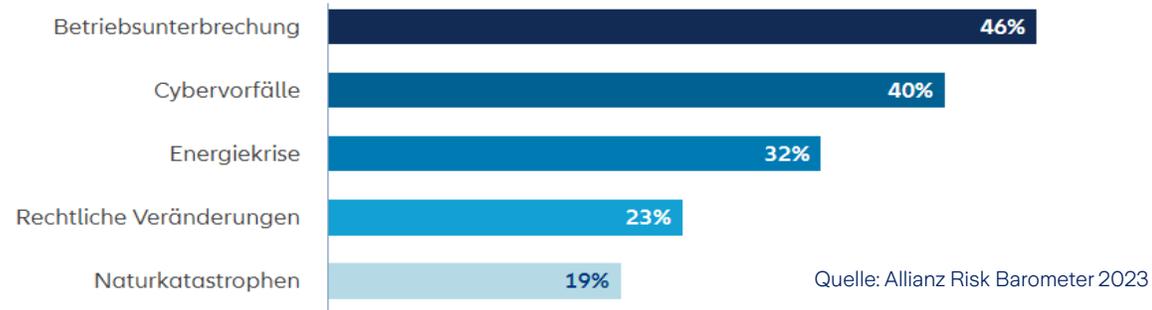


TOP 5 der Geschäftsrisiken für Unternehmen



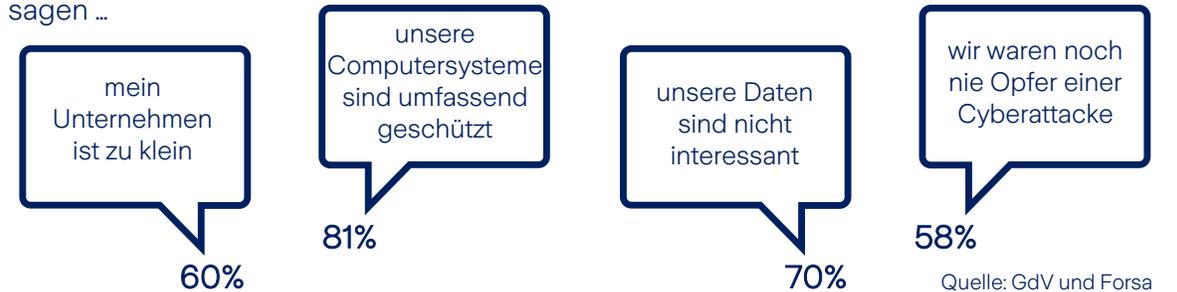
Die entscheidendsten Cyber-Risiken

-  1. **85% aller Cyber-Angriffe starten beim Faktor Mensch**
(menschliche Schwächen - Neugierde, Vergesslichkeit, Sorglosigkeit - machen das Unternehmen angreifbar)
-  2. **Technische Sicherheitslücken**
(Software-Schwachstellen, fehlende Sicherheitspatches und Updates)
-  3. **Steuerung durch externe IT-Dienstleistern**
(Risiko, das mit einem Cyber-Angriff einhergeht, liegt jedoch weiterhin vollumfänglich im eigenen Unternehmen)
-  4. **Unterschätztes Risiko-Management**
(welche Risiken möchte das Unternehmen eingehen und welche sollen vermieden werden)
-  5. **Fehlende Investitionen**
(veraltete Software, ungeschützte Hardware, ungeschulte Belegschaft)

Gefährlicher Irrglaube

Obwohl nicht funktionierende IT-Systeme schnell das ganze Unternehmen lahmlegen, wird die **Gefahr für die IT- und Datensicherheit oft nicht erkannt.**

Von den Befragten, die nur ein geringes Risiko für das eigene Unternehmen sehen, sagen ...



Darum Cyberversicherung

- **Notfallmanagement**
- Abwehr, Bewältigung und Nachbearbeitung von Cyberangriffen
- Rettung von Daten, Wiederherstellung der Handlungsfähigkeit nach einem Cyberangriff
- Absicherung gegen finanzielle Risiken und Folgen

Wer braucht eine Cyberversicherung

Jedes Unternehmen, das

- (vertrauliche und/oder personenbezogene) Daten verarbeitet
- IT-lastige Prozesse hat, also kaum noch analog arbeiten kann
- von der Verfügbarkeit von Daten und Systemen abhängig ist

IT-Sicherheit ist Chefsache!

