



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 Österreichs Entwurf für ein 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

Umsatz bis zu
EUR 10 Millionen

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 maximal 50 Personen

Silber

Umsatz zwischen
EUR 10 – 100 Millionen

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 maximal 50 Personen
- Bis zu 50 E-Mails

Gold

Umsatz zwischen
EUR 25 - 100 Millionen

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
- 24/7 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

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

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 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

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

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



Phishing-Simulation

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

Preise ab
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



Cyber Snapshot

Bewertung der Cybersicherheitslage anhand einer Reifegrad-Checkliste.

Preise ab
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

Technische Services



Externe und interne Schwachstellenscans

Automatisiertes Verfahren zur Identifizierung und Erkennung von Sicherheitslücken in Computersystemen und -netzwerken.

Preise ab
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 für Echtzeitüberwachung und schnelle Reaktion auf Cybersecurity-Bedrohungen auf Endpunktebene.

EUR 10.000



Managed Detection and Response (SOC)

Umfassendes Security Operations Center für Echtzeitüberwachung und schnelle Reaktion auf Cybersecurity-Bedrohungen.

EUR 15.000

Strategie-Support



Cyber Governance

Unterstützung bei der Ausarbeitung der Dokumentation zur Cybersicherheit (Zugangskontrolle, Passwörter, Datenklassifizierung, Verschlüsselung und mehr).

Preise ab
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



Danny Steiner

Head of Business Development

danny.steiner@zurich.com
+49 151 24148191



Marcus Appel

Cyber Risk Engineer

marcus.appel@zurich.com
+49 151 63574880

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

Haftungsausschluss

Alle in diesem Dokument enthaltenen Informationen wurden aus Quellen zusammengestellt und bezogen, die als zuverlässig und glaubwürdig gelten, aber weder die Zurich Insurance Company Ltd noch eines ihrer verbundenen Unternehmen (im Folgenden jeweils als 'Zurich' und zusammen als 'Zurich Group' bezeichnet) geben eine ausdrückliche oder stillschweigende Zusicherung oder Gewährleistung hinsichtlich deren Richtigkeit oder Vollständigkeit. Die hier geäußerten Meinungen sind die von Zurich zum Zeitpunkt der Veröffentlichung und können sich ohne vorherige Ankündigung ändern. Dieses Dokument wurde ausschließlich zu Informationszwecken erstellt. Einige der hierin enthaltenen Informationen können zeitkritisch sein. Daher sollten Sie das aktuellste Referenzmaterial konsultieren und zwischenzeitlich vorgenommene Aktualisierungen berücksichtigen.

Die Informationen in diesem Dokument beziehen sich auf Risikotechnik / Risikominderungsdienstleistungen und sind als allgemeine Beschreibung bestimmter Arten von Dienstleistungen gedacht. Sie sollen keinen Überblick über Versicherungsdeckungen, Dienstleistungen oder Programme geben und ändern oder ergänzen keine bestehenden Dienstleistungs- oder Versicherungsverträge, Angebote, Kostenvorschläge oder andere Dokumentationen. Die durch die Dienstleistung zur Verfügung gestellten Informationen stellen keine Rechtsberatung dar (und können eine individuelle rechtliche Beratung durch einen Rechtsanwalt nicht ersetzen).

Zurich und ihre Mitarbeiter übernehmen keinerlei Haftung, die sich aus der Verwendung oder dem Vertrauen auf die hierin enthaltenen Informationen, Materialien oder Verfahren ergibt. Zurich und ihre Mitarbeiter garantieren keine bestimmten Ergebnisse, und es können Bedingungen in Ihren Räumlichkeiten oder innerhalb Ihrer Organisation vorliegen, die für uns möglicherweise nicht erkennbar sind. Sie sind am besten in der Lage, Ihr Unternehmen und Ihre Organisation zu verstehen und Maßnahmen zur Risikominimierung zu ergreifen, und wir möchten Sie dabei unterstützen, indem wir Ihnen Informationen und Werkzeuge zur Verfügung stellen, um Ihr sich änderndes Risikoumfeld zu beurteilen.

In den Vereinigten Staaten sind Risikotechnik-/Risikominderungsdienstleistungen für qualifizierte Kunden über The Zurich Services Corporation verfügbar, und in anderen Ländern werden solche Risikotechnik-/Risikominderungsdienstleistungen von verschiedenen mit der Zurich Insurance Company Ltd verbundenen Rechtseinheiten erbracht.

Dieses Dokument und alle darin enthaltenen Informationen dürfen ohne vorherige schriftliche Genehmigung der Zurich Insurance Company Ltd, Mythenquai 2, 8002 Zürich, Schweiz, nicht veröffentlicht, lizenziert, verkauft oder anderweitig verbreitet werden. Personen und Unternehmen mit Sitz in den USA benötigen die vorherige schriftliche Genehmigung von The Zurich Services Corporation.

Kein Mitglied der Zurich Group übernimmt eine Haftung für Verluste, die sich aus der Verwendung oder Verbreitung dieses Dokuments ergeben.