SICHERHEITSRISIKEN FÜR KRITISCHE INFRASTRUKTUREN

Die häufigsten Schwachstellen bei Industrial Control Systems (ICS)

Eine sichere Umgebung?

Ausfall

Erpressung

Spionage

Manipulation

Zerstörung

Diebstahl

Die häufigsten ICS-Schwachstellen

Nutzen Bedrohungen die Schwachstellen von Industrial Control Systems (ICS) aus, sind Verfügbarkeit, Integrität und Vertraulichkeit der Systeme in Gefahr.

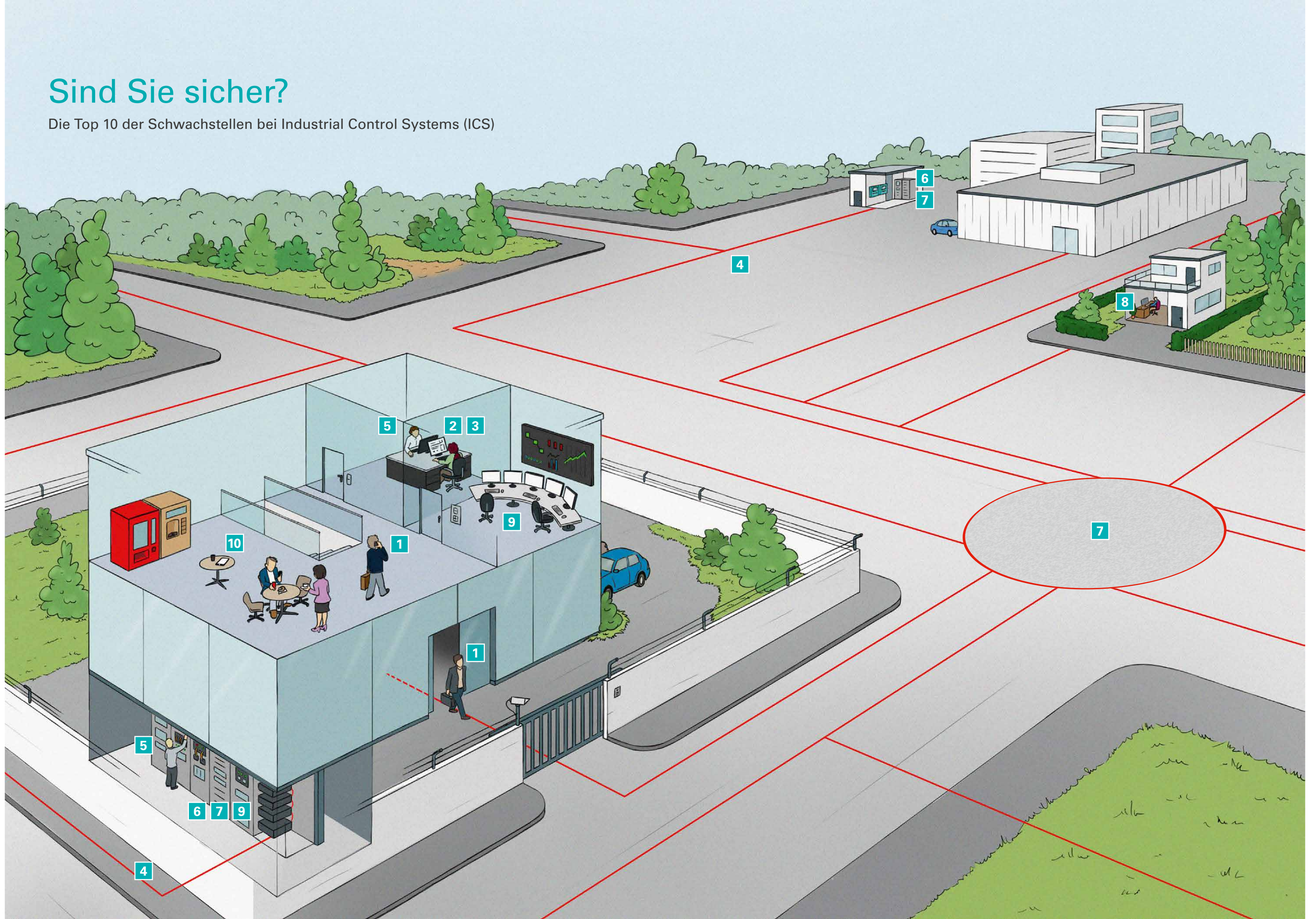
IT-Services von Rittmeyer schaffen Abhilfe:

- IT-Sicherheitsberatung
- Update-Service
- Cloud- und Backup-Lösungen
- Security Remote Client

Ausführliche Infos dazu und weitere Dienstleistungen finden Sie auf der Rittmeyer-Website.

Sind Sie sicher?

Die Top 10 der Schwachstellen bei Industrial Control Systems (ICS)



1 Social Engineering

Mit ‹Social Engineering› wird versucht, sicherheitstechnisch relevante Daten durch Ausnutzung menschlicher Komponenten in Erfahrung zu bringen. Menschen sind manipulierbar und generell das schwächste Glied in einer Kette.

Schutz

- Security-Awareness-Training
- Sicherheitsrichtlinien
- Zutrittskontrollen
- Gesunder Menschenverstand
- Etablierung von Alarmierungswegen

2 Wechseldatenträger: Einschleusen von Schadsoftware

Mitarbeitende verwenden Wechseldatenträger und externe Hardware, wie z. B. USB-Sticks, neben dem Einsatz im Office- und ICS-Netz häufig auch privat.

