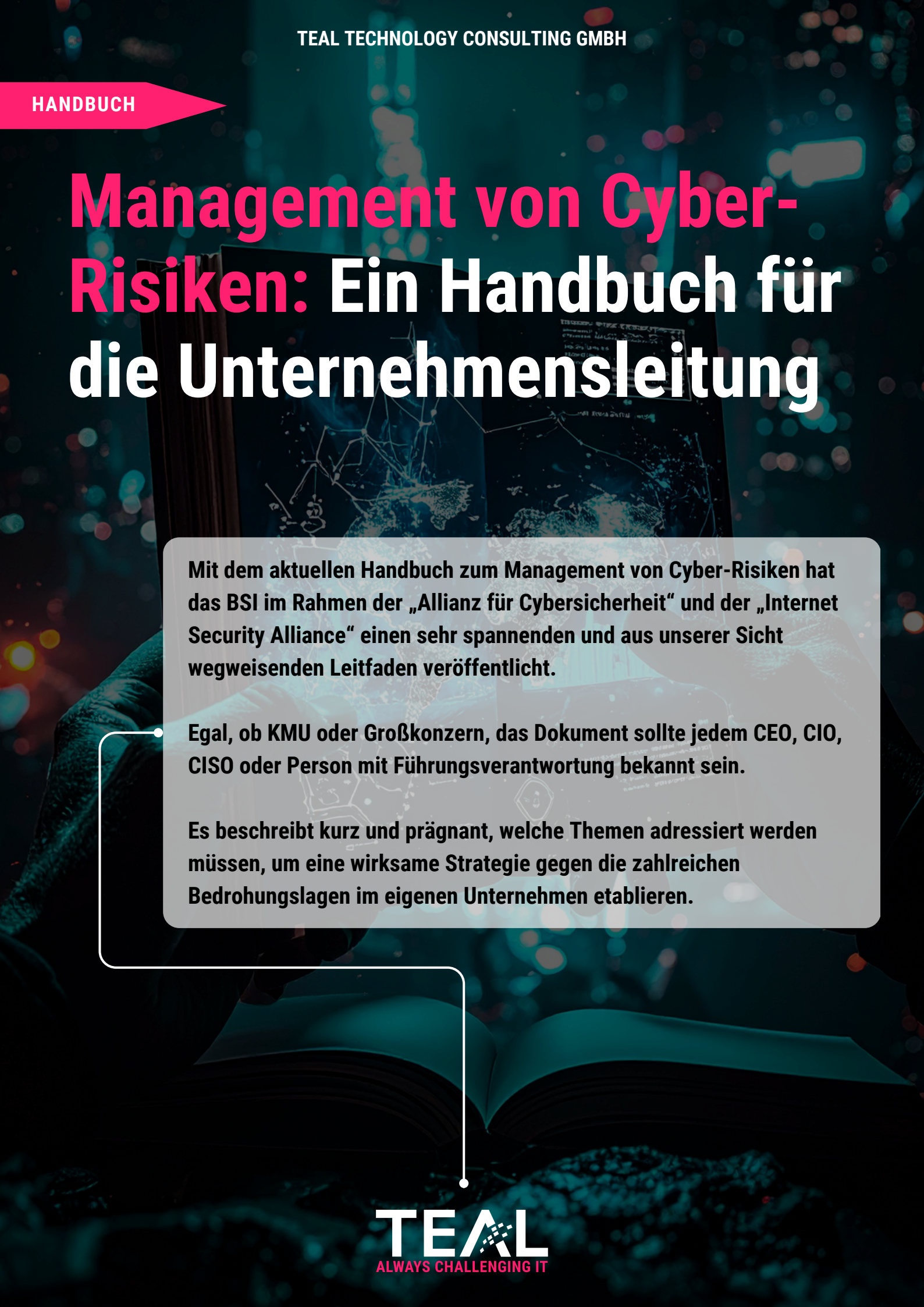
TEAL TECHNOLOGY CONSULTING GMBH

HANDBUCH

Management von Cyber-Risiken: Ein Handbuch für die Unternehmensleitung



Mit dem aktuellen Handbuch zum Management von Cyber-Risiken hat das BSI im Rahmen der „Allianz für Cybersicherheit“ und der „Internet Security Alliance“ einen sehr spannenden und aus unserer Sicht wegweisenden Leitfaden veröffentlicht.

