

Digitale Resilienz, Souveränität und Cybersecurity in Zeiten geopolitischer Instabilität

IT-Optionen für Versicherungen
Dr. Stephan Spieleder, Tobias Müller

16. September 2026

 Finanzgruppe

Agenda



- 1. Digitale Resilienz braucht Cybersecurity**
Identitätsmanagement, Verschlüsselung und Überwachung als Fundament
- 2. Weiterentwicklung digitale Resilienz**
Was ist zu tun, um aktuellen Bedrohungen und Anforderungen gerecht zu werden?
- 3. Cybersecurity bei der Versicherungskammer**
Unsere Maßnahmen, unsere Erfolge

Was ist digitale Resilienz?

Definition digitale Resilienz gemäß DORA-Verordnung:

„...die Fähigkeit eines Finanzunternehmens, seine operative Integrität und Betriebszuverlässigkeit aufzubauen, zu gewährleisten und zu überprüfen, indem es entweder direkt oder indirekt durch Nutzung der von IKT-Drittdienstleistern bereitgestellten Dienste das gesamte Spektrum an IKT-bezogenen Fähigkeiten sicherstellt, die erforderlich sind, um die Sicherheit der Netzwerk- und Informationssysteme zu gewährleisten, die von einem Finanzunternehmen genutzt werden und die kontinuierliche Erbringung von Finanzdienstleistungen und deren Qualität, einschließlich bei Störungen, unterstützen...“ - Verordnung 2022/2554 (DORA) - Artikel 3 Abs. 1

“



Oder kurz zusammengefasst:

...die Fähigkeit, IKT-gestützte Geschäftsprozesse auch unter Störungen und Angriffen aufrechtzuerhalten.

Welche Bedrohungen kennen wir Versicherer schon?

ANWENDUNG 12. Mai 2026

BaFin warnt vor KI-gestützten Cyber-Angriffen auf Finanzbranche und stärkt Verbraucherschutz

Die Finanzaufsicht BaFin warnt angesichts wachsender geopolitischer Unsicherheiten vor steigenden Risiken für die Finanzbranche – und rückt dabei insbesondere Cyber-Gefahren in den Fokus. Verbraucherschutz und Finanzstabilität hätten dabei „den gleichen Stellenwert“, betonte BaFin-Präsident MaBranson auf der Jahrespressekonferenz der Behörde in Frankfurt.

Cyberisiken

Aufseher warnen vor schweren Hackerangriffen auf Versicherer

Versicherer könnten zum bevorzugten Opfer von Cyberattacken werden. Die Pandemie haben die Gefahr zuletzt verstärkt. Die BaFin sind bereits alarmiert.

Schnell
12 - 12:50 Uhr

Studie: Cyberangriffe sind größte Herausforderung für Banken und Versicherungen bis 2030

27.10.2025 • Lesezeit 3 Minuten

Die BaFin / Publikationen & Daten / Risiken im Fokus / Risiken im Fokus 2025

4. Risiken aus Cyber-Vorfällen mit gravierenden Auswirkungen ↑

Cybersecurity als Fundament der digitalen Resilienz



Schwachstellen und
Patchmanagement



Identitäts- und
Zugriffsmanagement



Multi-Faktor
Authentisierung



Verschlüsselung von
Daten und des
Datenverkehrs



Kontinuierliche
Überwachung der IT und
Reaktion



Getestete Backups
und Wiederanlaufpläne

Digitale Resilienz entsteht durch die Summe an wirksamen Sicherheitsmaßnahmen

Geopolitische Veränderungen bedeuten neue Bedrohungen

Welche Veränderungen sehen wir



Die Versicherungsbranche kommt **zunehmend** in den **Fokus verschiedener Akteure**: Es geht dabei neben **finanziellem Gewinn** (z. B. durch Erpressung), der **Gewinnung** von **wertvollen (Kunden-)Informationen** auch um **Sabotage**.



Durch **internationale Konflikte zerstörte (IT-)Infrastruktur** kann zu signifikanten **Ausfällen** von **Geschäftsprozessen** führen und **schädigt** dadurch das **Vertrauen in das Unternehmen**.



ANWENDUNG 27. August 2026

Cyberangriffe: Geheimdienste nehmen auch Banken und Versicherungen stärker ins Visier

6:26 Ausländische Nachrichtendienste werden bei Cyberangriffen auf

Zwei AWS-Rechenzentren direkt von Drohnen getroffen: Reparatur wird dauern

AWS hat bestätigt, dass gleich zwei Rechenzentren in den Golfstaaten VAE und Bahrain "direkt" von Drohnen getroffen wurden. Die Lage bleibe unvorhersehbar.

