

# Cyber-Resilienz als strategische Chance im Versicherungsmarkt



Versicherungs-DNA als Wettbewerbsvorteil für Makler

## Was Cyber-Versicherungen leisten

Moderne Cyber-Policen bieten grundlegenden Schutz bei typischen Vorfällen:

-  **Sofortmaßnahmen nach Sicherheitsverletzungen:** Kosten für forensische Untersuchungen, rechtliche Erstberatung und Krisenmanagement
-  **Wiederherstellungskosten:** Direkte Ausgaben für die Beseitigung von Schadsoftware und Datenwiederbeschaffung
-  **Haftungsschutz:** Abwehr von Ansprüchen Dritter durch Datenschutzverletzungen
-  **Betriebsunterbrechung:** Entschädigung bei Ertragsausfälle während direkter Systemausfälle
-  **Cyber-Erpressung:** Unterstützung bei Lösegeldforderungen und teilweise Übernahme der Zahlungen

## Kritische Deckungslücken der Realität

Jenseits des Versicherungsschutzes bleiben jedoch signifikante finanzielle Risiken:

-  **Langfristige Reputationsschäden:** Der anhaltende Vertrauensverlust bei Kunden mit Umsatzrückgängen über Jahre
-  **Strukturelle IT-Investitionen:** Die notwendige technische Neuausrichtung nach einem Vorfall mit sechsstelligen Kosten
-  **Wertminderung geistigen Eigentums:** Die praktisch unversicherbare Entwertung von Forschungsdaten und Produktplänen
-  **Regulatorische Sanktionen:** Bußgelder wegen systematischer Compliance-Verstöße außerhalb einfacher Datenschutzverletzungen
-  **Überlaufende Schäden:** Kosten über das Sublimit hinaus.

## Chancen für Versicherungsmakler

Makler können ihre Position als Berater stärken, indem sie neben der Policenvermittlung Deckungslücken proaktiv ansprechen und ZRS-Lösungen anbieten. Diese Transparenz festigt das Kundenvertrauen und erhöht die Relevanz des Maklers im Risikomanagement-Prozess. Kunden verlassen sich langfristig auf Partner mit realistischen Einschätzungen.

Die Partnerschaft mit ZRS erschließt vier konkrete Wettbewerbsvorteile:

1. Fachliche Erweiterung	2. Effiziente Prozesse
<p><b>Herausforderung:</b> Technische Kompetenz bei komplexen Cyber-Risikofragen</p> <p><b>ZRS-Lösung:</b> Fachlicher Sparringpartner für Cyber-Risikofragen</p> <p><b>Ihr Mehrwert:</b> Fundierte Beratung ohne eigenes IT-Spezialwissen</p>	<p><b>Herausforderung:</b> Zeitaufwändige technische Risikoprüfungen</p> <p><b>ZRS-Lösung:</b> Vorvalidierte Risikobewertung für Underwriter</p> <p><b>Ihr Mehrwert:</b> Schnellere Deckungszusagen für Ihre Kunden</p>
3. Zusätzliche Geschäftsfelder	4. Strategische Positionierung
<p><b>Herausforderung:</b> Margendruck im traditionellen Versicherungsgeschäft</p> <p><b>ZRS-Lösung:</b> Provisionsmodelle für Resilienz-Services</p> <p><b>Ihr Mehrwert:</b> Neue Einnahmequellen bei gleichzeitiger Kundenbindung</p>	<p><b>Herausforderung:</b> Differenzierung im Wettbewerbsumfeld</p> <p><b>ZRS-Lösung:</b> Cyber Resilienz-Beratungskompetenz</p> <p><b>Ihr Mehrwert:</b> Position als ganzheitlicher Risikoberater</p>

## Ein standardisiertes Vorgehen



Ausgangssituation

Komplexe Platzierung von Cyber-Versicherungen durch unklare Risikolage und Zeitdruck.

ZRS-Ansatz

Systematische Analyse und Wissenstransfer zur optimalen Vorbereitung für den Versicherer.

Ergebnisse

Effizientere Platzierung, bessere Konditionen und ein höherer Schutz für Ihre Kunden.