Egal, ob KMU oder Großkonzern, das Dokument sollte jedem CEO, CIO, CISO oder Person mit Führungsverantwortung bekannt sein.

Es beschreibt kurz und prägnant, welche Themen adressiert werden müssen, um eine wirksame Strategie gegen die zahlreichen Bedrohungslagen im eigenen Unternehmen etablieren.

TEAL
ALWAYS CHALLENGING IT

HANDBUCH

Starke Allianzen für eine sichere digitale Zukunft

Die Allianz für Cyber-Sicherheit (ACS)...

… ist eine Initiative des Bundesamts für Sicherheit in der Informationstechnik (BSI) und des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM).

Die Initiative wurde im Jahr 2012 ins Leben gerufen, um Unternehmen und Organisationen in Deutschland bei der Verbesserung ihrer Cybersecurity-Fähigkeiten zu unterstützen. Die Allianz für Cyber-Sicherheit richtet sich an Unternehmen und Organisationen aller Größen und Branchen und bietet ihnen eine Plattform, um sich über Cyberbedrohungen auszutauschen und Best Practices zu teilen. Sie arbeitet eng mit anderen nationalen und internationalen Organisationen zusammen, um das Bewusstsein für Cybersecurity zu erhöhen und die Zusammenarbeit zwischen verschiedenen Akteuren zu fördern.

Die Initiative unterstützt auch die Entwicklung von Standards und Best Practices im Bereich der Cybersecurity und setzt sich für die Schaffung von Richtlinien und Gesetzen ein, die den Schutz von Daten und die Privatsphäre von Unternehmen und Einzelpersonen verbessern.

Die Internet Security Alliance (ISA)...

… ist eine in den USA ansässige gemeinnützige Organisation, die sich zum Ziel gesetzt hat, die Cybersecurity durch die Förderung von bewährten Praktiken und Zusammenarbeit zwischen der öffentlichen Hand und der Privatwirtschaft zu verbessern.

Unser Ansatz: Active Directory Hardening

Als IT-Security-Beratung fokussieren wir uns auf die systematische Härtung Ihrer AD-Umgebung. Ziel ist es, Schwachstellen zu identifizieren, Angriffsflächen zu minimieren und Ihre Verteidigungsmechanismen auf ein neues Level zu bringen. Das geschieht durch technische Maßnahmen, organisatorische Kontrollen und den gezielten Einsatz moderner Tools.

Das Handbuch – Management von Cyber-Risiken

Bereits 2014 erstellte die National Association of Corporate Directors (NACD) in Zusammenarbeit mit AIG und der Internet Security Alliance (ISA) die erste Version des Handbuchs. 2018 erschien die erste Version des deutschen Handbuchs, welches 2023 nun erneut auf die aktuellen Gegebenheiten angepasst wurde.

Das Handbuch umfasst insgesamt 6 Prinzipien:

- Cyber-Sicherheit nicht nur als IT-Thema, sondern als Baustein des unternehmens-weiten Risikomanagements verstehen
- Umsetzung geeigneter Rahmenbedingungen sowie Ressourcen für das Cyber-Risikomanagement sicherstellen
- Rechtliche Auswirkungen von Cyber-Risiken verstehen
- Risikoanalyse erstellen sowie Definition von Risikobereitschaft in Abhängigkeit von Geschäftszielen und -strategien formulieren
- Zugang zu Cyber-Sicherheitsexpertise sowie regelmäßigen Austausch sicherstellen
- Unternehmensweite Zusammenarbeit und den Austausch von Best Practice fördern

Unser Experte: Fabian Böhm

Managing Director und Security-Berater | Teal Technology Consulting GmbH

Mit über 20 Jahren Erfahrung im Security Consulting liegt der Schwerpunkt von Fabian Böhm vor allem auf Microsoft Active Directory, PKI und Cloud-Projekten. Er unterstützt Kunden nachhaltig dabei, ihr Sicherheitsniveau zu verbessern und Angriffe frühzeitig zu erkennen.

Diese Prinzipien sind nicht neu und vermutlich den meisten in der einen oder anderen Form bereits geläufig. Auch die Hinweise der ACS, dass die Bedrohungslage immer weiter zunimmt und KMUs immer mehr betroffen sind, werden informierte Verantwortliche nicht mehr schockieren. **Wir leben in Zeiten, in denen keine Woche vergeht, ohne dass ein oder manchmal sogar mehrere Unternehmen eine Ransomware Attacke verkünden müssen.** Man hat sich fast daran gewöhnt, es ist auch klar, dass etwas gemacht werden muss.
Die spannende Frage ist nur, was genau?

