

Risikobeurteilung für den Cyber Resilience Act

Beschreibung

Zu den Hauptanforderungen des Cyber Resilience Act gehört eine Risikobeurteilung. Dies stellt viele Unternehmen vor eine Herausforderung, gerade wenn es um Risiken geht, die sich aus IT/OT-Security Lücken ergeben. Die @-yet IIS unterstützt Sie bei der Durchführung dieser Beurteilung. Wir analysieren mit Ihnen die Zweckbestimmung und die vorhersehbare Nutzung Ihres Produkts unter Berücksichtigung der spezifischen Betriebsumgebung sowie der voraussichtlichen Nutzungsdauer, um alle relevanten Cybersicherheitsrisiken systematisch zu identifizieren.

Vorteile

- IT/OT-Sicherheitslücken minimieren
- Produktsicherheit nachhaltig steigern
- Risikobeurteilung nach CRA umgesetzt

Methodik

- Zweckbestimmung und Nutzung analysieren
- Betriebsumgebung und Lebenszyklus prüfen
- IT/OT-Sicherheitsrisiken identifizieren
- Analyse und Bewertung der identifizierten Risiken



Schnell und richtig reagieren

Sorgfältig ausgearbeitete Notfallpläne und ein Business Continuity Management sind eine sichere Grundlage. Im Notfall unterstützen Sie die Incident Response Teams der @-yet IIS, damit Sie schnell wieder arbeitsfähig werden.



Fachübergreifender Ansatz

Die @-yet IIS betrachtet klassische IT-Security und die Sicherheit in der Automatisierung als einheitlichen Prozess. Alle wichtigen Bereiche der Cybersicherheit von Industrieunternehmen werden so abgedeckt.



Umfassende Prävention

Die @-yet IIS sorgt mit fundierten Schulungsprogrammen für aufmerksame Mitarbeitende, damit der Ernstfall erst gar nicht eintritt. Diese Awareness wird durch professionelle technische Maßnahmen unterstützt.

