# Cyber Readiness Report 2026: Cyber-Risiken sind Geschäftsrisiko

## Die wichtigsten Zahlen für Ihre Kundenberatung auf einen Blick

**31 %**
der deutschen KMU wurden im vergangenen Jahr angegriffen oder stellten einen Angriffsversuch fest.

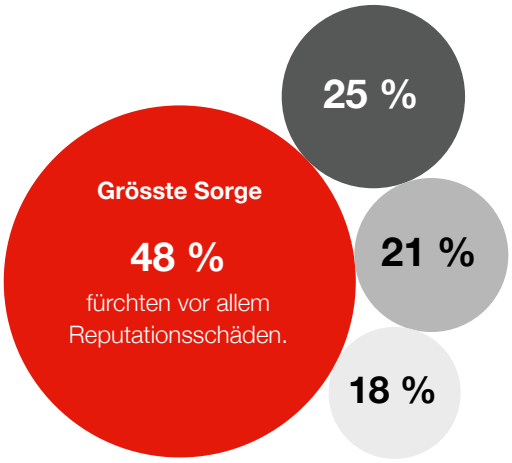
**33 %**
der Betroffenen sahen Zahlungsfähigkeit oder Existenz erheblich gefährdet.

**41,7 Std.**
durchschnittlicher Betriebsstillstand nach einem Angriff.

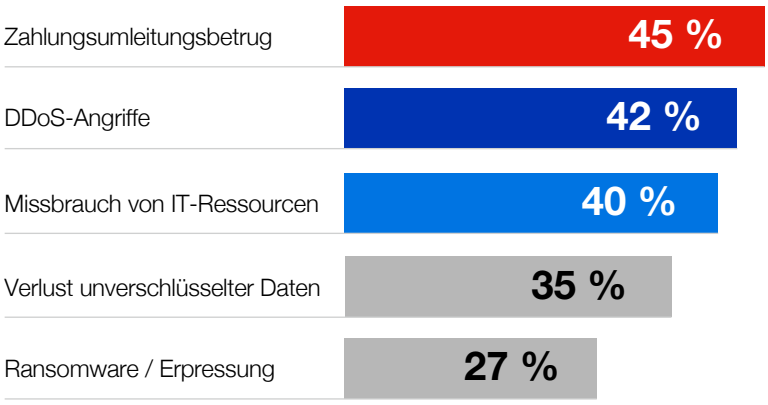
**39 %**
der Betroffenen mussten eine erhebliche Geldstrafe verkraften.

**Jedes 3. Unternehmen**
hat derzeit keine Cyber-Versicherung

## Wahrnehmung vs. Realität




## Die häufigsten erfolgreichen Angriffsarten




Tatsächlich berichten Betroffene deutlich seltener von negativer Öffentlichkeitswirkung (25 %), dem Verlust von Geschäftspartnern (21 %) oder Kunden (18 %). Die Außenwirkung wird damit häufig überschätzt, während finanzielle und operative Folgen schwerer wiegen.

**Take-away**

**Cyber-Angriffe sind vor allem ein Betriebs- und Finanzrisiko.** Kunden denken oft zuerst an Imageschäden. Für die Beratung sind jedoch vor allem Betriebsunterbrechungen, Liquiditätsengpässe, finanzielle Folgen und Krisenmanagement relevant.

*„Viele deutsche KMU sind für Cyberrisiken sensibilisiert und investieren in Absicherung. Ein erfolgreicher Angriff kann dennoch schnell existenziell werden. Im Ernstfall zählen vor allem Liquidität, Geschäftsbetrieb und schnelle Unterstützung. Eine vollwertige Standalone-Cyberversicherung kann finanzielle Schäden abfedern und Unternehmen mit Expertenhilfe durch den Vorfall begleiten“,*

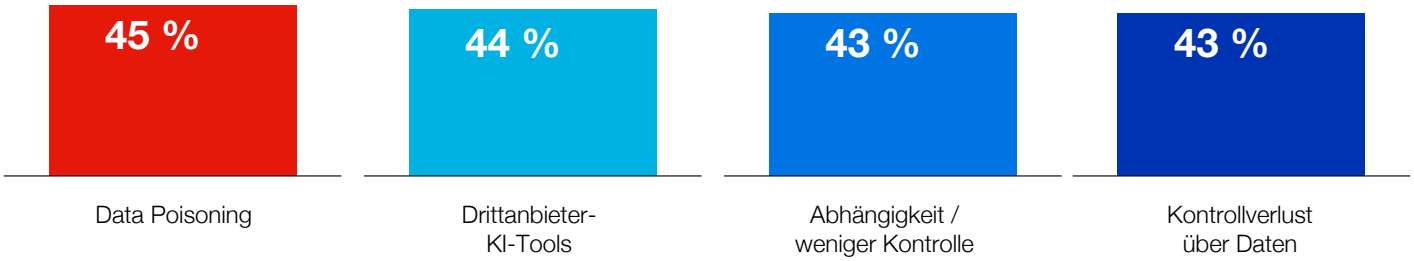
sagt **Klemens Lemke**, Underwriting Manager Cyber bei Hiscox.

HISCOX

Ausgezeichneter Schadenservice
4,7 / 5
Kundenzufriedenheit (Kundenbefragung 2023)

## KI verschärft die Risikolage

Künstliche Intelligenz verändert die Risikolandschaft. Als größte KI-bezogene Bedrohungen in den kommenden fünf Jahren nennen deutsche KMU:




## Vier Chancen für Ihr Beratungsgespräch

### 01 Kunden aktivieren

Nutzen Sie den Report als Anlass für ein Gespräch über konkrete Auswirkungen auf Geschäftsbetrieb und Liquidität.

