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.

ZRS Versicherungs-DNA als Wettbewerbsvorteil

ZURICH
Resilience Solutions

Die Partnerschaft mit ZRS erschließt vier konkrete Wettbewerbsvorteile:

1. Fachliche Erweiterung

Herausforderung: Technische Kompetenz bei komplexen Cyber-Risikofragen

ZRS-Lösung: Fachlicher Sparringpartner für Cyber-Risikofragen

Ihr Mehrwert: Fundierte Beratung ohne eigenes IT-Spezialwissen

2. Effiziente Prozesse

Herausforderung: Zeitaufwändige technische Risikoprüfungen

ZRS-Lösung: Vorvalidierte Risikobewertung für Underwriter

Ihr Mehrwert: Schnellere Deckungszusagen für Ihre Kunden

3. Zusätzliche Geschäftsfelder

Herausforderung: Margendruck im traditionellen Versicherungsgeschäft

ZRS-Lösung: Provisionsmodelle für Resilienz-Services

Ihr Mehrwert: Neue Einnahmequellen bei gleichzeitiger Kundenbindung

4. Strategische Positionierung

Herausforderung: Differenzierung im Wettbewerbsumfeld

ZRS-Lösung: Cyber Resilienz-Beratungskompetenz

Ihr Mehrwert: Position als ganzheitlicher Risikoberater

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

Ihre Kontakte

ZURICH
Resilience Solutions

Michael Guiao

Senior Cyber Risk Engineer

michael.guiao@zurich.com
+49 151 27 54 70 02

Liane Velten

Cyber Risk Engineer

liane.velten@zurich.com
+49 175 4108108

Christian Schottmüller

Head of Cyber
Business Development

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

ZURICH
Resilience Solutions

Deutschland

> 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 Cybersicherheits-lösungen 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

ZURICH
Resilience Solutions

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 Endpunktebene.

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

ZURICH
Resilience Solutions

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

	Umfang
Externer Penetrationstest Individuell angepasste manuelle Simulation von externen, realen Angriffen zur Ermittlung von Schwachstellen und Beurteilung potenzieller Risiken.	• 3 Tage • Bis zu 50 IP und Systeme
Interner Penetrationstest Individuell angepasste manuelle Simulation interner Angriffe zur Ermittlung von Schwachstellen und Beurteilung potenzieller Risiken.	• 5 Tage • Bis zu 50 IPs und Systeme
Phishing-Simulation Sensibilisierung der Mitarbeiter durch Nachbildung realer Phishing-E-Mails, um Angriffe zu erkennen und adäquat darauf zu reagieren.	• Bis zu 200 E-Mails
Cyber Awareness-Schulung (Online) Mitarbeiter befähigen, potenzielle Cyber-Bedrohungen zu erkennen und die Wahrscheinlichkeit erfolgreicher Cyber-Angriffe zu reduzieren.	• Zwei Online-Sessions • Ideal für maximal 150 Personen
Cyber Health Check: Cyber-Maturitäts-Assessment Evaluierung auf Basis von standardisierten Fragebögen und den NIST-Vorgaben, inklusive ausführlichem Bericht und geeigneten Empfehlungen.	• Begrenzt auf definierten Standort

Gold

Empfohlen bei Umsatz zwischen EUR 100 Millionen – 1 Milliarde

Ab EUR 29.900

	Umfang
"Silber"-Paket Alle Dienstleistungen aus dem "Silber"-Paket.	• Siehe oben
Cyber Quantifizierung Bewertung des finanziellen Risikos basierend auf vordefinierten Cyber-Risikoszenarien zur Festlegung und Priorisierung von Cyber-Investitionen.	• 2 maßgeschneiderte Risikoszenarien

Cyber Resilience für Großunternehmen

ZURICH
Resilience Solutions

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

	Umfang
Externer Penetrationstest Individuell angepasste manuelle Simulation von externen, realen Angriffen zur Ermittlung von Schwachstellen und Beurteilung potenzieller Risiken.	• 7 Tage • Bis zu 500 IP und Systeme
Cyber Quantifizierung Analyse des finanziellen Risikos basierend auf definierten Cyber-Risikoszenarien zur Festlegung und Priorisierung von Cyber-Investitionen.	• 2 maßgeschneiderte Risikoszenarien
Phishing-Simulation Sensibilisierung der Mitarbeiter durch Nachbildung realer Phishing-E-Mails, um Angriffe zu erkennen und adäquat darauf zu reagieren.	• Bis zu 500 E-Mails

Gold

Empfohlen bei Umsatz über EUR 5 Milliarden

Ab EUR 34.900

	Umfang
"Silber"-Paket Alle Dienstleistungen im "Silber"-Paket.	• Siehe oben
Krisenmanagement "Table-top Exercise" Szenario-basierte Übung zur Bewertung und Verbesserung Ihrer Bereitschaft und Reaktionsstrategien im Falle eines Cyberangriffs.	• Simulation eines Krisenszenarios • Test des aktuellen Reaktionsplans

Cyber Resilience à la carte

ZURICH
Resilience Solutions

Schulungen

	Preise ab
Phishing-Simulation Sensibilisierung der Mitarbeiter durch Nachbildung realer Phishing-E-Mails, um Angriffe zu erkennen und adäquat darauf zu reagieren.	EUR 1.000
Cyber Escape Game 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
Cyber Awareness-Schulung (Online) Mitarbeiter befähigen, potenzielle Cyber-Bedrohungen zu erkennen und die Wahrscheinlichkeit erfolgreicher Cyber-Angriffe zu reduzieren.	EUR 1.500
Vor-Ort-Schulung inkl. Cyber Escape Game Individuell angepasste Vor-Ort-Schulung zu bewährten Praktiken im Bereich Cyber und Datenschutz unter simulierten Angriffsbedingungen.	EUR 2.000
Krisenmanagement-Training Unternehmen lernen, wie sie Cyber-Krisen bewältigen und auf sie reagieren können, um den Schaden effektiv zu begrenzen.	EUR 2.000

Assessments

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

Cyber Resilience à la carte

ZURICH
Resilience Solutions

Technische Services

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

Strategie-Support

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