DataGuard

CHECKLISTE

CYBERSECURITY-STRATEGIE FÜR KMU

5 TIPPS, WIE KMU MITHILFE DER ISO 27001 IHRE CYBERSICHERHEITS-STRATEGIE VERBESSERN KÖNNEN

Cybersicherheit ist eines der am häufigsten diskutierten Themen in kleinen bis mittelgroßen Unternehmen (KMU). Hier die Gründe:

- Die Entwicklung einer Strategie zum Schutz vor Cyberattacken kann Unternehmen, die noch am Anfang stehen, zu teuer erscheinen.

- Unternehmensinhaber müssen viel Zeit und Aufmerksamkeit auf das Tagesgeschäft verwenden. Da bleibt oft keine Zeit, sich mit Cybersicherheitsstrategien zu beschäftigen.

Die gute Nachricht ist, dass die ISO 27001 Ihnen helfen kann, Cyberbedrohungen auf effektive Art anzugehen.

Und mit einer ISO 27001-Zertifizierung zeigen Sie Kunden, Geschäftspartnern, Behörden und Investoren gegenüber, dass Ihr Unternehmen sich für Datenschutz und Informationssicherheit einsetzt.

Die folgende Checkliste soll Ihnen dabei helfen, auf eine ISO-27001-Zertifizierung hinzuarbeiten und sie zu einem wichtigen Bestandteil Ihrer Cybersicherheitsstrategie zu machen.

CHECKLISTE: 5 TIPPS, WIE KMU MITHILFE DER ISO 27001 IHRE CYBERSICHERHEITSSTRATEGIE VERBESSERN KÖNNEN

Der erste Schritt ist der Aufbau eines soliden Informationssicherheits-Managementsystems (ISMS). Ihr ISMS ist das übergreifende Framework für die Cybersicherheitsstrategie Ihres Unternehmens. Es umfasst Richtlinien, Verfahren und Systeme zum Schutz der in Ihrem Unternehmen gespeicherten Daten.

Nach der Einrichtung Ihres ISMS können Sie unternehmensweit Maßnahmen umsetzen, um Ihre Sicherheitsprozesse zu optimieren.

1. GAP-ANALYSE DURCHFÜHREN

Eine Gap-Analyse macht deutlich, welche Schritte nötig sind, um die Zertifizierung zu erhalten. Sie betrachten dabei Ihre aktuelle Informationssicherheitsstrategie und prüfen sie auf ISO 27001-Compliance. Hier die Schritte:

- Das Team unter Leitung eines Projektmanagers zusammenbringen
- Projektziele, Zukunftsvisionen und den gewünschten Zeitrahmen festlegen
- Zu beteiligende Stakeholder identifizieren
- Rollen und Verantwortungsbereiche im Team festlegen
- Ermitteln, wie Ihr Unternehmen in Bezug auf die Umsetzung der relevanten Controls abschneidet
- Einen Implementierungsplan zum Schließen der Lücken entwerfen

2. EIN SOLIDES ASSET-MANAGEMENT AUFBAUEN

Asset-Management hat üblicherweise zwei Elemente: die Ermittlung von Risiken, Bedrohungen und Schwachstellen und (bei Bedarf) die Durchführung einer Risikobewertung.
Sie finden heraus, welche Assets in Ihrem Unternehmen vorhanden sind, wer für sie zuständig ist und wie mit ihnen umzugehen ist. Hier die erforderlichen Maßnahmen:

- Eine Liste der materiellen und immateriellen Vermögenswerte des Unternehmens erstellen
- Festlegen, wie diese Assets geschützt, verwaltet und überwacht werden können

3. RISIKOMANAGEMENT-STRATEGIE PRÜFEN

Risikomanagement bezeichnet die Analyse und Bewertung potenzieller Bedrohungen der Datensicherheit. Anschließend wird eine Rangordnung erstellt, um die schwerwiegendsten Probleme zuerst anzugehen. Je früher Sie Bedrohungen ermitteln, desto schneller können Sie darauf reagieren und desto geringer sind die Auswirkungen bei einem Sicherheitsvorfall. Risikomanagement umfasst Folgendes:

- Regeln zum Ermitteln von Risiken sowie das akzeptable Risikoniveau festlegen
- Die Auswirkungen auf das Unternehmen im Falle eines Risikoeintritts definieren
- Die Wahrscheinlichkeit des Risikoeintritts ermitteln

4. PROZESSE UND RICHTLINIEN DOKUMENTIEREN

Eine sorgfältige Dokumentation der Abläufe ist wichtig, um eine zuverlässige Referenz für Ihre Mitarbeiter bereitzustellen. So kann die vorhandene Belegschaft einfacher auf etablierte Verfahren und Richtlinien zugreifen, und neue Mitarbeiter machen sich schneller damit vertraut. Hier die Schritte:

