Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Veröffentlichungen zur Cyber-Sicherheit

EMPFEHLUNG: IT IN DER PRODUKTION

Empfehlungen für Fortbildungs- und Qualifizierungsmaßnahmen im ICS-Umfeld

Der akute Handlungsbedarf zur Absicherung von Industrial Control Systems (ICS) – also im Bereich Fabrikautomation und Prozesssteuerung – vor Cyber-Bedrohungen wird immer mehr seitens der Industrie erkannt. Hierzu bietet das BSI eine Fülle von Informationsmaterialien, Best Practices und weiteren Hilfsmitteln. In Ergänzung zu diesen Angeboten ist es aber unerlässlich, dass Unternehmen ihre Mitarbeiter entsprechend fortbilden und qualifizieren. Während für Mitarbeiter, wie Anlagenbediener, spezifische Sensibilisierungsmaßnahmen geeignet sind, müssen andere Zielgruppen ausführlicher geschult werden. Dies betrifft insbesondere solche Mitarbeiter, die für Planung, Entwicklung, Integration bzw. Errichtung, Betrieb und Wartung verantwortlich bzw. darin maßgeblich involviert sind und somit Cyber-Sicherheit an dieser Stelle aktiv mitgestalten. Auch Management oder Produktionsverantwortliche sollten in einem angemessenen Umfang qualifiziert werden, der über typische Sensibilisierung hinaus geht.

Der Bedarf an solchen Fortbildungs- und Qualifizierungsmaßnahmen wächst stetig. Dementsprechend gibt es immer mehr Dienstleister, die diesen Bedarf adressieren. Gerade mit einer wachsenden Zahl von Angeboten ist es wichtig, dass ein hinreichendes inhaltliches Mindestniveau gewährleistet ist. Dieses Dokument gibt eine Orientierungshilfe für zwei Arten von Schulungen:

1. Management und Produktionsverantwortliche
2. Mitarbeiter mit Verantwortung und/oder Einflussmöglichkeiten auf Cyber-Sicherheit eines ICS.

Im Fokus stehen also Experten aus dem Bereich Fabrikautomation und Prozesssteuerung, die ihre Qualifikationen um Cyber-Sicherheit für den eigenen Verantwortungsbereich erweitern wollen. Nicht behandelt werden allgemeine Sensibilisierungsmaßnahmen sowie Qualifizierungsmaßnahmen für IT- bzw. IT-Sicherheits-Experten, die den Anwendungsbereich ICS erschließen wollen (Administratoren, Dienstleister, Berater, Auditoren). Diese Zielgruppen werden ggf. in einer Überarbeitung dieser Empfehlung berücksichtigt.

Mit dieser Empfehlung des BSI ist keine Zertifizierung verbunden. Es handelt sich hierbei lediglich um eine unverbindliche Empfehlung für Schulungsinhalte.

1 Allgemeine Anforderungen

Die Struktur der Qualifizierungsmaßnahmen ist lediglich als Vorschlag zu verstehen, der auf Erfahrungswerten beruht und sich in der Vergangenheit bewährt hat. Alternativ können aber auch andere Strukturen oder Abläufe zur Anwendung kommen. Dies gilt insbesondere dann, wenn Qualifizierungsmaßnahmen auf einzelne Branchen oder für bestimmte Unternehmensgrößen zugeschnitten werden.

Hinsichtlich der einzelnen zu behandelnden Themen wird empfohlen, die in diesem Dokument dargestellten Vorschläge als Schulungsanbieter umzusetzen bzw. als Kunde aktiv einzufordern.

Auch die in diesem Dokument vorgeschlagenen zeitlichen Aufwände sind lediglich ein Richtwert. Eine Schulung für ICS-Experten kann für Mitarbeiter von KMUs einen anderen Umfang und somit eine andere fachliche Tiefe haben als für Mitarbeiter von Großkonzernen.

Die Qualifizierungsmaßnahmen sollten neben einem theoretischen Teil auch unbedingt einen praktischen Anteil aufweisen, um einen nachhaltigen Lerneffekt zu fördern. Hierzu gehören beispielsweise Übungen anhand von Beispielszenarien oder das Erproben von Softwaretools. Letztere sollten ggf. auf vereinfachten, aber unbedingt repräsentativen Plattformen durchgeführt werden, damit der Transfer in das eigene Unternehmen möglichst gegeben ist.

Die Referenten oder Trainer der Qualifizierungsmaßnahmen sollten die zu vermittelnden Inhalte aus der Praxis kennen. So eignen sich insbesondere Experten mit mehrjähriger Erfahrung aus dem Betrieb von industriellen Anlagen. Auch IT-Sicherheitsexperten sind dafür geeignet, sofern sie nicht nur über die theoretischen Grundlagen aus dem Bereich ICS verfügen, sondern dort seit mindestens fünf Jahren aktiv in der Beratung oder in IT-Sicherheitsprojekten tätig sind. Eine Kooperation von zwei Referenten – einen aus der Industrie und einen aus der IT-Sicherheit – ist ebenfalls sinnvoll. Anbieter sollten die entsprechenden Profile ihrer Referenten dahingehend transparent machen.

