SCHULZ
SYSTEMTECHNIK

CHECKLISTE:
CYBERRESILIENZ NACH NIS-2-RICHTLINIE

Im Rahmen der neuen NIS-2-Richtlinie gelten strengere Anforderungen an Unternehmen in verschiedenen Branchen. Unter anderem besteht die Pflicht für Risikoanalysen, Incident-Reportings, Security-Maßnahmen und Kontrollen der Lieferketten.

Mit dieser kompakten Checkliste identifizieren Sie mögliche Sicherheitslücken in Ihrer Produktions-IT. Nutzen Sie die Liste für eine erste Basis-Bewertung und überprüfen Sie, wie gut Ihr Unternehmen auf die Anforderungen der NIS-2-Richtlinie vorbereitet ist.

Grundstruktur & Organisation

- ☐ Ist Ihre IT- und OT-Infrastruktur klar voneinander getrennt (Netzwerksegmentierung)?
- ☐ Sind Zuständigkeiten für Cybersecurity im Unternehmen eindeutig geregelt?
- ☐ Gibt es einen dokumentierten Notfallplan (Disaster-Recovery-Szenarien)?

Systeme & Daten

- ☐ Werden regelmäßig Backups durchgeführt – und auch getestet?
- ☐ Arbeiten kritische Systeme (z. B. Steuerungen, SCADA) im Read-Only-Modus?
- ☐ Sind alle Software- und Firmwarestände aktuell (Patch-Management vorhanden)?

Zugriff & Kontrolle

- ☐ Werden Benutzerrechte regelmäßig überprüft und angepasst?
- ☐ Sind externe Wartungszugänge über VPN abgesichert – mit Logging und Zeitfensterfreigabe?
- ☐ Wird jede externe Verbindung (z. B. via Fernwartung) dokumentiert und gesteuert?

Überwachung & Schulung

- ☐ Gibt es ein Monitoring- und Alarmsystem für IT-/OT-Vorfälle?
- ☐ Werden Mitarbeitende regelmäßig für IT- und Betriebssicherheit sensibilisiert?
- ☐ Wurde ein externer Security-Audit innerhalb der letzten 12 Monate durchgeführt?

Die Empfehlung lautet: Jetzt vorbereiten, statt später haften. Durch die Integration der einzelnen Maßnahmen werden Unternehmen vor wirtschaftlichen Folgen im Fall eines geschützt. Darüber hinaus sichern sie auch Wettbewerbsvorteile in Bezug auf zuverlässigen Datenschutz gegenüber Geschäfts- und Projektpartnern.