- Den Umfang der Implementierung umreißen
- Informationssicherheitsrichtlinien auf Grundlage potenzieller Ergebnisse erstellen
- Dokumente verfassen, in denen die Unternehmensrichtlinien zu bestimmten Themen festgehalten werden, z. B. der Umgang mit Mobilgeräten
- Weitere Dokumente zu anderen Themen erstellen (z. B. Passwörter, Software, Hardware) und zugehörige Maßnahmen auflisten
- Controls und vorgeschriebene Prozesse implementieren

5. INTERNE UND EXTERNE AUDITS DURCHFÜHREN

Interne und externe Audits zeigen Bedrohungen von innerhalb und außerhalb des Unternehmens auf. Je früher diese erkannt werden, desto eher lassen sich Cyberattacken vermeiden.

Mit regelmäßigen Audits sorgen Sie dafür, dass Mitarbeiter sich an Sicherheitsprotokolle halten und potenzielle Probleme oder Vorfälle gemeldet werden. Hier die wichtigen Maßnahmen in Bezug auf Audits:

- Ermitteln, welche und wie viele Vorfälle aufgetreten sind
- Prüfen, ob alle internen Audits durchgeführt wurden
- Anhand der Ergebnisse interner Audits entsprechende Maßnahmen ermitteln
- Die Anforderungen zum Erreichen Ihrer ISMS-Ziele festlegen und prüfen sowie deren Einhaltung aufrechterhalten
- Einen Prozess zur Überwachung, Analyse und Bewertung Ihres ISMS etablieren

Die Umsetzung dieser Maßnahmen kann zeitintensiv sein, ist aber ein wichtiger Schritt auf dem Weg zum Erwerb der ISO 27001-Zertifizierung – und Sie schützen Ihr Unternehmen vor Cyberattacken.

DATAGUARD HILFT IHNEN GERN BEI DER ENTWICKLUNG IHRER CYBERSICHERHEITS-STRATEGIE

Wir teilen Best Practices mit Ihnen, geben branchenspezifische Tipps und unterstützen Sie beim Aufbau Ihres ISMS oder der Vorbereitung auf ein externes Audit.

Mit unserer Lösung „Informationssicherheit-as-a-Service" können Sie Ihre Informationssicherheitsstrategie effektiv verwalten und auf die ISO 27001-Zertifizierung hinarbeiten. Außerdem bieten wir Folgendes:

1. **Erfolg bei externen Audits -** Bisher haben alle unsere Kunden externe Informationssicherheitsaudits beim ersten Versuch bestanden.

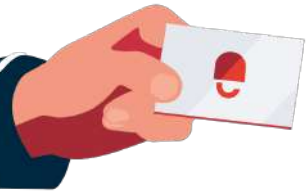
2. **Single Source of Truth -** Durch die Digitalisierung von Prozessen werden manuelle Aufgaben automatisiert und Ihre Informationssicherheitsstrategie übersichtlicher und zugänglicher gestaltet.

3. **Unterstützung beim Erwerb der ISO 27001-Zertifizierung,** die Ihrem Unternehmen **Wettbewerbsvorteile** verschafft

Wenn Sie mehr darüber erfahren möchten, wie sich die die Cybersicherheitsstrategie Ihres Unternehmens mit einer ISO 27001-Zertifizierung optimieren lässt, nehmen Sie gern Kontakt mit uns auf.

Gemeinsam schützen wir Ihr Unternehmen vor aktuellen und neuen Cyberbedrohungen.

→ **Jetzt Erstgespräch buchen**



DataGuard ist ein Compliance-Software-Unternehmen mit Fokus auf Datenschutz und Informationssicherheit. Als einer der europäischen Marktführer im Bereich Compliance-SaaS ermöglicht DataGuard Tausenden KMU und Großunternehmen die unkomplizierte Operationalisierung von Datenschutz (Privacy), Informationssicherheit und Compliance (kurz: „PIC"). Mit seiner Komplettlösung reduziert DataGuard für Unternehmen Zeit und Kosten bei der Einhaltung von Datenschutzgesetzen wie der DSGVO, der Einholung und Verwaltung von Einwilligungen und Präferenzen oder beim Erhalten von Zertifizierungen wie der ISO 27001. So können sich Kunden auf ihr Kerngeschäft konzentrieren, Mehrwert durch Vertrauen und Compliance schaffen und gleichzeitig Risiken minimieren. DataGuard hat Standorte in München, Berlin, London und Wien.

Jetzt Termin vereinbaren, um über Ihre Herausforderungen zu sprechen und erste Schritte zu definieren:

Erstgespräch buchen

Weiterführende Ressourcen:

→ **4 Maßnahmen für die ISO 27001-Zertifizierung**

→ **ISO 27001 - Informationssicherheit sichtbar machen**

→ **Die neue ISO 27001:2022 – das ändert sich**

dataguard.de kontakt@dataguard.de +49 89 452 459-900

DataGuard