Aufbau eines Managementsystems für Informationssicherheit (ISMS)

Systematisch – Zielgerichtet – Risikobasiert – Effizient – Verbessernd

Herausforderung / Ausgangslage:

Die Sicherheitslage ist branchenübergreifend angespannt. Die **Gefährdungslage** ist **hoch** und die Anzahl möglicher Bedrohungen nimmt weiter zu.

Ebenso wächst das Volumen und die Qualität der Angriffe, auf die Informationssicherheit von Unternehmen. Aufgrund des rentablen neuen und **kriminellen Geschäftsmodells** ist eine deutliche **Professionalisierung** zu erkennen.

Es werden immer mehr schwerwiegende Datendiebstähle und Ausfälle von IT-Systemen als Folge von Cyberangriffen gemeldet. Die **wirtschaftlichen Schäden** sind branchenübergreifend teilweise sehr hoch bzw. **existenzbedrohend**.

Beispiele für Sicherheitsvorfälle:

- **Autozulieferer,** Sitz: Hannover, August 2022, knapp acht Gigabyte sensible Daten gestohlen
- **Versorger , Sitz:** Hochsauerland**,** September 2023, Ausfall, Einschränkung Dienstleistungen
- **IT-Dienstleister,** Sitz: Dortmund, März 2023, Systeme / Infrastruktur gestört
- **Bau- und Maschinenbauunternehmen**, Sitz: Kelsterbach, November 2023, Einschränkung der Infrastruktur mit weltweitem Impact

Der **Gesetzgeber** hat auf solche **Bedrohungen reagiert** und nimmt mehr **Einfluss** auf **Unternehmen,** um das Informationssicherheitsniveau in der Wirtschaft und öffentlichen Raum anzuheben. Viele Verbände reagieren auf diese Entwicklung und bringen ihrerseits branchenspezifische Standards auf den Markt.

Beispiele für regulatorische Rahmen, Gesetze und Anforderungen:

- DSGVO
- NIS2
- IT-Sicherheitsgesetz (UBI)
- KRITIS
- B3S (Branchenstandard)
- TISAX (Bereich Automotive)

Zu der allgemein angespannten Sicherheitslage und existierenden Vorgaben können noch eine Reihe von individuellen Anforderungen hinzukommen.

Dazu gehören:

- Kenntnis und Berücksichtigung der verbundenen Stakeholder und deren Anforderungen
- Individuell geltende gesetzliche Anforderungen
- Obliegenheitspflichten aus Versicherungen
- Vertragliche Vereinbarungen und Verpflichtungen
- Auskunftsanfragen und Auditierungsrecht von Auftraggebern und Behörden

Nahezu alle Anforderungen erfordern die Kenntnis der eigenen individuellen Risiken, sowie definierte Methoden für den Umgang mit diesen Risiken.

Darüber hinaus wird eine Informationssicherheitsstrategie und – damit verbunden – die Kenntnis der eigenen Sicherheitsziele vorausgesetzt.

Wie kann man trotz des Blumenstraußes an Anforderungen und trotz der komplexen Themenvielfalt den Überblick behalten, seine Ziele erreichen und Risiken bestmöglich mindern, ohne Aufwände und Kosten ausufern zu lassen?

Hierfür bietet sich unser strukturiertes Vorgehen zum Aufbau eines ISMS nach ISO 27001 an.

Information Security

Unser Angebot

Wir gehen mit einem bewährten und gestuften **Standardvorgehen** vor. Dieses beinhaltet:

- **Standardisierte Bestandsaufnahmen** (Quick Checks / Reifegradeanalysen) - Basispaket zur Herleitung einer Aufwands- und Kostenabschätzung
- **Standardisierte Aufnahme von Werten -** Erfassung aller relevanten Assets, von Prozessen über IT-Systeme und Anwendungen bis hin zu Personal
- **Transparente Informationssicherheitsrisiken -** Unterstützung beim Risikomanagement von der Risikoidentifizierung bis hin zur Risikobehandlung
- **Bewährte Blaupausen für Methodik und Dokumentation -** Individuell auf die Unternehmensbedürfnisse anpassbare Vorlagen in Kombination mit unseren Erfahrungswerten
- **Gezielte Adressierung der geschäftsbedrohenden Risiken -** Schaffung einer Transparenz über die geschäftskritischen Prozesse, Informationen und deren Risiken, sowie die Planung und Priorisierung zur effektiven Maßnahmenumsetzung

Bei Bedarf stellen wir außerdem unsere Expertise als externer Informationssicherheitsbeauftragter (ISB/CISO) zur Verfügung.

Ihr Nutzen

Unser standardisiertes Vorgehen ermöglicht eine Reihe von Vorteilen:

- **Quick Wins** durch gestuftes Vorgehen
- Rasche **Anhebung des Informationssicherheitsniveaus** durch gezielte und effiziente Maßnahmen
- **Funktionierende Abläufe / Prozesse**
- **Klar definierte Zuständigkeiten**
- **Nachweisbarkeit** Dritten gegenüber
- Schaffen einer **Basis zur Erfüllung weiterer gesetzlicher und regulatorischer Anforderungen** (z.B. TISAX, NIS2) für ein Normen-konformes Managementsystem (ISMS)
- Aufbau von **Know-how**

Warum Controlware?

Die Controlware GmbH ist einer der führenden unabhängigen Systemintegratoren und Managed Service Providern. Das 1980 gegründete Unternehmen entwickelt, implementiert und betreibt anspruchsvolle IT-Lösungen für die Cloud-, Data Center-, Enterprise- und Campus-Umgebungen seiner Kunden mit nachgewiesener Servicequalität mit dem ISO 27001-zertifiziertem Customer Service Center.

Unsere Berater kommen aus allen Regionen in Deutschland und verfügen über langjährige Erfahrung und umfassende Skills in allen genannten GRC-Bereichen.

Durch unser branchen- und technologieübergreifendes Know-how, insbesondere auch in technischen Bereichen, können wir praxisnahe und passende Konzepte erstellen. Das können wir mit zahlreichen erfolgreichen Projekten und zufriedenen Kunden belegen.

Weitere Informationen und Details entnehmen Sie bitte der zugehörigen Leistungsbeschreibung.

Zentrale

Controlware GmbH
Waldstraße 92
63128 Dietzenbach
Tel. +49 6074 858-00
Fax +49 6074 858-108

info@controlware.de
www.controlware.de
blog.controlware.de

Besuchen Sie uns auf: