

ICS Security-Check

Cyber-Risiken in der Industrie- und Automatisierungstechnik erkennen und vermindern



Gezielte Angriffe auf kritische Infrastrukturen, Produktionsanlagen und Automatisierungstechnik (kurz: ICS, Industrial Control Systems) nehmen zu. Wir unterstützen Sie dabei, die Hauptbedrohungen von Anlagen im laufenden Betrieb zu identifizieren und zu minimieren.

CYBER-ANGRIFFE AUF ICS

Angriffe auf Industrie- und Automatisierungstechnik haben in den letzten Jahren stark zugenommen. Verwundbare Systeme lassen sich häufig bereits über das Internet recherchieren.

Beim Schutz von Unternehmenswerten und Personen kommt der IT-Sicherheit von Steuerungs- und Leitsystemen eine immer wichtigere Aufgabe zu.

BESONDERHEITEN VON ICS

Steuerungs- und Leitsysteme werden zunehmend vernetzt, sowohl untereinander als auch mit der Office-IT. Gleichzeitig nähern sich auch die eingesetzten Technologien immer mehr an.

Die Abwehr von Bedrohungen erfordert allerdings besondere Vorgehensweisen und dediziertes Fachwissen, um den Betrieb der Anlagen nicht zu gefährden.

DER ICS SECURITY-CHECK

Als erstes wird eine Bestandsaufnahme der hauptsächlichen IT-Risiken einer Anlage vorgenommen.

Um die Nebenwirkungen beim Testen produktiver Systeme zu begrenzen und den Produktionsprozess nicht einzuschränken, werden in einer kompakten Risikoanalyse zuerst konzeptionelle Lücken herausgearbeitet. Anschließend werden die eingesetzten Systeme und Anwendungen auf bekannte Schwachstellen und Sicherheitslücken hin untersucht.

Erst im nächsten Schritt erfolgt das eigentliche technische Audit bestehend aus Konfigurationsreview, gegebenenfalls Codereview und Penetrationstest.

Ziel ist es, die wichtigsten Maßnahmen für eine kurz- und mittelfristige Verbesserung des Sicherheitsniveaus zu erarbeiten und für die Umsetzung zu priorisieren.



ISMS IT-Risiken PROFINET
ISO 27001 OPC UA ISA-99 IEC 62443
Modbus **Cyber-Angriff** DNP3
S7 GaussDuquFlame **Stuxnet**
ISO 27019 Automatisierungstechnik

HiSolutions AG
Bouchéstraße 12
12435 Berlin

info@hisolutions.com
www.hisolutions.com

Tel.: +49 30 533 289 0
Fax: +49 30 533 289 900



BESTANDSAUFNAHME

In einem Workshop mit Verantwortlichen und Administratoren werden folgende Punkte unter Sicherheitsaspekten betrachtet:

- Eingesetzte Plattformen und Systeme
- Vernetzung (lokal/standortübergreifend)
- Zusammenwirken der Systeme
- Datenflüsse
- Kommunikationsprotokolle
- Netzanbindung (intern/extern)
- Vorhandene Schutzeinrichtungen (z. B. Firewalls, Gateways)
- Fernwartungszugänge
- Redundanz
- Virenschutzkonzept
- ggf. Monitoring/Angriffserkennung (IDS/IPS)

Sich aus der Analyse ergebende Schwachstellen werden dokumentiert und mit Handlungsempfehlungen hinterlegt, Ansatzpunkte für technische Einzelprüfungen identifiziert und in einem Prüfplan konsolidiert.

TECHNISCHE AUDITS

In den anschließenden technischen Audits werden die ermittelten Hauptbedrohungen für Ihre Umgebung abgedeckt.

Die einzelnen technischen Prüfungen können je nach ermitteltem Risikoprofil u. a. folgendes umfassen:

- Konfigurationsaudit kritischer Komponenten
- Test der Firewalls und sonstiger Security-Komponenten auf Einhaltung der Soll-Konfiguration
- Analyse des Datenverkehrs zur Aufdeckung verdeckter Kanäle und zur Ermittlung von Angriffsvektoren
- Identifikation versteckter Schnittstellen für Intrusion und Extrusion

- Externer Penetrationstest der von außen erreichbaren oder als Gateway nutzbaren Systeme
- Interner Penetrationstest kritischer Systeme in gesicherten Teststellungen
- Codereviews von zentralem und besonders kritischem Sourcecode

PENETRATIONSTEST

Je nach Anwendungsfall können unsere Penetrationstests eine, mehrere oder alle Ebenen der Automatisierungstechnik abdecken:

1. Schnittstellen zur Außenwelt (Office-Netz/Internet)
2. Prozessnetz-DMZ
3. Leittechnik (SCADA)
4. HMI/MMI
5. Steuerungstechnik (SPS/PLC)
6. Feldebene

Hierbei werden Scope und Methodik in unserem bewährten Verfahren gemeinsam darauf abgestimmt, den Betrieb nicht zu stören.

Sollte es sich im Rahmen des ICS Security-Checks als empfehlenswert erweisen, erhalten Sie auf Wunsch zudem Beratung zu:

- Sicherheitsmanagement nach nationalen und internationalen Standards
- Sicherheitskonzepte nach ISA-99/IEC 62443 u. ä.
- Sinnvolle Zonierung
- Betriebskompatibles Patch Management
- Praxistaugliche Virenschutzkonzepte
- Sichere Fernwartung
- Sichere Softwareentwicklung (SDLC)
- Ausschreibungsbegleitung

ÜBER DIE HISOLUTIONS AG

Seit mehr als 20 Jahren engagieren wir uns in der Planung und Umsetzung von Informationssicherheitsmaßnahmen für Kunden aus nahezu allen Branchen.

Die Prüfung und Gestaltung der Sicherheit von Automatisierungstechnik stand bereits im Mittelpunkt zahlreicher Projekte sowie eines Forschungsvorhabens mit der Universität Potsdam.

HiSolutions beschäftigt zahlreiche IT- und Branchenexperten, welche über jahrelange Erfahrung mit komplexen Anlagen verfügen.

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

Ihr Ansprechpartner:
David Fuhr

Senior Consultant
System Security

fuhr@hisolutions.com

Tel.: +49 30 533 289 0