## Vertriebsvorteile durch ZRS

- Praxisnaher Cyber-Risiko-Workshop und Schulungen für Ihr Team (IDD konform)
- Gemeinsame Kundenansprache entwickeln
- Regelmäßige Updates zur Bedrohungslage



**Michael Guiao**

Senior Cyber Risk Engineer

[michael.guiao@zurich.com](mailto:michael.guiao@zurich.com)  
+49 151 27 54 70 02



**Liane Velten**

Cyber Risk Engineer

[liane.velten@zurich.com](mailto:liane.velten@zurich.com)  
+49 175 4108108



**Christian Schottmüller**

Head of Cyber  
Business Development

[c.schottmueller@zurich.com](mailto:c.schottmueller@zurich.com)  
+49 151 20660174

## Zurich Resilience Solutions – Unser Mehrwert:



**Versicherbarkeit:** Optimierte Versicherungslösungen



**Schadenserfahrung:** Erkenntnisse aus realen Schadensfällen



**Risikoorientierung:** Passgenaue Lösungen für verschiedene Unternehmensprofile



**Fachexpertise:** Praxisorientierte Methodik



**Globale Präsenz:** Weltweites Expertennetzwerk mit lokalem Fokus

Dies ist eine allgemeine Beschreibung von (Versicherungs-)Dienstleistungen wie Risiko-Engineering oder Risikomanagement durch Zurich Resilience Solutions, die Teil des kommerziellen Versicherungsgeschäfts der Zurich Insurance Group ist, und stellt keine Versicherungspolice oder Dienstleistungsvereinbarung dar oder ändert diese. Solche (Versicherungs-)Dienstleistungen werden qualifizierten Kunden von verbundenen Unternehmen der Zürich Versicherungs-Gesellschaft AG erbracht, insbesondere von der Zurich American Insurance Company, 1299 Zurich Way, Schaumburg, IL 60196, USA, The Zurich Services Corporation, 1299 Zurich Way, Schaumburg, IL 60196, USA, Zurich Insurance plc, Zurich House, Ballsbridge Park, Dublin 4, Irland, Zurich Resilience Solutions Europe GmbH, Platz der Einheit, 2, 60327 Frankfurt am Main, Deutschland, Zurich Management Services Limited, The Zurich Centre, 3000b Parkway, Whiteley, Fareham, Hampshire, PO15 7Z, Großbritannien, Zurich Insurance Company Ltd, Mythenquai 2, 8002 Zürich, Schweiz, Zurich Australian Insurance Limited, ABN 13 000 296 640, Australien.

Die hierin zum Ausdruck gebrachten Meinungen sind die von Zurich Resilience Solutions zum Zeitpunkt der Veröffentlichung und können ohne vorherige Ankündigung geändert werden. Dieses Dokument wurde ausschließlich zu Informationszwecken erstellt. Alle in diesem Dokument enthaltenen Informationen wurden aus Quellen zusammengestellt, die als zuverlässig und glaubwürdig erachtet werden. Die Zürich Versicherungs-Gesellschaft AG oder eine ihrer Tochtergesellschaften (Zurich Insurance Group) geben jedoch weder ausdrücklich noch stillschweigend eine Zuschreibung oder Gewährleistung hinsichtlich ihrer Richtigkeit oder Vollständigkeit. Dieses Dokument ist nicht als Rechts-, Versicherungs-, Finanz-, Anlage- oder sonstige professionelle Beratung gedacht. Zurich Insurance Group lehnt jegliche Haftung ab, die sich aus der Verwendung dieses Dokuments oder dem Vertrauen auf dieses Dokument ergibt. Nichts in diesem Dokument ist ausdrücklich oder implizit dazu bestimmt, Rechtsbeziehungen zwischen dem Leser und einem Mitglied der Zurich Insurance Group zu schaffen. Dieses Dokument enthält gewisse zukunftsgerichtete Aussagen, die u.a. Voraussagen über zukünftige Ereignisse, Trends, Pläne, Entwicklungen oder Ziele beinhalten, aber nicht darauf beschränkt sind. Solche Aussagen sind mit Vorsicht zu genießen, da sie naturgemäß bekannten und unbekannten Risiken und Unsicherheiten unterliegen und von zahlreichen unvorhersehbaren Faktoren beeinflusst werden können. Der Gegenstand dieses Dokuments ist auch nicht an ein bestimmtes Dienstleistungsangebot oder ein Versicherungsprodukt gebunden und gewährleistet auch nicht den Schutz durch eine Versicherungspolice.

Dieses Dokument darf ohne vorherige schriftliche Genehmigung der Zürich Versicherungs-Gesellschaft AG, Mythenquai 2, 8002 Zürich, Schweiz, weder ganz noch auszugsweise verbreitet oder vervielfältigt werden. Kein Mitglied der Zurich Insurance Group übernimmt eine Haftung für Verluste, die sich aus der Verwendung oder Verbreitung dieses Dokuments ergeben. Dieses Dokument stellt weder ein Angebot noch eine Aufforderung zum Kauf oder Verkauf von Wertpapieren in irgendeiner Rechtsordnung dar.