Mit unserem Security Assessment prüfen wir die Infrastruktur von Unternehmen und bewerten die Ergebnisse mit einem risikobasiertem Ansatz. Dies hilft, den aktuellen Status so zu dokumentieren, dass sowohl Administratoren als auch das Management die aktuelle Situation verstehen. **Die Findings werden jedoch oftmals nur punktuell und weniger nachhaltig adressiert. Grundlegend ändern die wenigsten etwas an dem IT-Betrieb.**

Wieso ist das so?

- Sicherheits-Tools allein reichen nicht, sie müssen aktiv betrieben und gepflegt werden.
- Oft fehlen Zeit und Know-how im IT-Betrieb.
- **Folge:** Überforderung der IT, Frust im Management, Investitionsstopp.
- Sicherheitsprojekte scheitern oft an der fehlenden Integration in den laufenden Betrieb.
- **Resultat:** Nur kurzfristige Verbesserungen, langfristig verpufft der Effekt.

Beispiel: Veraltete Passwörter – ein unterschätztes Risiko

Wir erleben immer wieder, dass von >20% aller Benutzerkonten (inklusive Serviceaccounts und Adminkonten) die Kennwörter nicht regelmäßig geändert werden.

Das stellt ein hohes Sicherheitsrisiko dar, die aktuelle Empfehlung des BSI ist beispielsweise, alle Dienstkonten auf (Group) Managed Service Accounts umzustellen und kompromittierte Passwörter umgehend zu ändern. Die Lösung ist erst einmal recht simpel…

- Nicht mehr benötigte Accounts löschen
- Fine Grained Password Policies einführen
- (Group) Managed Service Accounts einführen
- Kennwortwechselprozeduren automatisieren
- Einen Prozess definieren, der regelmäßig den Kennwortwechsel erzwingt

Wenn man allerdings im Schnitt nur einen halben Tag pro Account benötigt, ist der Gesamtaufwand dennoch schnell bei mehreren hundert Personentagen. Für solch eine Aktivität ist das Management oft nicht bereit, Geld auszugeben und der IT-Betrieb hat nicht die Zeit, sich dem Thema anzunehmen. **Die Folge: Account-Passwörter bleiben veraltet und Anwender verwenden teils kompromittierte Passwörter, die nie oder nur sehr selten geändert werden.**

Die 6 Prinzipien im Detail

Cyber-Sicherheit nicht nur als IT-Thema, sondern als Baustein des unternehmensweiten Risikomanagements verstehen

IT-Abteilungen werden oft mit dem Thema IT-Sicherheit alleine gelassen. Klar ist es die Verantwortung der IT, für eine sichere Umgebung zu sorgen. Das heißt aber nicht, dass die vollständige Verantwortung dafür in der IT-Abteilung zu finden ist.

Vielmehr muss IT-Sicherheit bei jeder einzelnen Initiative im Unternehmen berücksichtigt werden. Das fängt bei der Unternehmensleitung an, die das Thema in die Risikoprozesse eingliedern muss.

Zudem muss die Führung ein klares Ziel und eine Cyber-Security-Strategie definieren, die dann entsprechend umzusetzen ist. Aber auch Fachabteilungen sind in der Pflicht. Die IT weiß selten, welche Applikationen geschäftskritisch sind. Dieses Wissen liegt in den Fachabteilungen. Alle beteiligten müssen zusammen definieren, welche Systeme kritisch sind und wie diese besser abgesichert werden können.

Rechtliche Auswirkungen von Cyber-Risiken verstehen

Im zweiten Prinzip geht es vor allem um das Thema Haftung. Verschiedene Vorschriften, Gesetze oder Versicherer schreiben Unternehmen vor, wie sie sich bei Cybervorfällen zu verhalten haben. Es geht zum einen darum, wann ein Vorfall gemeldet werden muss, aber auch darum, ob die Führung alles getan hat, um Angriffe zu verhindern bzw. abzumildern. Hier wird es interessant. In Australien gibt es das Beispiel der Medibank, einem Krankenversicherer, dem knapp 10 Millionen Kundendaten bei einem Angriff abhandengekommen sind. Es läuft eine Klage, bei der mehrere Anwaltskanzleien auf Schadensersatz klagen.

