SIEMENS

Praxis-Workshop Industrial Security (WS-I-SEC)

Kurzbeschreibung

Industrial Security
Wie können Sie Ihre Produktionsumgebung wirkungsvoll vor Cyberangriffen schützen und Hackern keine Chance lassen? Welche Schutzmöglichkeiten im Industriesektor stellen das TIA-Portal und die Vernetzungstechnik der Siemens SCALANCE-Serie bereit? Und wie können Sie die Vorteile der Automatisierung nutzen, ohne Sicherheitsrisiken einzugehen?
Workshop
Die Antwort auf diese Fragen erhalten Sie in unserem Praxis-Workshop zur Industrial Security (Sicherheit in der Industrie). Wir gehen auch kurz auf die NIS-Richtlinie, auf unsere Security Assessment-Leistungen und die SCALANCE-Netzwerktechnik unter Bezugnahme auf die Automatisierungsnetzwerke und deren Komponenten (SPS/PLC und Anzeige) ein. Neben der Hardware bietet Siemens seinen Kunden die Möglichkeit, ihr aktuelles Netzwerk auf Sicherheit analysieren und testen zu lassen (Kontrolle, Fehlererkennung, verfügbare Lösungen). Erfahren Sie, wie Sie Ihre Produktionsumgebung mit dem TIA-Portal und der SCALANCE-Netzwerktechnik am besten vor Cyberangriffen schützen können.

Ziele

Jüngste Entwicklungen wie Fernbedienung, digitale Zwillinge und offene Standards erweitern das Spektrum der Möglichkeiten. Sie machen Produktionsumgebungen aber auch anfälliger für Cyberangriffe.
Im Workshop befassen wir uns mit Schutzmöglichkeiten auf drei Ebenen: Systemintegrität, Netzwerkschutz und Sicherheit von Produktionsanlagen. Unseren Ausgangspunkt bildet die weltweite Norm ISA 99 / IEC 62443 für industrielle Automatisierung.
Wir vertiefen die verschiedenen Schutzaspekte, die das TIA-Portal und die SCALANCE-Netzwerktechnik bieten. Nach der Veranstaltung können Sie sich mit Beispielen für bewährte Methoden zum Schutz von Automatisierungsnetzwerken und -komponenten vertraut machen.

Inhalte

- **Die NIS-Richtlinie und das Konzept der "Defense in Depth" (tiefgestaffelte Verteidigung) (Theorie)**

Was genau enthält die NIS-Richtlinie, die erste EU-Gesetzgebung zur Cybersicherheit, und wie wirkt sie sich auf uns aus? Auf welchen Prinzipien beruht das Konzept der tiefgestaffelten Verteidigung? Sie erhalten die Antworten während der Sitzung.

- **Systemintegrität (Theorie + Praxis)**

Die integrierten Sicherheitsfunktionen von Siemens gewährleisten optimalen Schutz vor einer Vielzahl von Bedrohungen: vom Kopieren der Konfigurationsdaten bis hin zur Manipulation von Dateien.

- **Netzwerkschutz (Theorie + Praxis)**

Vom Netzwerkschutzmanagement über die Netzwerksegmentierung bis hin zur verschlüsselten Kommunikation: Wie schützen Sie Ihre Automatisierungsnetzwerke vor unbefugtem Zugriff? Erfahren Sie, wie Ihnen Siemens Professional Services helfen kann.

- **Anlagenschutz (Theorie)**

Anlagenschutz beginnt mit der physischen Zugangskontrolle und der Sicherung besonders schutzwürdiger Bereiche mithilfe von Badges. Ausgangspunkt für einen maßgeschneiderten Schutz ist immer eine gründliche Risikoanalyse, gefolgt von der Umsetzung der Lösung und einer genauen Überwachung.

Teilnahmevoraussetzung

Grundkenntnisse des TIA-Portals sind erforderlich. Wenn Sie sich in Zweiergruppen anmelden, reicht es aus, wenn einer der beiden Teilnehmer über das erforderliche Vorwissen verfügt.

Hinweise

8.30 Uhr – Begrüßung
9.00 Uhr
– Die NIS-Richtlinie und das Konzept der "Defense in Depth" (tiefgestaffelte Verteidigung)
– Systemintegrität: Teil 1
– Kaffeepause
– Systemintegrität: Teil 2
12.30 Uhr - Mittagessen
13.15 Uhr
– Netzwerkschutz
– Anlagenschutz
– Kaffeepause
– Netzwerkschutz
16.45 Uhr – Feedback und Abschlussworte

Typ

Präsenztraining

Dauer

1 Tag

Sprache

de