reduzierung der Beitragssumme bedeuten.

# Die Möglichkeiten und Grenzen einer Versicherungslösung

Eine Cyber-Versicherung ist zusammen mit einem guten IT-Konzept eine gute Grundlage, um Schäden abzuwehren und im Schadenfall die Situation beherrschbar zu halten. Entgegen den etablierten Produkten im Bereich der Sachversicherung unterliegt die Cyber-Versicherung noch einer starken Dynamik. Dies bedeutet, dass der Bedarf und die Angebote der Gesellschaften, auch nach einem Abschluss, jedes Jahr überprüft werden sollten.

Besonders im Bereich der Deckungssummen sind einige Gesellschaften noch zurückhaltend, da bisher noch keine ausreichenden Erfahrungswerte vorliegen. Daher erhalten Sie vielleicht im Moment nur mit viel Aufwand eine ausreichende Absicherung für Ihr Unternehmen oder müssen ggf. noch eigene Rückstellungen bilden. Deshalb ist es wichtig entsprechende Angebote bei einer Vielzahl von Gesellschaften anzufragen und auch nachzuverhandeln.

Grundlegend gilt festzuhalten, dass die Cyber-Versicherung Ihr Unternehmen vor einer existenzbedrohenden Lage bewahren kann. Jedoch ist im Vorfeld die Mitwirkungspflicht zu beachten, damit die Cyber-Versicherung im Schadenfall auch eintritt.

# Handlungsempfehlung

Die Handlungsempfehlung zum Cyber-Risk-Konzept kann man in drei Schritte einteilen. Diese sind die Risiken erkennen, Maßnahmen ergreifen und existenzbedrohende Risiken versichern.

## ➢ Risiken erkennen

Prävention beginnt mit der Erfassung und Bewertung von Risiken. Nur wer weiß, welche IT-Systeme im Unternehmen im Einsatz sind, welche Software sich auf diesen Geräten befindet und wie sie aktuell gehalten wird, mit welchen Daten im Unternehmen umgegangen wird, kann geeignete technische Schutz-Maßnahmen ergreifen und die notwendigen Regeln definieren.

Weitere potenzielle Angriffsziele gilt es zu verstehen und zu bewerten, wie z.B. den Themenkomplex Zahlungsmittel und Konten, aber auch die Online-Präsenz des Unternehmens und einzelner Personen. Das sich so ergebende Risikobild vor Augen, gilt es technische und organisatorische Maßnahmen abzuleiten und zu implementieren.

## ➢ Maßnahmen ergreifen

Es lassen sich im Wesentlichen zwei Kategorien von Schutz-Maßnahmen bei Cyber-Risk unterscheiden. Dabei handelt es sich einerseits um technische, andererseits um organisatorische Maßnahmen. Es gibt Standards und Richtlinien, die bei der Definition geeigneter Maßnahmen helfen, wie z.B. der BSI-Standard (IT-Grundschutz) oder etwa die Norm ISO/IEC 27001.

**Technische Maßnahmen**

Die Bandbreite denkbarer geeigneter technischer Maßnahmen ist erheblich. Diese reicht von dem rein physischen Schutz der Geräte vor unbefugtem Zugriff, über das Installieren von Schutz-Software und -Systemen, bis hin zum Einsatz von Daten-Verschlüsselung und von Sicherheitskopien (Backups), die von dem Hauptsystem getrennt aufbewahrt werden.

Unter Schutz-Software und -Systemen kann man sich beispielsweise Firewalls und Paketfilter, Malware-Schutz, aber auch eine Zwei-Faktor-Authentifizierung vorstellen.

**Organisatorische Maßnahmen**

Wie für viele andere Lebensbereiche auch, gilt insbesondere für Cyber-Risk, dass der Faktor Mensch eine ganz entscheidende Rolle spielt. Eine Vielzahl von Schadenbildern belegt, dass selbst bei einem aufwändigem technischen Schutzstandard immer wieder menschliches Verhalten für einen erfolgreichen Angriff auf IT-Systeme ausschlaggebend ist. Darum ist es unabdingbar, dass ein Unternehmen Regeln aufstellt für die Verantwortlichkeit für IT-Systeme sowie den Umgang mit ihnen.