Unternehmen müssen Systeme nach dem „Stand der Technik“ absichern. Da dies ein juristischer Begriff ist, stellt sich immer die Frage, was eigentlich der Stand der Technik ist. Hier kommen dann verschiedenste Standards wie der BSI-Grundschutz, die ISO oder CIS-Controls als Referenz zum Einsatz. Unternehmen sollten sich informieren, welche Pflichten aus juristischer Sicht existieren und welche Maßnahmen im Unternehmen zwingend umzusetzen sind, damit keine Fahrlässigkeit unterstellt werden kann.

Zugang zu Cyber-Sicherheitsexpertise sowie regelmäßigen Austausch sicherstellen

Oftmals ist in der Unternehmensleitung das Fachwissen für IT-Sicherheit nicht oder nur teilweise vorhanden. Gleichzeitig ändert sich die Bedrohungslage häufig und man muss gesteckte Ziele kontinuierlich prüfen und ggf. anpassen. Das Handbuch möchte mit diesem Prinzip vor allem sicherstellen, dass ein kontinuierlicher Austausch zu Sicherheitsthemen stattfindet, um das Bewusstsein für das Thema zu verstärken.

Gleichzeitig kann darüber nachgedacht werden, die Geschäftsführung oder das Management gezielt mit Expertise zu verstärken. Das Schaffen von Vorstandsposten oder Stabsstellen ist hier denkbar. Auch der Austausch mit anderen Unternehmen der Branche, aber auch externen Fachkräften ist sinnvoll und denkbar.

Prinzipien 4 & 5 des Handbuchs

„Umsetzung geeigneter Rahmenbedingungen sowie Ressourcen für das Cyber-Risikomanagement sicherstellen“ sowie **„Risikoanalyse erstellen sowie Definition von Risikobereitschaft in Abhängigkeit von Geschäftszielen und -strategien formulieren“**

Während sich Prinzipien 1, 2 und 3 dieses Handbuchs darauf konzentrieren, was die Unternehmensleitung selbst tun sollte, fokussieren sich die Prinzipien 4 und 5 eher darauf, was die Unternehmensleitung vom Management erwarten sollte. Damit die Unternehmensleitung wirksam ihre Aufsichtspflicht ausüben kann, ist es wichtig, dass sie die Verantwortlichkeiten des Managements im Hinblick auf die Cyber-Sicherheit der Organisation vollständig versteht.

Wie in Prinzip 1 dargelegt sollte sich die Unternehmensleitung vergewissern, dass das Management einen angemessenen unternehmensweiten Ansatz für die Cyber-Sicherheit verfolgt. Gleichzeitig sollte klar kommuniziert werden, dass die Erfüllung der regulatorischen Anforderungen nicht zwangsläufig bedeutet, dass das Unternehmen sicher ist.

Daher sollte ein geeigneter Rahmen für die dynamische Struktur des Unternehmens gewählt werden, um die von der Unternehmensleitung und dem Management festgelegte Risikobereitschaft zu erfüllen.

Unternehmensübergreifende Zusammenarbeit und den Austausch von Best Practice fördern

Das letzte Prinzip empfiehlt den Austausch und die Zusammenarbeit mit anderen Unternehmen in der eigenen oder fremden Branche. Dies kann insbesondere durch folgende Initiativen gefördert werden.

Wichtige Überlegungen für die Unternehmensleitung:

- Entwicklung einer 360-Grad-Sicht auf die Risiken und die Widerstandsfähigkeit des Unternehmens, um als sozial verantwortliche Partei in dem breiteren Umfeld, in dem das Unternehmen tätig ist, zu agieren.
- Aufbau von Peer-Netzwerken (beispielsweise in den Erfahrungs- und Expertenkreisen der Allianz für Cyber-Sicherheit) einschließlich anderer Mitglieder von Unternehmensleitungen zum Austausch bewährter Governance-Praktiken über institutionelle Grenzen hinweg.
- Sicherstellen, dass das Management Pläne für eine effektive Zusammenarbeit, insbesondere mit dem öffentlichen Sektor, zur Verbesserung der Cyber-Resilienz hat.
- Sicherstellen, dass das Management die Risiken berücksichtigt, die sich aus den breiteren Verbindungen der Branche ergeben (z. B. Dritte, Anbieter und Partner).

