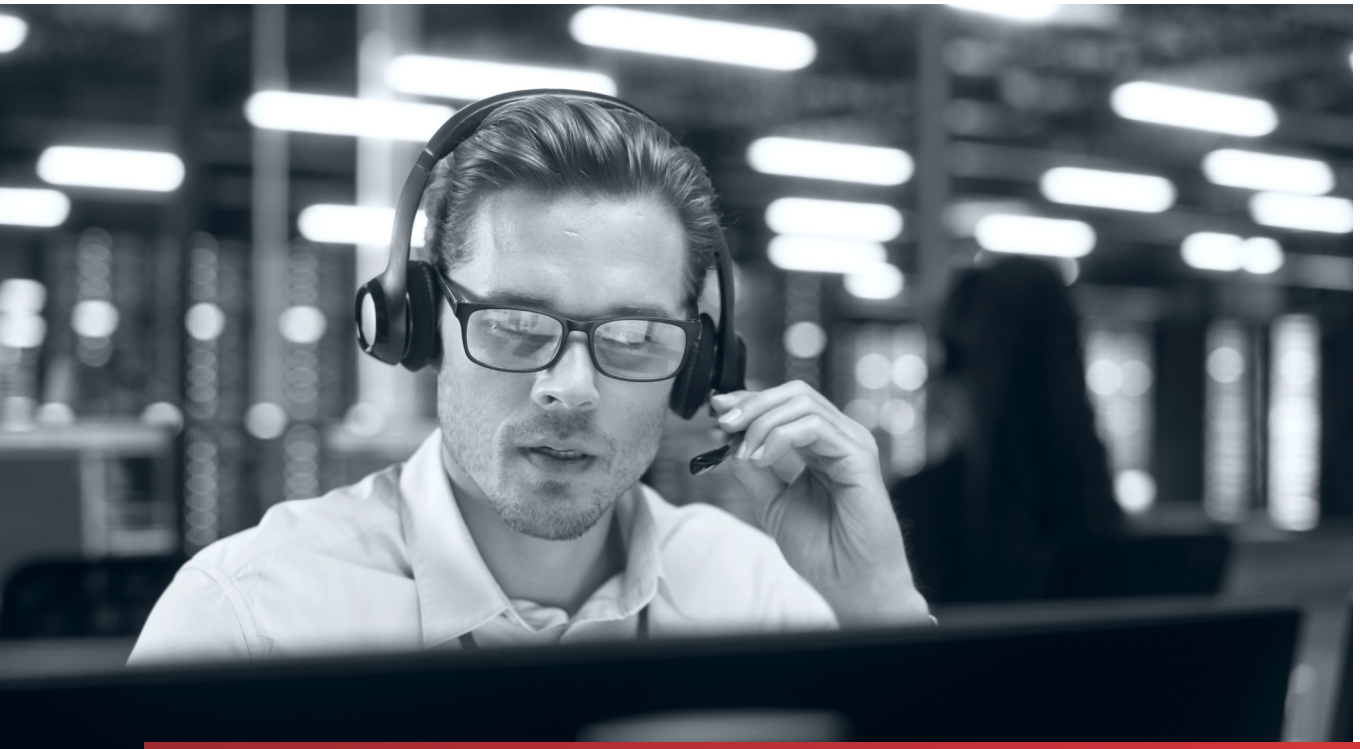
DataGuard



CHECKLISTE

NIS2 CHECKLISTE FÜR IT-LEITER:

IN 10 SCHRITTEN ZUR CYBERRESILIENZ UND COMPLIANCE

In 10 Schritten zur NIS2 Compliance - Wie Sie die IT Ihres Unternehmens für eine sichere Zukunft rüsten

NIS2 kommt. Für viele Unternehmen bedeutet das eine große Investition in die Cybersicherheit. Sichern Sie sich die Unterstützung der Führungsebene und zeigen Sie auf, wie proaktives Handeln nicht nur die Ressourcen schützt, sondern Ihr Unternehmen von der Konkurrenz abhebt.

Mit einem Informationssicherheits-Managementsystem (ISMS) nach ISO 27001 sind Sie für die Anforderungen von NIS2 bestens gerüstet - das haben führende NIS2-Regulatoren bestätigt. Bereiten Sie Ihre Organisation mit dieser Checkliste optimal vor.

1. Überprüfen Sie, ob Ihr Unternehmen in den Anwendungsbereich von NIS2 fällt

Die betroffenen Wirtschaftssektoren in der EU wurden in NIS2 deutlich ausgeweitet. Überprüfen Sie, ob Ihr Unternehmen einem dieser Sektoren zugerechnet werden könnte. Manchmal ist die Zuordnung noch nicht eindeutig definiert - sprechen Sie mit einem Berater. Beachten Sie auch die Schwellenwerte für die Unternehmensgröße: generell sind nur mittlere und große Unternehmen betroffen, es gibt jedoch auch Ausnahmen. Hier eine Übersicht der wesentlichen und wichtigen Sektoren:

Wesentliche Sektoren	Wichtige Sektoren
• Energie • Verkehr • Bankwesen • Finanzmarktinfrastruktur • Gesundheitswesen • Trinkwasser • Abwasser • Digitale Infrastruktur • Verwaltung von IKT-Diensten • Öffentliche Verwaltung • Weltraum	• Post- und Kurierdienste • Abfallbewirtschaftung • Chemische Stoffe • Lebensmittel • Verarbeitendes Gewerbe/ Herstellung von Waren • Anbieter digitaler Dienste • Forschungseinrichtungen

2. Stellen Sie sicher, dass Sie über angemessene Sicherheitsmaßnahmen verfügen

Kontrollieren Sie Ihre vorhandenen Maßnahmen und Prozesse zur Informationssicherheit und BCM. Sind Ihre Netzwerk- und Informationssysteme ausreichend vor Cyberbedrohungen geschützt?