2 Schulung für Management

Zielgruppe: Produktionsverantwortliche, Management (C-Level), ggf. (neue) Mitarbeiter mit operativem Bezug zu Security als Einstiegsmaßnahme

Zeitansatz: 6-7 Stunden (netto)

Ziele:

- ✔ Bedrohungslage aufzeigen,
- ✔ Handlungsbedarf verdeutlichen,
- ✔ grundlegendes Verständnis von elementaren Begrifflichkeiten und systematischen Ansätzen,
- ✔ Kenntnis der wichtigsten organisatorischen und technischen Maßnahmen auf abstraktem Niveau,
- ✔ Schaffung der Voraussetzungen um Projekte und Maßnahmen anzustoßen und diese auf Management-Ebene nachvollziehen zu können

Themengebiet	Inhalte
Grundlagen 1h	✔ Gemeinsame Begrifflichkeiten im Bereich ICS ✔ Netzwerk-Grundlagen: Router, Switche, Firewall, Wifi, Mobilfunk, etc. ✔ Kryptographische Grundlagen (symmetr. vs. asymmetr. Kryptographie, Hash-verfahren, Zertifikate (z.B. SSL), S/MIME, PGP, Nutzen und Nachteile für ICS) ✔ Rechtlicher Rahmen: IT-SiG (KRITIS-Bezug falls gegeben, Gesetz als Vorbildfunktion), Managerhaftung, Produkthaftung, Branchenstandards und Normenlandschaft, etc.
Bedrohungslage 1h	✔ Schutzziele ✔ Angriffsformen (z.B. DDoS, APT , Schadsoftware, MITM, Spoofing, etc.) ✔ Lagebild: häufigste Angriffe, Statistiken, ggf. Beispiele ✔ Kollateralschäden in ICS durch nicht-zielgerichtete Schadsoftware ✔ gezielte Angriffe: typische Vorgehensweisen / Anatomie eines gezielten Angriffs (über IT) auf ICS ✔ Informationsbeschaffung und Social Engineering (z.B. FOCA-Tool oder OSINT) ✔ Sicherheit von Partnern, Kunden, Drittfirmen (Supply Chain) ✔ Ausbreitung im Unternehmen (Lateral Movement) ✔ Unsicherheit von industriellen Protokollen ✔ Exfiltration, Manipulation, Sabotage in ICS ✔ Schadensfolgen ✔ weitere Gefährdungen (z.B. Fernwartung, Industrial Wireless, etc.) ✔ ggf. praktische Demonstration anhand von Metasploit, SET, o.ä.
Sicherheitsmanagement und übergreifende organisatorische Maßnahmen 2h	✔ Idee / Vorgehensweise und Aufbau eines ISMS ✔ Betrieb eines ISMS ✔ elementare Begriffe: Asset, Schwachstelle, Gefährdung, Risiko, etc. ✔ Standards / Normen ✔ Defense in depth ✔ Elementare Maßnahmen im Sicherheitsmanagement (insbes. organisatorisch) ✔ Netzplan ✔ Ausschreibung, Beschaffung, Security im Kontext FAT/SAT ✔ Inbetriebnahme ✔ Notfallvorsorge, BCM, Incident Response
User-zentrierte Maßnahmen 1h	✔ Policies / Richtlinien mit Beispielen (wesentliche Themen hierbei sind Verwendung von mobilen Datenträgern, Fremdfirmen und Anschluss neuer Komponenten bzw. Anlagen an das Netzwerk) ✔ Sensibilisierung / Awareness
Technische Maßnahmen 1,5h	✔ Allgemeine Klärung von Begrifflichkeiten: Firewall, AV, AWL, SIEM, IDS, IPS, etc. ✔ Firewall / Industrial Firewall ✔ Remote Access / VPN ✔ Systemhärtung ✔ Logdaten – Sammlung, Analyse ✔ Monitoring (Traffic, Systemeigenschaften) ✔ AV-Schutz, Wechseldatenträgerschleuse ✔ Vulnerability Scanner (Außensicht, z.B. am Beispiel OpenVAS) ✔ Industrial Wireless
Nächste Schritte 0,5h	✔ Erste organisatorische Maßnahmen (Rollen, Verantwortlichkeiten, Kooperation IT, erste Prozesse, etc.) ✔ Checkliste (z.B. BSI Top 10 Self Check) ✔ Erstellung und Analyse Netzplan; Etablieren als dauerhafte Aufgabe ✔ Planspiele (z.B. BSI Tabletop Exercises) ✔ Vorschläge/Handlungsmöglichkeiten sowie deren Aufwände und Potential ✔ (Kurz-)Revision ✔ Pilotprojekte