“

Wir machen Cyber-Risiken  
durch Resilienz-Strategien  
und Versicherung  
kontrollierbar



## Cyber Resilience Services

Unternehmen sind durch die schnelle digitale Transformation und neue Technologien vermehrt Cyber-Risiken ausgesetzt.

Unsere kombinierten Cybersicherheitslösungen schützen Ihr Unternehmen effektiv vor Cyber-Risiken.

### Ihre Herausforderungen



#### Zunahme von Cyberangriffen

Cyber-Bedrohungen werden komplexer und Angriffe raffinierter – bleiben Sie proaktiv.



#### Schutz kritischer Daten und Vermeidung finanzieller Verluste

Identifizieren Sie kritische Unternehmensdaten, um Betrieb und Kundenschutz zu sichern.



#### Regulatorische Anforderungen steigen und werden anspruchsvoller

EU-Regularien wie die DSGVO, NIS2 und der Cyber Resilience Act (CRA) sowie Deutschlands IT-Sicherheitsgesetz fordern verstärkte Cybersicherheits- und Datenschutzmaßnahmen.



### Unsere Lösung



#### Klarheit schaffen

Wir leiten sicher durch den Cyberspace und die rechtlichen Anforderungen.



#### Kombination von Präventionsdiensten und Risikotransferlösungen

Umsetzung wirksamster Sicherheitsmaßnahmen und optimierter Versicherungsschutz durch forschungsbasierten Ansatz.



#### Erhöhung der Cyber-Maturität und Widerstandsfähigkeit

Pragmatische und kosteneffiziente Methoden für eine höhere Sicherheit.



# Cyber Resilience für KMU's

Erhöhen Sie Ihre Cyber-Maturität und verbessern Sie Ihr Versicherungsrisikoprofil. Bevorzugte Bedingungen und Konditionen für Cyber-Versicherungen durch die Zurich Versicherung.



## Bronze

Empfohlen bei Umsatz bis zu  
EUR 10 Millionen

ab EUR 4.000



### Cyber Snapshot

Bewertung der Cybersicherheitslage anhand einer Reifegrad-Checkliste.



### Ext. and Int. Schwachstellenscans

Automatisiertes Verfahren zur Identifizierung und Erkennung von Sicherheitslücken in Computersystemen und Netzwerken.



### Cyber Awareness-Schulung

Mitarbeiter befähigen potenzielle Cyber-Bedrohungen zu erkennen und die Wahrscheinlichkeit erfolgreicher Cyber-Angriffe zu verringern.

### Umfang

- Begrenzt auf einen definierten Standort
- Outside-in Scan
- Inside-out Scan
- Eine Online-Session
- Ideal für ca. 50 Personen

## Silber

Empfohlen bei Umsatz zwischen  
EUR 10 – 100 Millionen

ab EUR 9.900



### Cyber Health Check: Cyber-Maturitäts-Assessment

Evaluierung auf Basis von standardisierten Fragebögen und den NIST-Vorgaben, inklusive ausführlichem Bericht und geeigneten Empfehlungen.



### Cyber Quantifizierung

Analyse des finanziellen Risikos basierend auf definierten Cyber-Risikoszenarien zur Festlegung und Priorisierung von Cyber-Investitionen.



### Cyber Awareness-Schulung (Online)

Mitarbeiter befähigen, potenzielle Cyber-Bedrohungen zu erkennen und die Wahrscheinlichkeit erfolgreicher Cyber-Angriffe zu reduzieren.



### Phishing-Simulation

Sensibilisierung der Mitarbeiter durch Simulation authentischer Phishing-E-Mails, um Angriffe zu erkennen und adäquat darauf zu reagieren.

### Umfang

- Begrenzt auf einen definierten Standort
- Momentaufnahme basierend auf öffentlichen Informationen
- Eine Online-Session
- Ideal für ca. 50 Personen
- Bis zu 50 E-Mails

## Gold

Empfohlen bei Umsatz zwischen  
EUR 25 - 100 Millionen

ab EUR 19.900



### "Silber"-Paket

Alle Dienstleistungen im "Silber"-Paket.



### Managed Detection Response für KMUs (SOC)

KMU Security Operations Center für Echtzeitüberwachung und schnelle Reaktion auf Cybersecurity-Bedrohungen auf Endpunkt ebene.