3. Identifizieren Sie kritische Infrastrukturen und bewerten Sie deren Sicherheitsniveau

Ihre kritischen Geschäftsprozesse und sensiblen Daten müssen besonders geschützt werden. Haben Sie auch Wiederherstellungspläne nach Angriffen auf Ihre Infrastruktur in der Schublade?

4. Richten Sie Mechanismen zur Erkennung von Cybervorfällen ein

Die durchschnittliche Zeit zur Erkennung und Behandlung eines Datenlecks lag im Jahr 2022 bei 277 Tagen. Gemessen an den Anforderungen, die NIS2 an Organisationen stellt, ist das zu langsam. Treffen Sie geeignete Vorkehrungen, um Cyberbedrohungen schnell zu erkennen - in allen Systemen.

5. Minimieren Sie Risiken und stellen Sie Incident Response-Pläne auf

Das Risikomanagement bildet den Kern eines ISMS und steht somit auch in der NIS2-Richtlinie im Fokus. Geeignete Strategien zur Bewältigung von Sicherheitsvorfällen gehören dazu. Außerdem sorgen Sie durch ein geeignetes Riskmanagement dafür, potenzielle Gefahren frühzeitig zu identifizieren, zu bewerten und zu behandeln, sodass Ihr Unternehmen Cybergefahren effektiv behandeln kann.

6. Legen Sie klare Zuständigkeiten fest

Definieren Sie Rollen und Verantwortlichkeiten für Cybersicherheit, Informationssicherheit und Business Continuity-Management. Die ISO 27001 verlangt, dass ein Mitarbeiter permanent als Ansprechpartner für diese Themen zur Verfügung steht.

7. Schulen Sie alle Mitarbeiter regelmäßig

Sensibilisieren Sie für korrekte Verhaltensweisen im Umgang mit Cybergefahren. Das schließt die Führungsebene mit ein: Geschäftsführer können durch NIS2 persönlich haftbar gemacht werden. Behalten Sie aktuelle Entwicklungen im Auge - die Schulungen müssen mit Veränderungen in der Risikolandschaft aktualisiert werden.

8. Vereinfachen Sie den Prozess der Vorfallsmeldung

Für die Meldung von Sicherheitsvorfällen gelten in NIS2 sehr kurze Fristen. Schwerwiegende Ereignisse müssen innerhalb von 24 Stunden an das BBK (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe) gemeldet werden. Stellen Sie sicher, dass alle zuständigen Mitarbeiter die notwendigen Schritte kennen.

9. Überprüfen Sie Ihre Sicherheitsmaßnahmen kontinuierlich

Der Betrieb eines ISMS nach ISO 27001-Standard ist ein fortlaufender Prozess (PDCA Zyklus). Ihre Organisation und deren spezifische Risiken befinden sich permanent im Wandel - daran muss Ihr ISMS laufend angepasst werden. Ebenso ist es mit der NIS2. Auch hier genügt nicht die einmalige Compliance, sondern eine stetige Überwachung der Sicherheitsmaßnahmen. Die ISO 27001 Zertifizierung deckt dabei große Teile der NIS2 Compliance Journey ab.

10. Informieren Sie sich über aktuelle Entwicklungen im Bereich der Cybersicherheit

Wenn neue Technologien auf den Markt kommen, können gänzlich neue Bedrohungen entstehen. Halten Sie sich über aktuelle Entwicklungen auf dem Laufenden und schätzen Sie ab, welche Auswirkungen diese auf Ihr Unternehmen haben könnten.

Wie geht es weiter?

Bis zum **17. Oktober 2024** haben die EU-Mitgliedstaaten Zeit, die NIS2-Richtlinie in nationales Gesetz zu überführen. Doch auch wenn sich dies noch nach genug Zeit, insbesondere auf Unternehmensseite anhört, sollte die Umsetzungsdauer auf keinen Fall unterschätzt werden.

Oft ziehen sich Umsetzungsprozesse in Unternehmen unvorhergesehen in die Länge. Holen Sie sich daher frühzeitig alle relevanten Stakeholder und vor allem das Management mit ins Boot, um unnötige Verzögerungen zu vermeiden. Bereiten Sie Ihr Unternehmen mit einer **ISO 27001 Zertifizierung** bereits jetzt darauf vor, um kosteneffizient vorzugehen und sich einen Wettbewerbsvorteil zu verschaffen.

DataGuard kann Sie auf dem gesamten Weg begleiten. Wir führen mit Ihnen eine Gap-Analyse durch, um Ihre individuellen Lücken zu den NIS2-Anforderungen zu identifizieren. Anschließend stellen wir gemeinsam Ihre Roadmap zur Compliance auf. Egal ob Sie bereits nach ISO 27001 zertifiziert sind oder nicht, wir helfen Ihnen die fehlenden Maßnahmen zur NIS2 Compliance umzusetzen!

Vereinbaren Sie jetzt einen Termin!

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:

→ **NIS2 Compliance erreichen: Ihr Weg zu mehr Cybersicherheit**

→ **NIS2 Guide für CEOs: Auf was sich Unternehmen bereits heute einstellen sollten**

→ **Leitfaden: In 10 Schritten zur Einhaltung der NIS2-Richtlinie**

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

DataGuard