SIEMENS
Ingenuity for life

Security Assessments

Risiken identifizieren und bewerten – für einen umfassenden Security-Fahrplan mit Assess Security

siemens.de/industrial-security-services

Der Einsatz wirkungsvoller Security-Maßnahmen gegen Cyberangriffe oder Fehlverhalten ist für Betreiber von Produktionsstätten heutzutage unerlässlich. Doch wo setzt man am besten die Prioritäten, um mit dem verfügbaren Budget eine möglichst effektive Security-Lösung umzusetzen?

Siemens nimmt mit Assess Security alle Aspekte der IT-Security von Produktionsstätten unter die Lupe. Dabei kann die Einhaltung einschlägiger Normen wie etwa IEC 62443 oder ISO 27001 ebenso im Mittelpunkt stehen wie der optimale Einsatz bestimmter Siemens-Produkte.

Die Assessments bieten maximale Transparenz und vermitteln einen umfassenden Überblick über den Security-Ist-Zustand Ihrer Automatisierungssysteme. Das ist ideal, um den Handlungsbedarf hinsichtlich Industrial Security zu erkennen und die richtigen Maßnahmen zum Schließen eventueller Sicherheitslücken zu ergreifen.

»Die Optimierungsvorschläge von Assess Security sind sehr präzise. Sie unterstützen uns dabei, Aufwand und Nutzen jeder Einzelmaßnahme abzuschätzen und zu priorisieren. Das Assessment hat sich für uns rundum gelohnt.«

Alojz Ivicic, Verantwortlicher für die Wartung und Instandhaltung der Automatisierungstechnik bei den Kreiswerken Grevenbroich

Ihre Vorteile

- **Identifizierung und Bewertung von Risiken in den Kategorien Technologie, System- und Netzwerkarchitektur sowie Mitarbeiter**
- **Empfehlung und Priorisierung geeigneter Security-Maßnahmen**
- **Basis für eine transparente Kosteneinschätzung**
- **Eine anlagenspezifische und risikobaiserte Security Roadmap gewährleistet ein umfassendes und einheitliches Sicherheitsniveau**
- **Verfügbar für Siemens- und Drittanbieter-Systeme**

Assess Security auf einen Blick

Alle Security Assessments umfassen Aspekte wie Netzwerkarchitektur, Datenflüsse, Produktionssysteme und -prozesse sowie Mitarbeiter. Der Ablauf eines solchen Assessments ist denkbar einfach und klar strukturiert: Die Spezialisten von Siemens haben dafür sowohl Datenerfassungsprogramme als auch verschiedene Fragenkataloge entwickelt. Diese werden gemeinsam mit den Verantwortlichen aus relevanten Bereichen wie Produktion, Wartung, Planung oder Security abgearbeitet.

Anhand des Ergebnisses wird sofort ersichtlich, in welchen Bereichen akuter oder weniger dringender Handlungsbedarf besteht.

Der anschließend von Siemens erstellte Abschlussbericht enthält konkrete, exakt auf die untersuchten Unternehmensbereiche zugeschnittene Vorschläge und Konzepte zur schrittweisen Verbesserung der Industrial Security.

Industrial Security Check

Dieser Ansatz basiert auf dem Defense-in-Depth-Konzept, kombiniert mit Best Practices und unserer Erfahrung in internationalen Standards wie IEC 62443 und ISO 27001.

- Interviewbasierte Checkliste zur Identifizierung und Klassifizierung von Risiken
- Basierend auf Erfahrungen und Best Practises im Bereich von Industrial Security Assessments
- Kompakter Bericht mit Empfehlungen von Maßnahmen zur Risikominderung

IEC 62443 Assessment

IEC 62443 ist die führende Normenreihe für Security im Automatisierungsumfeld. Allgemeingültige, ganzheitliche Lösungen zum Schutz von Produktionsstätten und Automatisierungssystemen werden in der IEC 62443 beschrieben.

- Interviewbasierte Evaluierung des Sicherheitsstatus entsprechend den Anforderungen von IEC 62443
- Für Automatisierungssysteme von Siemens im Rahmen von Totally Integrated Automation und Systeme von Drittanbietern
- Bericht mit Empfehlung zur Schließung der identifizierten Sicherheitslücken

ISO 27001 Assessment

ISO 27001 ist eine führende Norm, die Anforderungen für Informationssicherheits-Managementsysteme beinhaltet.

- Interviewbasierte Evaluierung des Sicherheitsstatus entsprechend den Anforderungen von ISO 27001
- Für Automatisierungssysteme von Siemens im Rahmen von Totally Integrated Automation und Systeme von Drittanbietern
- Bericht mit Empfehlung zur Schließung der identifizierten Sicherheitslücken

Risk & Vulnerability Assessment

In diesem Assessment werden zunächst die relevanten Bedrohungen ausgewählt. Danach erfolgt die Suche nach eventuellen Schwachstellen, um auf dieser Basis Risiken zu identifizieren, zu klassifizieren und zu bewerten.

- Tool-gestützte Erfassung oder Sammlung von sicherheitsrelevanten Daten aus Automatisierungssystemen
- Risikoklassifizierung und -auswertung entsprechend dem Common Vulnerability Scoring System (CVSS)
- Grundlage für einen risikobasierten, anlagenspezifischen Security-Fahrplan

Securityhinweise

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen nur einen Bestandteil eines solchen Konzepts. Weitergehende Informationen über Industrial Security finden Sie unter **siemens.com/industrialsecurity.**

Siemens AG
Digital Factory
Postfach 48 48
90026 Nürnberg
Deutschland

Artikel-Nr.: DFPL-B10031-01
Gedruckt in Deutschland | fb 8425

siemens.de/industrial-security-services