

IT-Sicherheit in der Fabrikautomation und Prozesssteuerung

Die Bedrohung für Betriebstechnik (OT), Fabrikautomation und Prozesssteuerung nimmt stetig zu. Die OT rückt zunehmend in das Interessenfeld der IT-Kriminalität. Gezielte Angriffe werden häufiger und effektiver. Industriespionage, Erpressung und Sabotage sind keine Einzelfälle mehr. Wir unterstützen Sie dabei, Ihre OT nachhaltig und wirtschaftlich abzusichern. Im Folgenden finden Sie unsere Leistungen zu einzelnen Themenbereichen.

IT und OT verschmelzen sowohl auf technologischer als auch auf organisatorischer Ebene zu einer gemeinsamen Informations- und Telekommunikationstechnik (ITK).

Eine klare Abgrenzung ist heute nur noch selten möglich. Bereits aus der IT bekannte Bedrohungen durch Schadprogramme wie Trojaner, Viren und Ransomware werden dadurch zu ernstzunehmenden Risiken auch für die OT. Bisherige Isolationskonzepte und technologische Barrieren fallen zunehmend. Die Konvergenz ist in vollem Gange.

Während für die IT bewährte technische und organisatorische Verfahren für den sicheren Betrieb verfügbar sind, können diese oft nur eingeschränkt auf die OT übertragen werden. Falls die hieraus entstehenden Risiken nicht systematisch erhoben, bewertet und angemessen behandelt werden, können schwerwiegende Schwachstellen entstehen.

SICHERHEITSMANAGEMENT (ISMS)

Während standardisierte Sicherheitsprozesse und -verfahren im Bereich der IT-Betriebsführung heute breit akzeptiert sind, etablieren sich diese Verfahren im Bereich der OT erst schrittweise. Das IT-Sicherheitsgesetz und die Kritis-Verordnung haben diesen Prozess wesentlich vorangebracht.

Wir beraten und unterstützen Sie bei der Wahl und Einführung eines geeigneten Sicherheitsmanagements, das im Bedarfs-

fall auch den gesetzlichen Anforderungen an Kritis-Betreiber entspricht.

Unsere ISM-Leistungen:

- Auswahl, Anpassung und Implementierung eines geeigneten ISMS im Einklang mit Ihren Anforderungen
- Durchführung von ISMS-Compliance Audits, GAP-Analysen und Reifegradbeurteilungen auf Basis unseres Maturity Models
- Konzeption, Vorbereitung und Durchführung von Schulungen und Sensibilisierungsmaßnahmen

BUSINESS CONTINUITY MANAGEMENT (BCM)

Auch kurze Betriebsunterbrechungen können im Bereich der OT bereits große Schäden verursachen, unter Umständen mit Folgen für Mensch und Umwelt. Ein effektives Betriebskontinuitätsmanagement, welches die ITK-Notfall- und Wiederanlaufplanung über Systemredundanzen hinweg berücksichtigt, ist daher unverzichtbar.

Unsere BCM-Leistungen:

- Entwicklung geeigneter Betriebskontinuitätsprogramme
- Business Impact Analysen (BIA)
- Erstellen organisatorischer und technischer Notfallpläne sowie Planung, Vorbereitung und Begleitung von Notfallübungen



HiSolutions AG

Schloßstraße 1
12163 Berlin

info@hisolutions.com
www.hisolutions.com

Fon +49 30 533 289-0
Fax +49 30 533 289-900

ORDNUNGSGEMÄßER IT-BETRIEB

Voraussetzung für den zuverlässigen Betrieb von ITK sind wirksame und praktikable Verfahren und Prozesse zur Störungsvermeidung und -behebung. Praktikable Betriebskonzepte strukturieren den IT-Betrieb, gewährleisten die Einhaltung der geforderten Standards und schaffen Freiraum für neue Anforderungen.

Nutzen Sie unsere Expertise:

- Operationalisierung von Vorgaben in Betriebsprozessen
 - Change- und (Security) Incident Management
 - Schwachstellenmanagement
 - Berechtigungsverwaltung
 - Security Monitoring (Detektion)
- Betriebsorganisation
- Dokumentationsführung.

PLANUNG UND KONZEPTION

Gewachsene IT/OT-Infrastrukturen zeichnen sich oftmals durch hohe Komplexität und Silobildung aus. Hohe betriebliche Aufwände im Tagesgeschäft bei abnehmender Flexibilität sind die unvermeidbare Folge. Ergänzende IT-Sicherheitsanforderungen sind in solchen Strukturen häufig nicht mehr umsetzbar und werden vernachlässigt. Die IT-Risiken steigen.

Wir unterstützen Sie durch maßgeschneiderte Lösungen in den Bereichen:

- IT-Strategie für OT und IT unter Berücksichtigung der IT-Sicherheitsziele
- Berücksichtigung von IT-Sicherheit im Projektmanagement und Systementwicklungsprozess
- risikobasierte Sicherheitskonzeption u. a. in den Bereichen
 - Zonierungskonzepte
 - Virenschutz
 - Fernzugriff und (Predictive) Maintenance

SICHERHEITSÜBERPRÜFUNGEN UND AUDITS

Technische Audits sind ein wirksames Instrument zur Bestandsaufnahme oder zur Erfolgskontrolle. Richtig eingesetzt können sie für Fragestellungen der IT-Sicherheit sensibilisieren und sowohl organisatorische als auch technische Schwachstellen aufdecken.

Profitieren Sie von unserer Erfahrung und identifizieren Sie Schwachpunkte, bevor Schäden entstehen. Wählen Sie hierzu aus unserem Portfolio:

- ICS Cyber-Resilience-Checkup zur Standortbestimmung
- Compliance Audits bzw. GAP-Analysen gegen Standards, Regelungen oder Best-Practices
- angepasste technische Schwachstellenanalysen (Vulnerability Assessments/ Penetrationstests), die auch für den OT-Bereich geeignet sind
- Sicherheitsbeurteilung von Netzwerkdesign, Systemarchitektur und Fernzugängen

ÜBER DIE HISOLUTIONS AG

Seit über 25 Jahren engagieren wir uns in der Planung und Umsetzung von Informationssicherheitsmaßnahmen für Kunden aller Branchen.

Die Experten der HiSolutions verfügen über jahrelange Erfahrung mit komplexen Anlagen. Das Prüfen und Gestalten der Sicherheit von Automatisierungstechnik steht im Mittelpunkt zahlreicher Projekte in

Wirtschaft, Verbänden sowie Forschungsvorhaben.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die HiSolutions AG als erstes deutsches Unternehmen gleichzeitig sowohl für den Bereich Informationssicherheitsrevision und -beratung als auch für die Durchführung von Penetrationstests zertifiziert.



Ihr Ansprechpartner

Andreas Salm
Principal
Security Consulting

info@hisolutions.com
Fon +49 30 533 289-0