

CYBERVORFÄLLE – DIE UNSICHTBARE GEFAHR AUS DEM NETZ

Cyberfälle sind weiterhin das größte Risiko mit globalen Schäden von etwa 8,6 Billionen Euro und besonders kritischen Angriffen auf Datenschutz, Infrastrukturen und durch Ransomware.

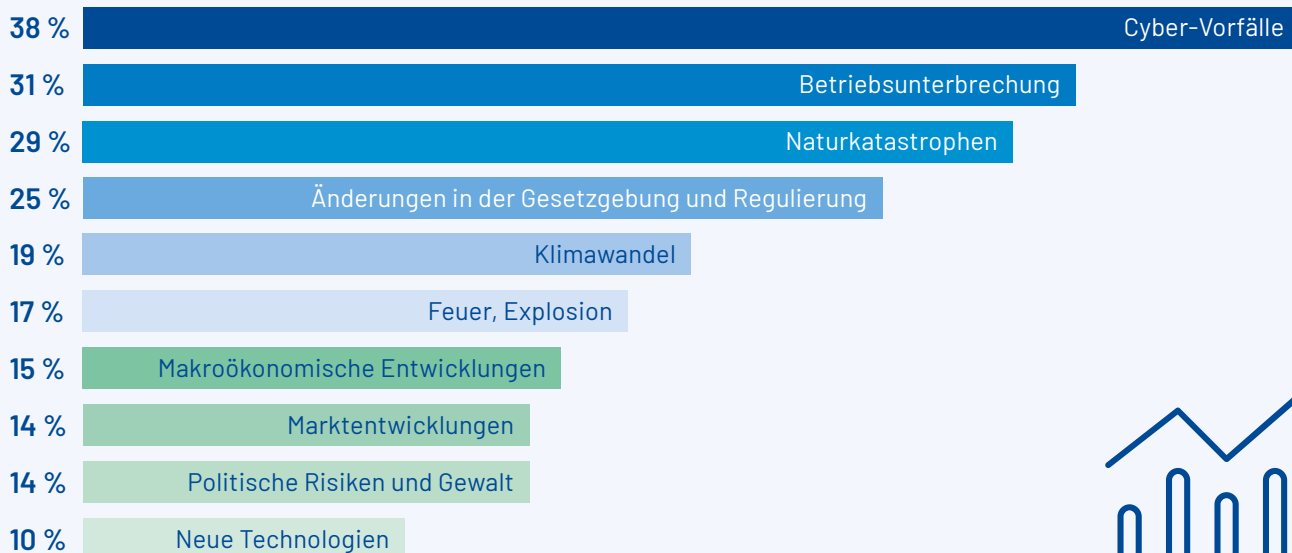


Das größte Risiko für Unternehmen und Institutionen

2025 führen zum vierten Mal in Folge Cyberfälle die Liste der weltweit gefürchtetsten Risiken im Allianz Risk Barometer an – und zwar mit deutlichem Abstand. Schäden durch Cyberkriminalität werden global auf 8,6 Billionen Euro geschätzt – nahezu die Hälfte des Bruttoinlandsprodukts der gesamten EU. Allein in Deutschland summieren sich die Schäden laut Bundesamt für Sicherheit in der Informationstechnik (BSI) auf etwa 206 Milliarden Euro im Jahr. Besonders kritisch werden Datenschutzverletzungen (59 %), Angriffe auf kritische Infrastrukturen und physische Vermögenswerte (53 %) sowie Ransomware-Angriffe (53 %) eingestuft. Die Auswirkungen sind sowohl finanziell als auch reputationsseitig oftmals existenzbedrohend.

Cyberkriminelle gehen dabei immer professioneller vor und nutzen Technologien wie künstliche Intelligenz, um Angriffe zu automatisieren. So erhöhen sie Geschwindigkeit und Schlagzahl der Attacken. Außerdem führt die angespannte geopolitische Lage vermehrt zu politisch motivierten Cyberangriffen, die häufig im Kontext hybrider Kriegsführung auftreten. Das BSI warnt zudem vor einer Verlagerung der Angriffe auf kleinere und mittelständische Unternehmen (KMUs), auch als Einfallstor in die Lieferketten von Großunternehmen. Insgesamt wird deutlich: Es ist für alle Unternehmen und Institutionen essenziell, sich frühzeitig und strategisch mit Cyber Risiken auseinanderzusetzen, um eventuelle Schäden zu begrenzen und Resilienz aufzubauen.

Top 10 Risiken, Quelle: Allianz Risk Barometer 2025



Effektiver Schutz

Ganzheitlich gedacht

Die Bedrohungslage macht deutlich, wie wichtig Prävention im Bereich Cyber ist. Auch wenn selbst die beste Vorbereitung keine absolute Sicherheit garantiert, lässt sich das Risiko eingrenzen. Dazu gehört es, möglichst hohe Hürden für Cyberkriminelle aufzubauen, aber auch, die Auswirkungen eines Vorfalls bestmöglich zu minimieren. Grundlage dafür ist ein ganzheitliches Risikomanagement bestehend aus vier zentralen Bausteinen, die erst in Kombination nachhaltig wirksam werden und bei denen unser Expertenteam von **eccyber** Sie ganzheitlich unterstützt:

1. Organisatorische Maßnahmen sorgen dafür, dass Unternehmen auch im Ernstfall handlungsfähig bleiben und Schäden somit so gering wie möglich gehalten werden können.



2. Personelle Maßnahmen sind besonders wichtig, weil über zwei Drittel der Cyberschäden durch die eigenen Mitarbeitenden verursacht oder begünstigt werden.
3. Technische Maßnahmen schaffen Hürden für Cyberkriminelle und Handlungsfähigkeit für Betroffene im Ernstfall.
4. Der Risikotransfer in eine Cyberversicherung bildet den Abschluss, da selbst, wenn alle Maßnahmen erfolgreich implementiert sind, ein erhebliches Restrisiko bleibt.



"Unsere langjährige Erfahrung in unterschiedlichen Geschäftsfeldern und das in uns gesetzte Vertrauen sind unser Ansporn auch das Thema Cyber für unsere Kunden in gewohnter Qualität darzustellen."

Johannes Vakalis
Senior Fachbetreuer Vertrieb
Ecclesia Cyber



Ihre Vorteile auf einen Blick:

- Versichererunabhängiger Risikobericht
- Unterstützung bei Optimierungsmaßnahmen der Cybersicherheit
- Passgenauer Versicherungsschutz
- 24/7-Notfallservice
- Professionelles Schadenmanagement

Unser hochspezialisiertes Team steht Ihnen mit seinem ganzheitlichen Ansatz bei Ihrer Cybersicherheit gerne zur Seite. Wir freuen uns auf Ihre Kontaktanfrage.

☎ +49 89 38177-160 ✉ team@ecclesia-cyber.de



Ihre Dienstleistungen und Versicherungslösungen aus einer Hand

Von der Evaluierung bis zum Incident Response: Unsere Spezialeinheit **eccyber** bietet Ihnen alle Versicherungslösungen und Dienstleistungen, die Sie für ein ganzheitliches Risikomanagement benötigen. Alle Informationen dazu finden Sie hier: qr.ecclesia.de/r/hierbistdu richtigig

