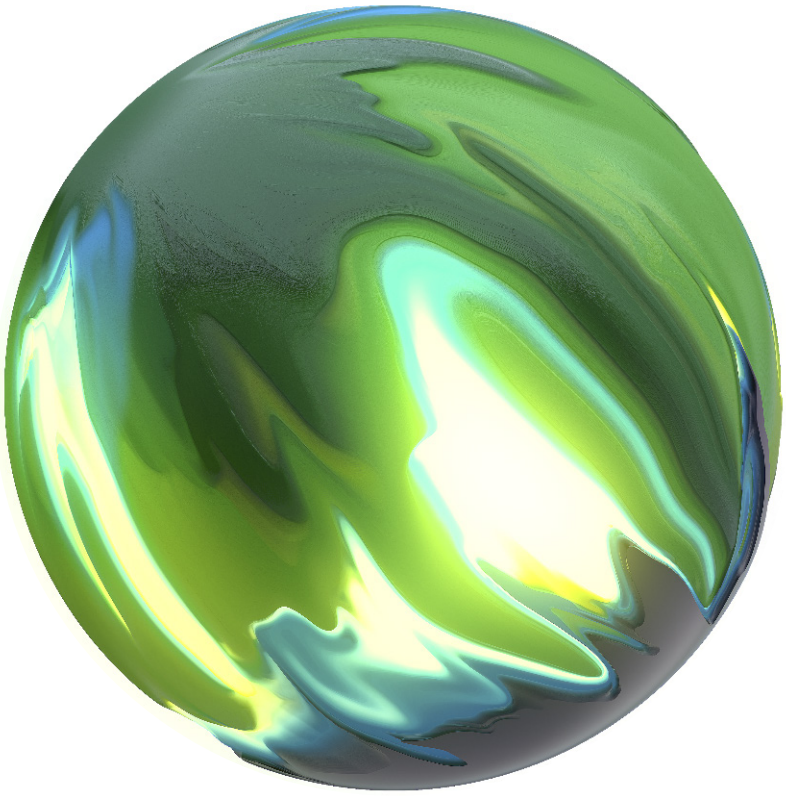
Deloitte.



Cyber Risk Solutions für Ihr Unternehmen

Informationssicherheit betrifft auch Ihr Unternehmen. Das Zusammenspiel von Menschen, Technik und betrieblichen Abläufen wird zunehmend komplexer und ist entscheidend für den Unternehmenserfolg. Eine Vielzahl an Risiken und Bedrohungen geht mit Digitalisierung und modernen Geschäftsmodellen einher. Deloitte unterstützt Sie bei der Einführung und Verbesserung von Sicherheitskonzepten und -maßnahmen.

Zugriffs- und Berechtigungsmanagement

Zugriffsanalyse: Eingehende Untersuchung der bestehenden Zugriffsrechte auf Systeme und Daten, um übermäßige oder unangemessene Berechtigungen zu identifizieren.

Berechtigungsprüfung: Überprüfung und Anpassung der Zugriffsrechte für User und Gruppen, um sicherzustellen, dass nur autorisierte Personen auf sensible Informationen zugreifen können.

Rollenbasiertes Management: Entwicklung klar definierter Rollen und Berechtigungsstufen, um den Zugriff entsprechend den **organisatorischen Anforderungen** zu steuern und zu verwalten.

Ergebnis: Optimierte und sichere IT-Infrastruktur durch effiziente Zugriffsverwaltung, Reduzierung von Risiken und Stärkung der Compliance.

Application Security

Unser Team für Application Security unterstützt Sie dabei, das Programmieren und Entwickeln von Applikationen durch **agile oder klassische Entwicklungsmethoden** sowie durch technische Prozessoptimierung sicher zu gestalten.

(Web-)Applikationen/geschriebener Softwarecode werden nach Schwachstellen untersucht, um potenzielle Sicherheitslücken aufzudecken.

Ergebnis: Erhöhte Anwendungssicherheit, identifizierte Schwachstellen sowie maßgeschneiderte Handlungsempfehlungen, die die Widerstandsfähigkeit gegenüber Cyberangriffen erhöht.

Cyber Quick Check

Ganzheitliche Evaluierung der aktuellen Sicherheitsstrategie und -ausrichtung des Unternehmens (IT und/oder Operationelle Technologien/OT, z.B. Produktionsstätten).

Risikobewertung: Einschätzung von Sicherheits- und Betriebsrisiken, um potenzielle Bedrohungen und Auswirkungen auf die Systeme zu erkennen, sowie Maßnahmen zur Risikominderung vorzuschlagen.

Business Impact im Fokus: Entwicklung einer strategischen Positionierung, die eng an den Unternehmenszielen ausgerichtet ist, um den größtmöglichen Nutzen zu erzielen.

Ergebnis: Fahrplan mit Aktivitäten/Projekten, um den gewünschten Ziel-Reifegrad zu erreichen, Optimierung der **Wertschöpfungskette** sowie **Stärkung der Cybersicherheit** des Unternehmens.

Supply Chain Security

Lieferantenaudit: Umfassende Bewertung der Sicherheitspraktiken und -maßnahmen von Lieferanten sowie Analyse der Lieferkette, um potenzielle Risiken in der Lieferkette (durch Lieferanten oder Dritte) zu identifizieren.

Sicherheitsrichtlinien: Entwicklung und Umsetzung robuster Sicherheitsrichtlinien und -standards, die von den Lieferanten eingehalten werden müssen, um die **Gesamtsicherheit der Lieferkette** zu gewährleisten.

