Cyber-Security-Check – Wo steht Ihr Unternehmen?

Bitte ankreuzen:
1 = trifft kaum zu
5 = trifft voll zu

Cyber-Sicherheit ist bei uns **unternehmensweit verankert** und durch klar definierte Rollen und Verantwortlichkeiten besetzt: von der Chefetage über die IT-Leitung bis in die Fachbereiche. Personal für die Besetzung der Rollen ist vorhanden.

1 2 3 4 5

Wir haben eine **Inventar-Übersicht und damit Überblick** über unsere Daten und alle Assets, z. B. Software, Systeme, User, Identitäten, Infrastruktur, Vendoren und Umgebungen. Daten klassifizieren wir nach Kategorien wie *Public*, *Confidential* und *Internal*.

1 2 3 4 5

Wir haben **feste Regeln**, wie Mitarbeitende und Externe mit Firmen-IT-Ressourcen und kritischen Daten umgehen sollen. Die Regeln orientieren sich mindestens an Standards wie ISO oder Standards des BSI.

1 2 3 4 5

Unser IT-Personal baut durch Schulung kontinuierlich **Cyber-Security-Wissen** auf. Ein grundlegendes Bewusstsein für Cyber-Sicherheit schaffen wir bei allen Mitarbeitenden durch Trainings und eine gezielte Kommunikationsstrategie.

1 2 3 4 5

Durch regelmäßige Security-Tests und Assessments minimieren wir das Risiko von **Cyber-Sicherheitsvorfällen**. Bei einem Vorfall wissen alle Verantwortlichen, woran sie ihn erkennen und wie sie zu reagieren haben.

1 2 3 4 5

Wir nutzen ein **zentrales Identity & Access Management (IAM)-System** für alle Daten, Ressourcen, Applikation und Maschinen sowie standardisierte IAM-Prozesse für z. B. *Joiner*, *Mover*, *Leaver*, *Grant* und *Revoke*. Die Absicherung erfolgt durch Passwortrichtlinien, starke Multifaktor-Authentifizierung und dynamische Zugriffskontrollen.

1 2 3 4 5

Datenschutz stellen wir durch moderne Technologien und Data Governance sicher. Wir verschlüsseln Daten abhängig von ihrer Nutzung, z. B. durch Secure Mailing & Messaging. Vor Datenverlust schützen wir uns durch Data Loss Prevention (DLP) sowie Backup- & Recovery-Maßnahmen. Außerdem kennen wir die zu erfüllenden Compliance-Anforderungen in all unseren Business-Prozessen.

1 2 3 4 5

Vor **Cyber-Angriffen** schützen wir uns umfassend durch Endpoint-Security und Firewalling, Netzwerksegmentierung, Malwareschutz / Antivirus-Programme, Cloud Security Posture Management, automatische Security-Scanner, Device Management und Patching.

1 2 3 4 5

Wir haben ein **Security Monitoring**.

1 2 3 4 5

Wir wissen um die Fehleranfälligkeit manueller Prozesse und **automatisieren** so viele Prozesse wie möglich, z. B. Monitoring, Risk Detection, Daten-klassifizierung und Patching.

1 2 3 4 5

Bringen Sie Ihre Cyber-Security auf das nächste Level!

Addieren Sie bitte die angekreuzten Punkte. Abhängig von diesem Wert geben wir Ihnen folgende Empfehlungen:

Summe 10 – 20: Sie befassen sich mit dem Thema, wissen aber auch, dass an einigen Stellen akuter Handlungsbedarf besteht. Wie helfen Ihnen dabei, Sicherheitslücken zu identifizieren und Maßnahmen zur Lösungs-Implementierung auf den Weg zu bringen.

Summe 21 – 40: Sie sind bereits auf dem Weg, Cyber-Sicherheit zu einem festen Bestandteil ihres Unternehmens zu machen. Gemeinsam können wir erarbeiten, wo es weiteres Verbesserungspotenzial gibt, z. B. durch Konzepte wie Zero Trust. So können Sie Sicherheitsrisiken weiter minimieren.

Summe 41 – 50: Sie sind in puncto Cyber-Security bereits sehr gut aufgestellt. Jetzt gilt es, Ihr Sicherheitsniveau stets auf einem aktuellen Stand zu halten. Sprechen Sie uns gerne an und wir finden gemeinsam heraus, wie Sie Ihre Strategie dafür verfeinern!

Ihr Wegbegleiter

Wo auch immer Sie aktuell stehen: Lassen Sie uns gerne den Dialog vertiefen. Zusammen finden wir heraus, wie Sie sich noch sicherer aufstellen können und welche Maßnahmen kurz-, mittel- und langfristig für Ihr Unternehmen hilfreich sind.

Dr. Jan Ciupka
Executive Manager Consulting
+49 228 9770-0

Schreiben Sie mir und wir vereinbaren einen Austauschtermin!

KONTAKT AUFNEHMEN