### Umfang

- Siehe oben
- Einschliesslich Next-Gen Antivirus
- Bis zu 99 Server und Computer
- 8/5 Überwachung und Reaktion
- Abonnement für 1 Jahr

# Cyber Resilience für den Mittelstand



Erhöhen Sie Ihre Cyber-Maturität und verbessern Sie Ihr Versicherungsrisikoprofil. Bevorzugte Bedingungen und Konditionen für Cyber-Versicherungen durch die Zurich Versicherung.

## Silber

Empfohlen bei Umsatz zwischen  
EUR 100 – 500 Millionen

Ab EUR 19.900



### Externer Penetrationstest

Individuell angepasste manuelle Simulation von externen, realen Angriffen zur Ermittlung von Schwachstellen und Beurteilung potenzieller Risiken.



### Interner Penetrationstest

Individuell angepasste manuelle Simulation interner Angriffe zur Ermittlung von Schwachstellen und Beurteilung potenzieller Risiken.



### Phishing-Simulation

Sensibilisierung der Mitarbeiter durch Nachbildung realer Phishing-E-Mails, um Angriffe zu erkennen und adäquat darauf zu reagieren.



### Cyber Awareness-Schulung (Online)

Mitarbeiter befähigen, potenzielle Cyber-Bedrohungen zu erkennen und die Wahrscheinlichkeit erfolgreicher Cyber-Angriffe zu reduzieren.



### Cyber Health Check: Cyber-Maturitäts-Assessment

Evaluierung auf Basis von standardisierten Fragebögen und den NIST-Vorgaben, inklusive ausführlichem Bericht und geeigneten Empfehlungen.

### Umfang

- 3 Tage
- Bis zu 50 IP und Systeme
- 5 Tage
- Bis zu 50 IPs und Systeme
- Bis zu 200 E-Mails
- Zwei Online-Sessions
- Ideal für maximal 150 Personen
- Begrenzt auf definierten Standort

## Gold

Empfohlen bei Umsatz zwischen  
EUR 100 Millionen – 1 Milliarde

Ab EUR 29.900



### "Silber"-Paket

Alle Dienstleistungen aus dem "Silber"-Paket.



### Cyber Quantifizierung

Bewertung des finanziellen Risikos basierend auf vordefinierten Cyber-Risikoszenarien zur Festlegung und Priorisierung von Cyber-Investitionen.

### Umfang

- Siehe oben
- 2 maßgeschneiderte Risikoszenarien



# Cyber Resilience für Großunternehmen



Erhöhen Sie Ihre Cyber-Maturität und verbessern Sie Ihr Versicherungsrisikoprofil. Bevorzugte Bedingungen und Konditionen für Cyber-Versicherungen durch die Zurich Versicherung.

## Silber

Empfohlen bei Umsatz zwischen EUR 1 – 5 Milliarden

Ab EUR 22.900



### Externer Penetrationstest

Individuell angepasste manuelle Simulation von externen, realen Angriffen zur Ermittlung von Schwachstellen und Beurteilung potenzieller Risiken.



### Cyber Quantifizierung

Analyse des finanziellen Risikos basierend auf definierten Cyber-Risikoszenarien zur Festlegung und Priorisierung von Cyber-Investitionen.



### Phishing-Simulation

Sensibilisierung der Mitarbeiter durch Nachbildung realer Phishing-E-Mails, um Angriffe zu erkennen und adäquat darauf zu reagieren.

### Umfang

- 7 Tage
- Bis zu 500 IP und Systeme
- 2 maßgeschneiderte Risikoszenarien
- Bis zu 500 E-Mails

## Gold

Empfohlen bei Umsatz über EUR 5 Milliarden

Ab EUR 34.900



### "Silber"-Paket

Alle Dienstleistungen im "Silber"-Paket.



### Krisenmanagement "Table-top Exercise"

Szenario-basierte Übung zur Bewertung und Verbesserung Ihrer Bereitschaft und Reaktionsstrategien im Falle eines Cyberangriffs.