Fazit

Mit dem Handbuch zum „Management von Cyber-Risiken“ für die Unternehmensleitung gibt es einen sehr guten Leitfaden, der einer Unternehmensleitung ermöglicht, einen umfassenden Überblick über die notwendigen Schritte im Umgang mit Cyber-Risiken zu erhalten. Begleitend zu dem Handbuch gibt es noch ein sogenanntes Toolkit, das konkrete Handlungsempfehlungen und Begleitmaterial zur Verfügung stellt.

Wir sind überzeugt davon, dass Cyber-Sicherheit mehr in den Fokus der Unternehmensleitung rücken muss. Dadurch kann das nötige Bewusstsein geschaffen werden, die richtigen Maßnahmen für das Unternehmen auszuwählen. Zu oft erleben wir bei unseren Kunden, dass zahlreiche Tools eingeführt werden, aber die wirklichen Basics nicht berücksichtigt werden. Das möchten wir ändern und bieten dabei auch gerne unsere Hilfe an.

TEAL
ALWAYS CHALLENGING IT

Die nächsten Schritte

Die konsequente Einbindung von Cyber-Sicherheit in das unternehmensweite Risikomanagement ist heute kein „Nice-to-have“ mehr, sondern Pflichtaufgabe für jede Unternehmensleitung. Das vom BSI veröffentlichte Handbuch zeigt eindrucksvoll, worauf es dabei ankommt und warum punktuelle Maßnahmen, einzelne Tools oder Projektinseln nicht ausreichen. Entscheidend ist, dass Sicherheit als strategisches Ziel im Unternehmen verankert wird und IT wie Management an einem Strang ziehen.

Als erfahrenes IT-Security-Consulting-Unternehmen unterstützt **Teal Technology Consulting GmbH** dich gezielt dabei, diesen strategischen Wandel umzusetzen. Wir helfen dir, Schwachstellen in deiner Infrastruktur zu identifizieren, Prioritäten zu setzen und praxisnahe Maßnahmen zu entwickeln, die sich auch in deinem Betrieb umsetzen lassen. Unsere Ansätze basieren auf etablierten Standards wie BSI, CIS oder ISO und auf dem Verständnis, dass Sicherheit immer auch ein Führungs- und Kommunikationsthema ist.

Vereinbare jetzt ein kostenloses 30-minütiges Beratungsgespräch, um zu erfahren:

- ✓ wie du deine Cyber-Security-Strategie ganzheitlich bewertest,
- ✓ welche Maßnahmen wirklich Wirkung zeigen,
- ✓ und wie du deine IT-Umgebung nachhaltig absicherst, jenseits von bloßen Tools.

Nutze die Chance, fundiertes Fachwissen mit klarer Handlungsempfehlung zu verbinden und deine Organisation resilient gegen die Bedrohungen von morgen aufzustellen.

BERATUNGSGESPRÄCH VEREINBAREN

TEAL
ALWAYS CHALLENGING IT

About TEAL

Teal Technology Consulting GmbH ist Ihr Trusted Advisor in allen Fragen rund um die Informationssicherheit – sowohl on-premises als auch in der Cloud. Unsere gesammelte Erfahrung und unser Know-how im Bereich Microsoft-Infrastruktur, Active Directory-Sicherheit und Microsoft Entra ID setzen wir gezielt ein, um moderne hybride und Cloud-basierte Umgebungen sicher zu gestalten.

Neben kundenspezifischer Projektumsetzung bieten wir auch spezialisierte Sicherheitslösungen an. Unser Ziel ist es, kontinuierlich die Sicherheit in Unternehmensumgebungen zu erhöhen, unabhängig davon, ob sie lokal, hybrid oder vollständig in der Cloud betrieben werden.

CANYON · KIRCHHOFF AUTOMOTIVE · AWO Karlsruhe gemeinnützige GmbH · ivi · OTTO CHEMIE Dichtstoffe • Klebstoffe

Mit einem engagierten Team aus Security-Experten arbeiten wir daran, aktuelle Sicherheitsherausforderungen zu bewältigen und präventive Maßnahmen zu implementieren.

- IT-Security Made in Germany **seit 2017**
- **150 Jahre Consulting-Erfahrung** garantieren höchste Qualität
- Über **50 zufriedene** Konzern- und Mittelstands-**Kunden**
- Mehr als **250.000 geschützte Identitäten & IT-Assets**
- **ISMS** nach globalen Standards
- Langfristige **Partnerschaften** für eine vertrauensvolle Zusammenarbeit