Regeln allein lösen das Problem aber nicht. Es ist notwendig, dass Mitarbeiter regelmäßig geschult und die Einhaltung der Regeln überwacht werden.

- **existenzbedrohende Risiken versichern**

Das Verstehen von Cyber-Risiken und das Ergreifen geeigneter Maßnahmen ist die eine, das Versichern verbleibender Risken die andere Seite der gleichen Medaille. Die Eintrittswahrscheinlichkeit eines Cyber-Schadens lässt sich durch technische und organisatorische Maßnahmen positiv beeinflussen, ausschalten lässt sie sich nicht. Um die verbleibenden Risiken geht es bei der Cyber-Versicherung, die eingetretene Schäden zu beheben hilft und die wirtschaftlichen Folgen aus diesen Schäden trägt.

## Fazit zur Handlungsempfehlung


Die Bedrohungslage durch Cyber-Angriffe ist allgegenwärtig. Die Absicherung der eigenen IT-Systeme ist alternativlos. Diese zwei Fakten sind sicher nicht diskutabel. Die Lösung, die Cyber-Versicherung ist kein Produkt von der Stange und ohne ein Grundverständnis für digitale Prozesse und den Unterschieden in den Versicherungsbedingungen ist eine Versicherungslösung unmöglich.

Leider vermitteln alle Gesellschaften Ihnen als Endkunden das Gefühl, die perfekte Lösung zu haben. Daher raten wir Ihnen bei der Ermittlung von Risiken, der Ermittlung von Versicherungsbedarf und dem Abschluss einer Versicherungslösung sich von einem Versicherungsexperten, wie der Vinzentz GmbH, für Cyber-Risiken unterstützen zu lassen. Ein spezialisierter Versicherungsexperte versteht das Thema IT-Sicherheit und kann mit Ihren IT-Fachkräften auf Augenhöhe kommunizieren.

Im Moment ist die Anzahl an spezialisierten Versicherungsmaklern noch sehr gering. Daraus lässt sich schließen, dass die Cyber-Versicherung kein Thema für die klassische Versicherungsberatung ist, sondern ein Thema für Spezialisten. Weiterhin ist, aufgrund der aktuellen Lage, priorisiertes Handeln gefordert. Von der Risikoermittlung bis zum Abschluss und der Einrichtung können mehrere Wochen vergehen. Daher raten wir Ihnen das Thema zeitnah und priorisiert zu lösen. Hier sind wir, gemeinsam mit Ihrer eigenen IT-Fachkraft oder einem externen IT-Dienstleister, Ihr Partner mit dem Verständnis für Ihr Unternehmen und dem vertieften Wissen zum Thema Cyber-Versicherung.

## Wir sind Ihr Partner, denn wir kümmern uns!

Bereits seit vielen Jahren setzen wir uns mit dem Thema Cyber-Versicherung auseinander. Wir stehen nicht nur im engen Kontakt zu unseren Kunden, sondern auch mit den Produktanbietern. Wir hinterfragen Lösungen kritisch und bleiben im Gespräch mit Ihren IT-Dienstleistern.

### Wir achten für Sie auf:

- das Preis-Leistungsverhältnis und die Obliegenheiten der Versicherungsgesellschaft

### Wir übernehmen für Sie:

- Analyse Ihres Bedarfs
- Gemeinsam mit Ihrer IT-Betreuung oder einem externen Dienstleister überprüfen wir Ihrer IT-Struktur und Risiken.
- Auswahl der passenden Versicherungslösung
- Regelmäßige Überprüfung und Austausch
- Unterstützung im Schadenfall


Unsere Informationsseite mit der Möglichkeit direkt eine Anfrage an uns zu stellen.
Dort können Sie auch Ihre bestehende Absicherung überprüfen lassen

https://www.vinzentz-makler.de/cyber-versicherung

Vinzentz
Ihr Versicherungspartner

Vinzentz GmbH
Campus Fichtenhain 63, 47807 Krefeld
Tel: 0 21 51 – 2 56 21
info@vinzentz-gmbh.de

dieBUexperten
Unser Service zum Thema
Arbeitskraftsicherung