DataGuard

NIS2-RICHTLINIE

EIN LEITFADEN ZUR EINHALTUNG

FÜR EU-UNTERNEHMEN

SCHRITT 1

Prüfen Sie, ob Ihr Unternehmen von der NIS2-Richtlinie betroffen ist

Stellen Sie fest, ob Ihr Unternehmen in den von der NIS2 definierten Sektoren tätig ist.

Betrachten Sie den geografischen Anwendungsbereich und prüfen Sie, ob Ihr Unternehmen dort hineinfällt.

SCHRITT 2

Verschaffen Sie sich einen Überblick über die Anforderungen und Strafen der NIS2

Damit die Einhaltung der Richtlinie ernstgenommen wird, sollte die Geschäftsführung auf die zwei Sanktionstypen der NIS2 aufmerksam gemacht werden:

1. Hohe und vordefinierte Bußgelder
2. Haftung von Geschäftsführern sowie C-Level-Führungskräften innerhalb des Unternehmens

SCHRITT 3

Informieren und schulen Sie Ihr Management in Sachen Cybersicherheits-Risikomanagement

Vergewissern Sie sich, dass sich Ihre Führungsebene der Cybersicherheitsrisiken bewusst ist und weiß, wie damit umzugehen ist.

Führen Sie regelmäßige Schulungen durch und stellen Sie Ressourcen zur Sensibilisierung zur Verfügung.

Lassen Sie außerdem spezifische Cybersicherheits-Risikomaßnahmen inkl. Rechenschaftspflicht bei Nichteinhaltung genehmigen, deren Umsetzung Sie streng überwachen.

SCHRITT 4

Planen und budgetieren Sie entsprechende Ausgaben

Ermitteln Sie die Ausgaben, die Sie für die Einhaltung der NIS2-Richtlinie benötigen, und planen Sie ein entsprechendes Budget dafür ein.

SCHRITT 5

Überprüfen Sie die 10 von der NIS2 vorgeschriebenen Maßnahmen zum Management von Cybersicherheitsrisiken

Überprüfen Sie die Umsetzung der 10 geforderten Maßnahmen zum Risikomanagement aus der NIS2.

Bewerten Sie anschließend wie gut Ihre aktuellen Richtlinien und Verfahren zur Cybersicherheit sind und ob sie mit den Maßnahmen aus der NIS2 übereinstimmen.

SCHRITT 6

Bewerten Sie Ihre Lieferketten-Sicherheit

Analysieren Sie Ihre Lieferketten in Bezug auf Cybersicherheitsrisiken.

Stellen Sie außerdem sicher, dass auch Lieferanten die NIS2-Richtlinie einhalten.

SCHRITT 7

Vereinfachen Sie den Prozess der Vorfallsmeldung

Optimieren Sie Ihre Meldeverfahren für Zwischenfälle.

Stellen Sie sicher, dass alle zuständigen Mitarbeitenden die richtigen Meldekanäle kennen.

SCHRITT 8

Entwickeln Sie einen Plan zur Geschäftskontinuität und zum Krisenmanagement

Erstellen Sie einen Plan zur Aufrechterhaltung des Geschäftsbetriebs (Business Continuity Plan), der die NIS2-Ansprüche berücksichtigt.

Stellen Sie sicher, dass Ihr Plan auch Verfahren für das Krisenmanagement enthält.

SCHRITT 9

Implementieren Sie ein Informationssicherheits-Managementsystem (ISMS) unter Berücksichtigung der NIS2-Kriterien

Stellen Sie bei der Umsetzung des ISMS sicher, dass es den Anforderungen Ihrer Organisation entspricht und sich nach den Vorgaben und Maßnahmen der ISO 27001 richtet.

SCHRITT 10

Fördern Sie sichere Entwicklungsmethoden

Führen Sie in Ihrer Organisation sichere Entwicklungsmethoden ein, um die NIS2 zu erfüllen.

Stellen Sie sicher, dass Mitarbeitende sich der Bedeutung dieser Praktiken bewusst sind.

Beachten Sie:

Die Einhaltung der NIS2 ist für EU-Unternehmen von entscheidender Bedeutung. Mit dieser Schritt-für-Schritt-Anleitung stellen Sie sicher, dass Sie die entsprechenden Anforderungen einhalten.