Umsetzung der EU NIS Direktive und IT-Sicherheitsgesetzes 2.0 in Schaltanlagen und Leitstellen

1 h | Deutsch | # rWcyb11de

In diesem gemeinsamen Webinar analysieren Experten von Siemens und OMICRON, wie die Cyber-Security-Anforderungen der EU NIS Direktive und des deutschen IT-Sicherheitsgesetzes 2.0 in der Schutz- und Leittechnik umgesetzt werden können.
Dazu präsentiert Walter Wutzl im ersten Teil des Webinars, wie die Anforderungen der EU NIS Direktive in der Sekundärtechnik umgesetzt werden können.
Im zweiten Teil des Webinars berichtet Thomas Wolf, Sales und Application Engineer bei OMICRON, Praxiserfahrungen über die Umsetzung von Angriffserkennungssystemen in den Netzwerken von Leitstellen und Schaltanlagen, wie es im IT-Sicherheitsgesetz 2.0 gefordert wird. Er berichtet über die Erfahrungen bei der Inbetriebnahme von Angriffserkennungssystemen im DACH-Raum und über erste Ergebnisse nach 6 Monaten Betrieb.

Ziele

> Kennenlernen der Anforderungen der EU NIS Direktive in der Sekundärtechnik
> Lernen Sie aus Praxiserfahrungen bei der Inbetriebsetzung von Angriffserkennungssystemen und deren Betrieb nach den ersten 6 Monaten.
> Erfahren Sie die Beweggründe, warum viele EVUs im DACH-Raum ein Angriffserkennungssystem in ihre Leitstellen und Schaltanlagen einbauen.

Inhalte

> Überblick über Anforderungen an Systeme und Produkte aus Sicht der Cyber Security
> Konkrete Beispiele aus der Praxis für die Umsetzung der Anforderungen in der Sekundärtechnik
> Praxiserfahrungen bei Inbetriebsetzung und Betrieb von Angriffserkennungssystemen in Leitstellen und Schaltanlagen
> Was hat diese EVUs motiviert, Angriffserkennung in diesen Netzwerken einzusetzen?
> Wo liegen die Schwierigkeiten beim Einsatz von solchen Systemen?

Lösungen

StationGuard – Angriffserkennung für das Stromnetz

Teilnehmerkreis

Security-Verantwortliche in Energieversorgungsunternehmen

Vorwissen

Grundkenntnisse der Cyber Security