Bei der Darstellung der Bedrohungslage ist wichtig, dass Angriffe häufig im Office-Netz beginnen und im weiteren Verlauf in der Produktion fortgesetzt werden. Ein Schutz allein im Office bzw. am äußeren Perimeter des Unternehmens genügt nicht zur Absicherung. Die Darstellung der Maßnahmen sollte sich auf ICS konzentrieren und auf die speziellen Anforderungen eingehen. Nur wo nötig sollte auf die allgemeine IT abgezielt werden.

Im letzten Abschnitt sollten die Teilnehmer konkrete Empfehlungen (action items) erhalten, wie das vermittelte Wissen im eigenen Unternehmen in die Praxis umgesetzt werden kann.

3 Schulung für Experten der Produktion

Zielgruppe: Produktions-CISO, Ingenieure, Infrastruktur-Betriebspersonal, Wartungstechniker, Instandhalter – also mit einem technischen Hintergrund in ICS und mit der Planung, Entwicklung, Integration/Errichtung, Betrieb oder Instandhaltung betraut.

Zeitansatz: 21-35 Stunden (netto) / 3-5 Tage

Ziele:

- ✔ grundlegendes Verständnis der relevanten Begrifflichkeiten, Technologien und Elemente der IT / IT-Sicherheit,
- ✔ fundiertes Verständnis der Bedrohungslage zur Bewertung der eigenen Betroffenheit / Gefährdungslage,
- ✔ Vermittlung der Grundsätze von ISMS,
- ✔ vertiefende Kenntnisse von organisatorischen und technischen Maßnahmen,
- ✔ konkrete Ansatzpunkte für die Umsetzung im operativen Betrieb / bei der Planung neuer Anlagen / bei der Leitung von Sicherheitsprojekten (ggf. mit externer Beauftragung),
- ✔ Anspruch an diese Qualifizierungsmaßnahme ist nicht, dass die Teilnehmer sämtliche behandelten Themen eigenverantwortlich als operative Aufgabe ohne Unterstützung durch Dritte oder weitere Fortbildungsmaßnahmen übernehmen können.

Themengebiet	Inhalte
Grundlagen 2h	✔ Gemeinsame Begrifflichkeiten ICS ✔ Netzwerk-Grundlagen: Router, Switche, Firewall, Wifi, Mobilfunk ✔ Netzwerkprotokolle und Dienste (aus der klassischen IT) ✔ Kryptographische Grundlagen (symmetrische vs. asymmetrische Verschlüsselung, Signaturen, Hashverfahren, Zertifikate (z.B. SSL), S/MIME, PKI, PGP, Nutzen und Nachteile für ICS) ✔ Rechtlicher Rahmen: IT-SiG (KRITIS-Bezug falls gegeben, Gesetz als Vorbildfunktion), Managerhaftung, Produkthaftung, Branchenstandards und Normenlandschaft, etc.

Themengebiet	Inhalte
Bedrohungslage 4-6h	✔ Schutzziele ✔ Angriffsformen (z.B. DDoS, APT , Schadsoftware, MITM, Spoofing, etc.) ✔ Lagebild: häufigste Angriffe, Statistiken, Beispiele ✔ Kollateralschäden in ICS durch nicht-zielgerichtete Schadsoftware ✔ Klassifizierung von Angreifern ✔ gezielte Angriffe: typische Vorgehensweisen / Anatomie eines gezielten Angriffs (über IT) auf ICS ✔ Sicherheit von Partnern, Kunden, Drittfirmen (Supply Chain) ✔ Informationsbeschaffung und Social Engineering (z.B. FOCA-Tool oder OSINT) ✔ Ausbreitung im Unternehmen (Lateral Movement) ✔ Typischer Funktionsumfang von ICS-Komponenten ✔ Typische Schwachstellen in ICS-Komponenten ✔ Typische Schwachstellen im Konzept/Architektur ✔ Unsicherheit von industriellen Protokollen ✔ Angreifbarkeit von Safety-Systemen ✔ Exfiltration, Manipulation, Sabotage in ICS ✔ Schadensfolgen ✔ weitere Gefährdungen (z.B. Fernwartung, Industrial Wireless, etc.) ✔ Praxisteil zu Angriffen, lateral movement und Manipulation ICS-Komponenten; z.B. unter Verwendung von Tools wie nmap, metasploit, snmpcheck, sqlmap, plcscan, etc. ✔ Ggf. Praxis: Tabletop Übung, konkretes Szenario
Sicherheitsmanagement und übergreifende organisatorische Maßnahmen 6-11h *ab hier Fokus auf Maßnahmen in ICS bzw. an den Schnittstellen nach außen*	✔ Idee / Vorgehensweise und Aufbau eines ISMS ✔ elementare Begriffe: Assets, Schwachstelle, Gefährdung, Risiko, etc. ✔ Standards / Normen ✔ Defense in depth ✔ Elementare Maßnahmen im Sicherheitsmanagement (Schwerpunkt organisatorisch) ✔ Netzplan (inkl. Erfassung, Discovery, Darstellungsformen) ✔ Configuration/Change Management ✔ Sicherheit von Partnern, Kunden, Drittfirmen (Supply Chain) ✔ Ausschreibung, Beschaffung, Security im Kontext von Factory bzw. Site Acceptance Tests (FAT/SAT) ✔ Inbetriebnahme ✔ Vulnerability & Patch Management ✔ Nutzung von aktuellen Informationen (Advisories, Warnungen, etc.) ✔ Praxisbeispiel inkl. Asset-Erfassung, Netzplanerstellung, Schutzbedarfsfeststellung, Modellieren, Maßnahmen ableiten, ... ✔ Zertifizierung
User-zentrierte Maßnahmen 1-2h	✔ Policies / Richtlinien mit Beispielen (wesentliche Themen hierbei sind Verwendung von mobilen Datenträgern, Fremdfirmen und Anschluss neuer Komponenten/Anlagen an das Netzwerk) ✔ Sensibilisierung / Awareness