Geschäftsführer sind für die IT-Sicherheit des Unternehmens verantwortlich – unabhängig davon, ob sich die persönliche Expertise auf diesen Bereich erstreckt oder nicht – ggfs. haften sie auch persönlich gegenüber geschädigten Dritten.

Die Leistungsmerkmale der Cyberversicherung kurz erklärt

Cyberversicherung für den Datenschutz

Wenn Sie Opfer eines Hackerangriffs und dabei z.B. Kundendaten erbeutet werden, können Ihre Kunden von Ihnen Schadenersatz verlangen.

Für den Fall, dass Ihnen durch Cyberkriminalität eigene Schäden und ein Imageschaden aufgrund einer Datenpanne entstehen, übernimmt der Versicherer beispielsweise auch die Kosten für die **Datenrettung oder eine PR-Beratung**.

Ein Bußgeld seitens der Datenschutzbehörde **wegen eines DSGVO-Verstoßes**, ist ebenfalls versichert, solange dies nach geltendem Recht möglich ist.

Was deckt die Cyberversicherung ab



- Krisenmanagement, PR-Kosten
- IT-Forensik und Beratungskosten
- Daten- und Systemwiederherstellung
- Kosten für Austausch / Reparatur von beschädigter oder zerstörter Computerhardware
- Betriebsunterbrechung, Ertragsausfall sowie Mehrkosten / Aufwendungen zur Vermeidung, Minimierung oder Verkürzung der Betriebsunterbrechung
- Kosten infolge einer Datenschutzverletzung
- Cyber-Drittsschäden

Zusätzlich im TopSchutz enthalten:

- Cyber-Erpressung
- Vertragsstrafen infolge der Nichterfüllung von Liefer- oder Abnahmeverpflichtungen
- E-Discovery
- PCI-DSS Vertragsstrafen

Optional im TopSchutz möglich:

- Cyber-Betrug und unautorisierte Nutzung des Telefonsystems

Vorsorge treffen - Awareness

- ✓ E-Learnings zu Cybersicherheit, Datenschutz und Phishing
- ✓ Phishing-Kampagnen
- ✓ Gefahrenwarnung per Mail
- ✓ E-Mail Scan und Darknet-Scan
- ✓ IT-Sicherheitsprüfung mit Checkliste und Score
- ✓ Mitarbeiter-Aktivierung



perseus.

Cyber Dritt- und Eigenschäden

- ✓ Haftpflicht infolge Informationssicherheitsverletzung
- ✓ Abwehr unbegründeter und Freistellung von begründeten Haftpflichtansprüchen
- ✓ Abfederung finanzieller Folgen
- ✓ PR – Konzept zur Abwendung negativer Auswirkungen
- ✓ DSGVO: Übernahme von Geldbußen
- ✓ Daten- / Systemwiederherstellung
- ✓ Ertragsausfall
- ✓ Medienhaftpflicht *
- ✓ Freistellung externer Datenverarbeiter*
- ✓ PCI-DSS Vertragsstrafen*



* Je nach gewähltem Deckungskonzept

Krisenmanager im Schadenfall

- ✓ 24 Stunden pro Tag, sieben Tage pro Woche, 365 Tage pro Jahr
- ✓ Koordination aller Maßnahmen aus einer Hand
- ✓ erster Ansprechpartner
- ✓ legt fest, welche Schritte als Nächstes zu unternehmen sind
- ✓ benennt und koordiniert die unterstützenden Cyber-Experten



perseus.

Cyber Betrug

- ✓ Erstattung von direkten finanziellen Verlusten
- ✓ Erstattung erhöhter Kosten für den Datenverbrauch bei Telefonhacking
- ✓ Optionale Ergänzung gegen Cyberkriminalität
- ✓ Ausschnittsdeckung der Vertrauensschadenversicherung



Perseus Hotline: +49 (0)30 2332 730 94