### 02 Entscheider ansprechen

Cybersecurity ist Managementaufgabe: Nach einem Angriff koppeln 41 % die Vergütung der Führungsebene an Cybersecurity-Ziele.

### 03 Vertriebspotenzial sichern

Jedes dritte Unternehmen verfügt derzeit über keine Cyberdeckung. Weitere 32 % haben Cyberschutz über eine andere Versicherung als eine Standalone-Cyberversicherung. Das bietet die Chance, den bestehenden Versicherungsschutz zu überprüfen und mögliche Deckungslücken aufzudecken.

### 04 KI-Risiken aufgreifen

KI eröffnet neue Gesprächsanlässe, etwa zu Data Poisoning, Drittanbieter-KI-Tools oder dem Verlust der Kontrolle über Unternehmensdaten.

## Vom Risiko zur Lösung: So unterstützt CyberClear by Hiscox

| Risiko | CyberClear by Hiscox |
|---|---|
| **Payment Diversion & Cyber-Betrug** | Schutz bei Cyber-Betrug und Forderungsausfällen sowie Unterstützung durch Experten im Schadenfall. |
| **DDoS-Angriffe & Betriebsstillstand** | Optionaler Baustein Cyber-Betriebsunterbrechung zur Absicherung von Betriebsunterbrechungen. Inkl. schnelle Hilfe durch einzigartige Tagessatzpauschale. |
| **Ransomware & Datenverlust** | Kostenübernahme für z. B. IT-Forensik, Wiederherstellung, Krisenmanagement und Soforthilfe. |
| **Haftungsrisiken nach Cybervorfällen** | Cyber-Haftpflicht inklusive Prüfung und Abwehr unberechtigter Ansprüche. |
| **Neue KI-Risiken** | Cyber-Trainings, Phishing-Simulationen, Sicherheits-Scan und Business Academy mit Inhalten zu Datenschutz- und KI-Risiken. |

Weitere Highlights der Cyber-Versicherung entdecken

HISCOX

Ausgezeichneter Schadenservice
4,7 / 5
Kundenzufriedenheit
(Kundenbefragung 2023)

## Drei Fragen für das nächste Kundengespräch

| 1 | 2 | 3 |
|---|---|---|
| Wie lange kann Ihr Unternehmen einen Ausfall zentraler Systeme verkraften? | Welche finanziellen und operativen Folgen deckt Ihre bestehende Lösung ab? | Wer unterstützt Sie im Ernstfall bei IT-Forensik, Krisenmanagement und Wiederanlauf? |

## Glossar

| Risiko | CyberClear by Hiscox |
|---|---|
| **Payment Diversion bzw. Zahlungsumleitungsbetrug** | Beim Zahlungsumleitungsbetrug geben sich Kriminelle als Lieferanten/Geschäftspartner aus und manipulieren Zahlungsdaten oder Rechnungen. Dadurch werden eigentlich legitime Zahlungen auf Konten der Betrüger überwiesen. |
| **DDoS-Angriff** | Bei einem DDoS-Angriff überfluten Cyberkriminelle Server, Webseiten oder IT-Systeme mit einer großen Anzahl automatisierter Anfragen. Die Systeme werden dadurch überlastet und sind für Kunden oder Mitarbeitende zeitweise nicht mehr erreichbar. |
| **Data Poisoning** | Beim Data Poisoning manipulieren Angreifer gezielt die Daten, mit denen KI-Systeme oder andere digitale Anwendungen arbeiten. Dadurch können fehlerhafte Ergebnisse, falsche Entscheidungen oder Sicherheitslücken entstehen. |
| **Ransomware** | Ein Angriff auf den eigenen Computer per schädlicher Software (Malware), die bösartig eingeschleust wurde. Die Malware sorgt dafür, dass der Computer infiziert wird und die Dateien auf der Festplatte und auf beschreibbaren Laufwerken verschlüsselt werden. Cyberkriminelle fordern häufig ein Lösegeld, damit die Daten wieder entschlüsselt werden. |
| **Cyber-Betriebsunterbrechung** | Von einer Cyber-Betriebsunterbrechung spricht man, wenn ein Unternehmen aufgrund eines Cybervorfalls seinen Geschäftsbetrieb ganz oder teilweise nicht fortführen kann. |

### Über die Umfrage

Der internationale Hiscox Cyber Readiness Report (CRR) liefert seit 2016 jährlich ein aktuelles Bild der Cyber-Bereitschaft von Unternehmen und bietet eine Blaupause für Best Practices im Umgang mit einer sich ständig weiterentwickelnden Bedrohung. Die Befragung zum CRR 2026 wurde vom Marktforschungsinstitut Wakefield Research im Auftrag von Hiscox durchgeführt. Grundlage sind 6.800 Cybersecurity-Fachexpertinnen und -experten sowie Entscheiderinnen und Entscheider, die für die Cybersecurity-Strategie ihres Unternehmens verantwortlich sind. Die Befragten arbeiten in Unternehmen mit weniger als 250 Mitarbeitenden in den USA, Frankreich, Deutschland, Spanien, dem Vereinigten Königreich, Irland, Portugal, Italien, den Niederlanden und Belgien. Berücksichtigt wurden bei Unternehmen mit weniger als 50 Mitarbeitenden die Funktionen Owner, Principal und Partner, bei Unternehmen mit 50 bis 249 Mitarbeitenden die Funktionen CIO, CISO, Director+ Security und Director+ IT. Die Befragung wurde vom 5. bis 17. Juni 2026 per E-Mail-Einladung und Online-Umfrage durchgeführt.

**Hiscox**
Bernhard-Wicki-Straße 3, 80636 München
**T** +49 89 54 58 01 100 **E** hiscox.info@hiscox.de
**W** **makler.hiscox.de**