Schutz

- Benutzerrichtlinien
- Technischer Schutz
- Virenschutz
- Rechteverwaltung
- Härtung des Computers
- Datensicherung

3 Internet und Intranet: Infektion mit Schadsoftware

Browser und E-Mail-Clients sind in der Regel an das Internet angebunden.

Schutz

- Benutzerrichtlinien
- Virenschutz
- Software-Updates
- Rechteverwaltung
- Verantwortlichkeiten
- Härtung des Computers
- Datensicherung

4 Fernwartungszugänge

Bei ICS-Installationen sind externe Zugänge für Wartungszwecke weit verbreitet. Häufig existieren dabei Default-Zugänge mit Standardpasswörtern oder sogar fest kodierte Passwörter. Das vereinfacht Cyber-Kriminellen das Eindringen.

Schutz

- Firewall
- SSL/TLS-Verschlüsselung
- Pre-Shared-Keys
- Zertifikate
- Personalisierte Zugänge
- Audits
- Änderung der Standardpasswörter
- Granulare Segmentierung der Netze
- Verschlüsselung sensibler Daten
- Freischaltung von Fernwartungszugängen durch internes Personal
- Protokollierung von Fernzugriffen

5 Menschliches Fehlverhalten und Sabotage

Das Arbeitsumfeld von ICT-Personal nimmt sicherheitstechnisch eine besondere Stellung ein. Manipulationen in diesen Umgebungen können absichtlich oder unabsichtlich erfolgen.

Schutz

- Physischer Schutz
- Benutzerrichtlinien
- Schulungen
- Rechteverwaltung
- Etablieren des ‹Need to know›-Prinzips
- Autom. Überwachung von Systemzuständen und -konfigurationen

6 Mit dem Internet verbundene Steuerungskomponenten

Oftmals werden ICS-Komponenten, wie beispielsweise speicherprogrammierbare Steuerungen (SPS), direkt mit dem Internet verbunden (Internet of Things, IoT).

Schutz

- Firewall
- Software-Updates
- Änderung der Standardpasswörter

7 Technisches Fehlverhalten und höhere Gewalt

Softwarefehler in sicherheitsspezifischen Komponenten sowie ICS-Komponenten, die zu unvorhergesehenem Fehlverhalten führen, lassen sich ebensowenig ausschliessen wie mögliche Hardwaredefekte und Netzwerkausfälle.

Schutz

- Physischer Schutz
- Redundante Systeme
- Tausch- oder Ersatzgeräte
- Wartung
- Aufbau eines Notfallmanagements
- Nutzung von standardisierten Schnittstellen

8 Kompromittierung von Extranet und Cloud-Komponenten

Der in der konventionellen IT verbreitete Trend zum Outsourcing von IT-Komponenten hält mittlerweile auch in ICS Einzug.

Schutz

- VPN-Zugänge
- Zertifizierte Anbieter
- Redundante Systeme
- Service Level Agreement
- Kryptografische Mechanismen

9 (D)DoS-Angriff

Die Kommunikation zwischen ICS-Komponenten kann über drahtgebundene sowie drahtlose Verbindungen erfolgen. Werden diese Verbindungen gestört, können u. a. Mess- und Steuerdaten nicht mehr korrekt übertragen werden. Eine Komponente kann beispielsweise durch eine sehr hohe Anzahl von Anfragen überlastet werden, sodass keine fristgerechte Antwort mehr geliefert werden kann.

Schutz

- Intrusion Detection (IDS)
- Redundante Anbindungen mit unterschiedlichen Protokollen
- Dedizierte kabelgebundene Verbindungen für kritische Funktionen
- Härtung von Netzzugängen

10 Produktionsumfeld: Kompromittierung von Smartphones/Tablets

Anzeige und Veränderung von Betriebs- oder Produktionsparametern auf Smartphones oder Tablets wird bei immer mehr ICS-Komponenten als zusätzliche Produkteigenschaft beworben und eingesetzt.

Schutz

- Benutzerrichtlinien
- Rechteverwaltung
- VPN-Zugänge
- Mobile Device Management
- Nutzung zertifizierter App-Stores
- Keine Apps zum direkten Zugriff auf ICS

Rittmeyer, ein Unternehmen der BRUGG GROUP, entwickelt und liefert schlüsselfertige Mess- und Leittechniklösungen für Energie- und Wasserversorgungen, Wasserkraftwerke und Abwasserreinigungsanlagen. Seit 1904 steht der Name Rittmeyer für höchste Produkt- und Leistungsqualität. Rittmeyer begleitet seine Kunden partnerschaftlich über den gesamten Lebenszyklus ihrer Anlagen – von der Konzeption über die Planung, Installation, Inbetriebnahme und Schulung bis hin zu einem umfassenden Service. Mit sechs Tochtergesellschaften, einem Verkaufs- und Repräsentanzbüro sowie Vertretungen in über 25 Ländern ist Rittmeyer weltweit tätig.

www.rittmeyer.com

rittmeyer
BRUGG

Rittmeyer AG
Inwilerriedstrasse 57
Postfach 1660
CH-6341 Baar
+41 41 767 10 00
security@rittmeyer.com

82824.1.D | 1803 ERN