Höchste Zeit zur Ergreifung von Maßnahmen

Die NIS2-Richtlinie für Netz- und Informationssicherheit ist auch für Coburger Unternehmen relevant

„Der nächste Informationssicherheitsvorfall ist nur eine Frage der Zeit", warnt Markus Vollmuth, Informationssicherheitsberater und ISO 27001 Lead Auditor bei der atarax Unternehmensgruppe.

Das Bundesministerium für Sicherheit in der Informationstechnik (BSI) spricht im aktuellen Berichtszeitraum von einer angespannten bis kritischen Lage in Bezug auf die IT-Sicherheit in Deutschland. Kleine und mittlere Unternehmen (KMU) wurden überproportional häufig angegriffen. „Jedes Unternehmen sollte daher alle denkbaren Maßnahmen ergreifen, um sich gegen Cyber-Bedrohungen zu schützen", rät IHK-Referent Rico Seyd. In vielen Industriesektoren ist das nicht nur sinnvoll, sondern sogar gesetzlich verpflichtend – Stichwort: NIS2.

Die NIS-2-Richtlinie ist am 27. Dezember 2022 im Amtsblatt der Europäischen Union veröffentlicht worden und am 16. Januar 2023 in Kraft getreten. Bis zum 17. Oktober 2024 muss NIS2 in deutsches Recht umgesetzt werden.

Wer ist von NIS2 betroffen?

Der Anwendungsbereich wurde im Vergleich zur alten NIS-Richtlinie erweitert. Damit sollen bereits Einrichtungen (Unternehmen sowie Behörden) erfasst werden, welche die folgenden Kriterien erfüllen:

1. Zugehörigkeit zu einem von 18 Sektoren/Branchen, unterteilt in „wesentliche Einrichtungen" und „wichtige Einrichtungen"
2. Einordnung als mittlere oder große Einrichtung
   a. mittlere Unternehmen: 50 bis 250 Mitarbeiter, 10 bis 50 Mio. Euro Umsatz, Bilanzsumme kleiner als 43 Mio. Euro
   b. große Unternehmen: mehr als 250 Mitarbeiter, mehr als 50 Mio. Euro Umsatz, Bilanzsumme größer als 43 Mio. Euro
3. Einstufung als „Sonderfall"

Die Coburger Wirtschaft ist geprägt von mittelständischen Unternehmen der Automotive- und Automobilzulieferindustrie, des Maschinenbaus, der Elektrotechnik, der Kunststoffverarbeitung sowie der Möbel- und Spielwarenproduktion. Der Sektor Herstellung bestimmter industrieller Produkte (Medizinprodukte und In-vitro, Datenverarbeitung / Computer, Elektronik, Optik, elektrische Ausrüstung, Maschinenbau, Kraftwagen und Teile, Fahrzeugbau) ist damit hinsichtlich NIS2 von Bedeutung.

Was ist zu tun?

Von NIS2 betroffene Einrichtungen müssen laut Referentenentwurf des NIS2 Umsetzungsgesetzes u. a. folgende Maßnahmen für die Cybersicherheit ergreifen:

- Maßnahmen des Risikomanagements § 30
- Meldepflichten § 31
- Registrierung § 32 und § 33
- Informationsaustausch § 35 und § 36

Im § 30 Risikomanagementmaßnahmen des Referentenentwurfs des NIS2 Umsetzungsgesetzes werden folgende Maßnahmen genannt:

1. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme,
2. Bewältigung von Sicherheitsvorfällen,
3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit,
7. grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit,
8. Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,
9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen,
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Um strategisch gut aufgestellt zu sein, sollten sich Unternehmen konkret Gedanken über ein Informationssicherheitsmanagementsystem (ISMS) machen. Ein ISMS besteht unter anderem aus Richtlinien, Maßnahmen, Prozessen und Tools, mit denen Informationssicherheitsrisiken identifiziert und behandelt werden können. So können Notfall- und Krisenkonzepte, Backup-Strategien und Assessments dabei helfen, das Risiko eines Angriffs zu verringern und, falls es doch zu einem Vorfall kommt, dessen Folgen abzuschwächen.

Kostenloses Webinar

Zum Thema findet am 24. April 2024 von 15 bis 17 Uhr ein kostenloses Web-Seminar unter dem Titel „NIS-2 – Eine neue Richtlinie für Cybersicherheit richtig umsetzen" statt. Mehr Informationen hierzu unter
URL tinyurl.com/nis2-webinar ■

Autoren: Markus Vollmuth und Rico Seyd

Information
tinyurl.com/nis-2-richtlinie

Kontakt
Rico Seyd, Tel.: 09561 7426-46
E-Mail: rico.seyd@coburg.ihk.de