### Umfang

- Siehe oben
- Simulation eines Krisenszenarios
- Test des aktuellen Reaktionsplans



## Schulungen

		Preise ab
	<b>Phishing-Simulation</b> Sensibilisierung der Mitarbeiter durch Nachbildung realer Phishing-E-Mails, um Angriffe zu erkennen und adäquat darauf zu reagieren.	EUR 1.000
	<b>Cyber Escape Game</b> Immersives Erlebnis, das die Teilnehmer herausfordert, Cyber-Rätsel zu lösen und so ihr Wissen und ihre Fähigkeiten auf innovative Weise zu verbessern. Sowohl in einer physischen Umgebung als auch mit einem Virtual-Reality-Headset umsetzbar.	EUR 1.000
	<b>Cyber Awareness-Schulung (Online)</b> Mitarbeiter befähigen, potenzielle Cyber-Bedrohungen zu erkennen und die Wahrscheinlichkeit erfolgreicher Cyber-Angriffe zu reduzieren.	EUR 1.500
	<b>Vor-Ort-Schulung inkl. Cyber Escape Game</b> Individuell angepasste Vor-Ort-Schulung zu bewährten Praktiken im Bereich Cyber und Datenschutz unter simulierten Angriffsbedingungen.	EUR 2.000
	<b>Krisenmanagement-Training</b> Unternehmen lernen, wie sie Cyber-Krisen bewältigen und auf sie reagieren können, um den Schaden effektiv zu begrenzen.	EUR 2.000

## Assessments

		Preise ab
	<b>Cyber Snapshot</b> Bewertung der Cybersicherheitslage anhand einer Reifegrad-Checkliste.	EUR 2.500
	<b>Cyber Healthcheck: Cyber-Maturitäts-Assessment</b> Evaluierung auf Basis von standardisierten Fragebögen und den NIST-Vorgaben, inklusive ausführlichem Bericht und geeigneten Empfehlungen.	EUR 6.000
	<b>Datenschutz-Audit &amp; Cyber-Maturitäts-Assessment</b> Prüfung der Einhaltung lokaler und internationaler Datenschutzvorschriften sowie Bewertung des Reifegrads der Cybersicherheit.	EUR 9.000
	<b>ISO 27001 Audit</b> Prüfung der Cyber-Maturität gemäß ISO 27001 zur Vorbereitung auf die Zertifizierung.	EUR 12.000
	<b>Krisenmanagement-Audit</b> Bewertung der Bereitschaft, Reaktionsfähigkeit und Widerstandsfähigkeit gegenüber Cyber-Bedrohungen und -Zwischenfällen.	EUR 10.000
	<b>Krisenmanagement "Table-top exercise"</b> Szenario-basierte Übung zur Bewertung und Verbesserung Ihrer Bereitschaft und Reaktionsstrategien im Falle eines Cyberangriffs.	EUR 14.000

## Technische Services

	Preise ab
 <b>Externe und interne Schwachstellenscans</b> Automatisiertes Verfahren zur Identifizierung und Erkennung von Sicherheitslücken in Computersystemen und -netzwerken.	EUR 1.000
 <b>Penetrationstests</b> Individuell angepasste manuelle Simulation von externen, realen Angriffen zur Ermittlung von Schwachstellen und Beurteilung potenzieller Risiken.	EUR 4.000
 <b>Managed Detection and Response für KMUs (SOC)</b> KMU Security Operations Center (8/5) für Echtzeitüberwachung und schnelle Reaktion auf Cybersecurity-Bedrohungen auf Endpunktenebene.	EUR 10.000
 <b>Managed Detection and Response (SOC)</b> Umfassendes Security Operations Center (24/7) für Echtzeitüberwachung und schnelle Reaktion auf Cybersecurity-Bedrohungen.	EUR 15.000

## Strategie-Support

	Preise ab
 <b>Cyber Governance</b> Unterstützung bei der Ausarbeitung der Dokumentation zur Cybersicherheit (Zugangskontrolle, Passwörter, Datenklassifizierung, Verschlüsselung und mehr).	EUR 3.000
 <b>Incident Response</b> Dokumentiertes Verfahren, das die Reaktion und das Management von Cybersicherheitsvorfällen definiert.	EUR 4.000
 <b>Cyber Quantifizierung</b> Bewertung des finanziellen Risikos basierend auf vordefinierten Cyber-Risikoszenarien zur Festlegung und Priorisierung von Cyber-Investitionen.	EUR 5.000
 <b>Cyber Supply Chain Risk Management</b> Dienstleistung zur Überwachung der Cyber-Reife der gesamten Lieferkette (Preise gelten pro Dienstleister).	EUR 1.000
 <b>Business-Continuity-Services</b> Definition der Business-Continuity-Strategie, einschließlich Durchführung einer Business Impact Analyse, Entwicklung von Richtlinien, Anweisungen und mehr.	Auf Anfrage
 <b>CISO-as-a-Service</b> Adhoc-Unterstützung durch Bereitstellung von Fachwissen für die Entwicklung, Umsetzung und Verwaltung einer Cyber-Strategie.	Auf Anfrage