Schutz vor Cyberangriffen
für städtische Versorgungsunternehmen

Unterstützung bei der Einhaltung von EU-Richtlinien

Der steigende Automatisierungsgrad vieler Prozesse und die damit einhergehenden Vernetzungen innerhalb eines Unternehmens erhöhen die Komplexität von benötigten Systemen und damit die Anfälligkeit für Cyberangriffe. Aufgrund der steigenden Anzahl von Cyberangriffen, wurden neue regulatorische Vorgaben (EU NIS2) beschlossen, die Unternehmen ein minimales Sicherheitsniveau vorschreiben. Dieses Sicherheitsniveau bezieht sich auf IT- (Information Technology) sowie OT-Systeme (Operational Technology). IT-Systeme dienen der elektronischen Datenverarbeitung und nutzen Standardfunktionen zum Schutz der Integrität und Geheimhaltung. Diese unterscheiden sich maßgeblich von OT-Systemen, welche physische Anlagen steuern und überwachen. Der Fokus des Schutzes liegt dabei auf der Zuverlässigkeit und funktionalen Sicherheit (Safety).

Was sind die Herausforderungen?

- **Gesetzliche Anforderungen,** wie z.B. umfassende technische Risikoanalysen für Produktionsanlagen und der Einsatz von Systemen zur Angriffserkennung.
- **Fehlendes Wissen zu aktuellen unternehmensspezifischen Cyberbedrohungen** und damit eine falsche oder verzögerte Reaktion in den Bereichen IT und OT im Falle eines Angriffs.
- **Keine zentrale Steuerung der OT-Security-Aktivitäten**, wodurch Sicherheitsmaßnahmen nicht vollständig oder effizient umgesetzt werden und die Produktionsanlagen nicht ausreichend geschützt sind.
- **Unzureichende Kenntnis des aktuellen Sicherheitsniveaus** und über aktuell umgesetzte Sicherheitsmaßnahmen, wodurch Lücken in Ihrer Sicherheitsarchitektur unerkannt bleiben.

EU NIS2 (Network and Information Systems Directive)

NIS2 ist eine europäische Richtlinie zur Stärkung der Widerstandsfähigkeit kritischer Infrastrukturen gegenüber Cyberangriffen. Dabei werden Unternehmen aufgefordert, ein definiertes Sicherheitsniveau zu garantieren.

- Betroffene Unternehmen und Organisationen müssen angemessene Maßnahmen in Bereichen wie Cyber-Risikomanagement, Sicherheit in der Lieferkette und Business Continuity Management ergreifen und Berichterstattung an die Behörden sicherstellen.
- Der Handlungsdruck für betroffene Organisationen wird durch die Erhöhung von Obergrenzen für Bußgelder und die persönliche Haftbarkeit von Mitgliedern der Leitungsebenen dramatisch erhöht.
- Die Umsetzung ins nationale Recht muss bis Oktober 2024 erfolgen. Es gibt Stand Juli 2023 dazu bereits einen Referentenentwurf des BMI (NIS2UmsuCG).

Wie unterstützt PwC?

Als größtes Team für Industrial und Product Cyber Security innerhalb der Big4 (DE/ EMEA) haben wir es uns zur Aufgabe gemacht, das Sicherheitsniveau in Ihrem Unternehmen zu erhöhen und Sie bei der Einhaltung der Compliance zu unterstützen. Dazu führen wir eine gesamtheitliche Studie Ihres Unternehmens durch, um den Ist-Zustand zu erfassen, relevante gesetzlichen Vorgaben und potentielle Bedrohungen zu analysieren und schließlich eine Bewertung mit möglichen Handlungsempfehlungen auszuarbeiten. So können wir dabei unterstützen, gesetzliche Anforderungen einzuhalten und das Sicherheitsniveau der Unternehmen zu erhöhen.

Erfassung Ist-Zustand

- Untersuchung Ihrer existierender Sicherheitsmaßnahmen
- Sichtung Ihrer vorhandener Dokumentation zu den IT- und OT-Sicherheitsmaßnahmen
- Durchführung von Interviews mit Ihren Experten aus den verschiedenen Bereichen

Gesetzliche Vorgaben, potentielle Bedrohungen und die Bewertung des Sicherheitsniveaus

- Beschreibung relevanter regulatorischen Vorgaben (NIS2, IT-Sicherheitsgesetz 2.0, KRITIS-Dachgesetz, etc.)
- Beschreibung potentieller Bedrohungsakteure, sowie Auflistung vergangener Angriffe in Ihrem Sektor und die damit verbundenen Konsequenzen für die Unternehmen
- Bewertung Ihres IT-/OT-Sicherheitsniveaus unter Berücksichtigung gängiger Standards, wie IEC 62443 und ISO 27001

Handlungsempfehlung

- Vorschläge für verschiedene organisatorische Möglichkeiten zur Etablierung von IT- und OT Security
- Berücksichtigung der bestehenden Managementsysteme
- Maßnahmen für die verschiedenen Bereiche wie z.B. Risikomanagement oder die Sicherheit in Ihrer Lieferkette.

Mehrwert unseres Services

- Transparente und unabhängige Darstellung des Sicherheitsniveaus über die verschiedenen Bereiche und Organisationen
- Verbessertes Sicherheitsbewusstsein für die Besonderheiten von Industrieumgebungen und Unterschiede zur klassischen IT
- Sicherheitsmaßnahmen basierend auf bewährten Standards wie IEC 62443 und ISO 2700, aber spezifische Auswahl für Ihr Unternehmen

Haben Sie Fragen? Kontaktieren Sie unsere Experten

Dr. Oliver Hanka
Partner

PwC Deutschland
+49 160 5105836
oliver.hanka@pwc.com

Sebastian Frenzel
Senior Manager

PwC Deutschland
+ 49 1512 9257784
sebastian.f.frenzel@pwc.com