Ergebnis: Gestärkte Lieferketten-Sicherheit durch Risikominderung, vertrauenswürdige Partnerschaften und gesteigerte Resilienz gegenüber Angriffen.

Compliance Check

Der Compliance Check eines Unternehmens umfasst eine **vollständige Analyse** der Datenschutzrichtlinien, -verfahren, -technologien und -kontrollen, um den aktuellen Ist-Zustand zu ermitteln. Dabei werden zusätzlich potenzielle Datenschutzrisiken und -lücken identifiziert.

Weitere, konkret für das Unternehmen zutreffende Regulatorien werden ebenfalls betrachtet, wie z.B. **DORA, NIS2.**

Ergebnis: Sicherstellung der **Compliance** mit regulatorischen Vorschriften sowie angemessener Schutz von Daten; bei Feststellung von Lücken: Entwicklung einer Roadmap und Formulierung von **Handlungsempfehlungen.**

Krisen- und Notfallpläne

Erstellung **eines strategischen Plans sowie Notfallhandbücher,** die sicherstellen, dass Geschäftsaktivitäten auch unter widrigen Bedingungen fortgesetzt werden können.

Eine **Business Impact Analyse** (BIA) hilft dabei zu ermitteln, welche Geschäftsprozesse und Funktionen bei Unterbrechungen besonders betroffen wären und welche daher **besondere Priorität haben.**

Entwurf von gezielten Maßnahmen und Strategien zur Risikominderung und Sicherstellung der Betriebskontinuität in Krisenzeiten.

Ergebnis: Ein umfassender Geschäftskontinuitätsplan mit funktionalen Notfallplänen.

Incident Response Retainer

Ein Ansatz zur **effektiven Bekämpfung und Behebung** von Cyber-Vorfällen, der gleichzeitig das Schutzniveau von Unternehmensinformationen kontinuierlich verbessert.

24/7 Hotline im Cyber-Notfall.

Bei nicht vollständiger Nutzung des Retainer-Budgets im aktuellen Jahr steht das Budget im Folgejahr für **proaktive Beratungsleistunge**n zur Verfügung.

Ziel: Schnelle und **professionelle Reaktion auf Sicherheitsvorfälle,** um potenzielle Risiken und Schäden für das Unternehmen zu minimieren.

Ergebnis: Ein erhöhtes **Sicherheitsniveau**, kontinuierliche **Beratung** und **Flexibilität** bei optimaler Ausnutzung des Budgets für Sicherheitsinvestitionen.

Zero Trust

Eine innovative Sicherheitsstrategie, die davon ausgeht, dass **keine Vertrauensannahmen** – weder innerhalb noch außerhalb des Netzwerks – gemacht werden sollten. Bei diesem Ansatz wird der **Zugriff auf Systeme, Anwendungen und Daten** unabhängig von Ort und Identität streng kontrolliert und überwacht.

Aufteilung des Netzwerks in isolierte Mikrosegmente, Implementierung strenger Identitätsverifikation und Berechtigungsprüfungen sowie Verhaltensanalysen erhöhen das Sicherheitsniveau.

Ergebnis: Flexibilität, Skalierbarkeit und Minimierung von Risiken ermöglichen in einer zunehmend vernetzten Welt sicheres Operieren, unabhängig von Standorten und Geräten.

Cyber Angriffssimulation / PenTesting

Umfassende Simulation echter Bedrohungsakteure, die alle Aspekte Ihres Unternehmens ins Visier nehmen – von IT-Systemen bis hin zu Mitarbeiter:innenzugängen.

Durch die **Kombination** von physischen, technischen und sozialen Angriffswegen und den Einsatz von **fortschrittlichen Werkzeugen und Techniken,** die von professionellen Hackern genutzt werden, sorgen wir für ein tiefgehendes Verständnis möglicher Angriffspunkte.

Ziel: Erkennen und Bewerten der gesamten Risikolandschaft sowie **Aufdeckung von Schwachstellen** in der Sicherheitsstruktur.

Ergebnis: Detaillierter Bericht über technische, physische und menschliche Sicherheitslücken, begleitet von maßgeschneiderten Handlungsempfehlungen.

Ransomware Assessment

In einer **umfassenden Analyse** der **IT-Landschaft** des Unternehmens werden Schwachstellen und Sicherheitslücken mit Blick auf die **Anfälligkeit für Ransomware-Attacken** identifiziert

Es wird ein Blick auf die **verschiedenen Ebenen** des Unternehmens geworfen und so jeder Aspekt des Unternehmens genaustens mit innovativen Lösungen analysiert:

- Überpfüung von Selbsteinschätzung und Dokumente mittels Interviews
- Auf **Datenebene** blicken wir auf Datensicherheit und Berechtigungen
- Die Durchleuchtung des **Netzwerks** legt potenzielle Einfallstore offen

Ergebnis: Umfassende Bewertung der Anfälligkeit für Ransomware-Angriffe

Weitere Services

- Table Top Excercises
- Physical Pentest
- Micro Segmentation
- Source Code Review/Analyse
- Cloud Security
- Secure Operation Center (SOC) Effectiveness Assessment

Ihre Ansprechpersonen:

Georg Schwondra
Partner
+43 664 80 537 3760
gschwondra@deloitte.at

Gerald Kattnig
Director
+43 664 80 537 3762
gkattnig@deloitte.at