Versicherung

Was die Versicherungsbranche für die zivile Verteidigung tun kann

Angesichts einer immer unsicheren geopolitischen Lage müsse sich die Branche besser auf Krisenfälle vorbereiten, fordert der Chef der Versicherungskammer Bayern.

Tami Holderried, Susanne Schlier
26.05.2026 - 15:14 Uhr

Multi-Cloud als Antwort auf die neue Bedrohungslage



Unser Ansatz: Hybrides Rechenzentrum mit Multi-Cloud

Hybride Rechenzentren und Multi-Cloud in IT-Strategie verankert



Wir nutzen bereits **hybride Rechenzentren mit Multi-Cloud-Ansatz**. Dies ermöglicht uns die **Verteilung kritischer Arbeitsprozesse** auf **unterschiedliche Umgebungen** und **reduziert** damit signifikant **die Ausfallwahrscheinlichkeit**.

Unsere Ausgestaltung des Multi-Cloud-Ansatzes



Einheitliches Identitätsmanagement und eine **Verschlüsselung** der kritischen Daten ermöglicht den Cloud-übergreifenden Schutz der Daten.



Die Nutzung eines Multi-Cloud Ansatzes ermöglicht die **Nutzung innovativer neuer Technologien** (z.B. moderne Modelle künstlicher Intelligenz).



Kontinuierliche Überwachung der gesamten Infrastruktur (Rechenzentrum und Cloud) durch **Security Operation Center**.



Durch die **Nutzung von EU-Rechenzentren** halten wir strenge Datenschutzvorgaben ein.

Weiterentwicklung der Cybersicherheitsmaßnahmen



**Umsetzung neuer
Verschlüsselungs-
standards**



**Eigenständige
Verwaltung der
Schlüssel zur
Verschlüsselung**



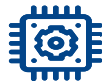
**Zentrales Key- und
Zertifikatsmanagement**



**Resiliente
IAM-Architektur**



**Einheitliches Zugriffs- und
Rollenkonzept**



**Privileged Access
Management (PAM) und
risikobasierte
Authentifizierung**



**Kontinuierliche
Überwachung**



Integration in SIEM/SOAR

Weiterentwicklung des Risikomanagements



Beispiele unserer vielfältigen Cybersecurity-Maßnahmen

PRÄVENTIV



Schwachstellenmanagement: Fokus auf schnelle Behebung von Schwachstellen.



Netzsegmentierung: Verbesserung der Widerstandsfähigkeit des internen Netzwerks, bestätigt durch Penetrationstester.



Datensicherheit:

Sensible Daten in zentralen Datenbanken sind verschlüsselt.



Privileged Access Management:

Einführung eines PAM-Tools zum Schutz der privilegierten Nutzerkonten.

ÜBERWACHUNG



Security Operation Center

Automatisierte Erkennung von Cyberangriffen und 24x7 Reaktion auf Angriffe.



Darknet-Monitoring:

Accounts mit abgegriffenen Zugangsdaten wurden umgehend zurückgesetzt.



Systemisolation:

Isolation von durch kritische Schwachstellen verwundbaren, exponierten Systemen bei bekannten Angriffen, um Datenabflüsse zu verhindern.



Angriffsabwehr:

Sofortige Isolation von Endpunkten nach bestätigter Malware-Infektion.

ÜBERPRÜFUNG



Testprogramm:

Erarbeitung einer Strategie und eines Programms zur flächendeckenden Testung der digitalen Resilienz.



Penetrationstesting:

Durchgängiges und regelmäßiges Penetrationstesting aller kritischer Anwendungen.



Red Team Tests:

Realitätsnahe Angriffstests.



DORA-Prüfung:

Erste Jahresabschlussprüfung mit DORA-Anforderung bestätigt unsere Arbeit mit sehr gutem Ergebnis.

Fazit



Digitale Resilienz unter dem blauen Schirm ist kein reines IT-Vorhaben, sondern ein strategisches Architektur- und Governance-Prinzip des gesamten Unternehmens.

Ansprechpartner



Dr. Stephan Spieleder

Vorstandsmitglied Konzern
Versicherungskammer,
Ressort IT



Tobias Müller

Generalbevollmächtigter der VKB und
Geschäftsführer InsureConnect GmbH