Themengebiet	Inhalte
Technische Maßnahmen 6-11h	✔ Allgemeine Klärung von Begrifflichkeiten: Firewall, AV, AWL, SIEM, IDS, IPS, Honeypot, etc. ✔ Schnittstelle IT / ICS ✔ Zones & Conduits, Absicherung Netzübergänge, ICS-DMZ ✔ Firewall / Industrial Firewall inkl. wichtiger zu berücksichtigender Aspekte, wie Auswirkungen auf Echtzeitanforderungen oder Latenzen ✔ Remote Access / VPN ggf. inkl. Praxisteil ✔ Systemhärtung (allgemein); ggf. Praxisteil z.B. zu Gruppenrichtlinien; PLCs, HMIs, Historians/DB ✔ Sicherheit von ICS-Serverkomponenten, HMI, PLC ✔ Access Management – Zugriffsmodelle, Verzeichnisdienste, Management von Rollen und Rechten ✔ 3rd Party Devices (e.g. Servicetechniker) ✔ Logdaten – Sammlung, Analyse ggf. inkl. Praxisteil ✔ Monitoring (Traffic, Systemeigenschaften) ✔ Absicherung von Datenbanken und Historians ✔ AV-Schutz, Wechseldatenträgerschleuse ✔ Vulnerability Scanner (Außensicht) ✔ Industrial Wireless ✔ Mobile Devices im Feld
Audit, Revision, Pentest 0,5-2h	✔ Grundlagen ✔ Vorgehensweisen, Standards ✔ Besonderheiten bei ICS, z.B. erforderliche Rules of Engagement ✔ Beispiel für eine praktische Durchführung
Notfallvorsorge, BCM, Incident Handling 0,5-2h	✔ Backup & Recovery, Testen von Backups, unterschiedliche Methoden für Backups ✔ Grundlagen von Notfallvorsorge, BCM, Incident Response ✔ Vorgehensweisen und Standards ✔ Forensik ✔ Praxisbeispiel: Notfallvorsorge, BCM, Incident Response
Abschließende Diskussion, nächste Schritte, Resümee 1-2h *Teilnehmer sollen konkrete Empfehlungen / Action Items nach Hause nehmen*	✔ Vorschläge/Handlungsmöglichkeiten sowie deren Aufwände und Potential ✔ Erste organisatorische Maßnahmen (Rollen, Verantwortlichkeiten, Kooperation IT, erste Prozesse, etc.) ✔ Checkliste (z.B. BSI Top 10 Self Check) ✔ Erstellung und Analyse Netzplan; Etablieren als dauerhafte Aufgabe ✔ Planspiele (z.B. BSI Tabletop Exercise) ✔ (Kurz-)Revision

Wünschenswert für diese Qualifizierungsmaßnahme wäre ein durchgängiges Szenario zur Veranschaulichung und als Grundlage für praktische Übungen. So kann beispielsweise ein vereinfachtes Szenario ohne Sicherheitsmaßnahmen sukzessive abgesichert werden.

Als weitere Möglichkeiten für einen praktischen Anteil eignen sich u.a.

✔ Systemhärtung am Beispiel einer verbreiteten oder im jeweiligen Unternehmen genutzten SPS

✔ Konfiguration einer Firewall für industrielle Szenarien

✔ Konfiguration eines VPN

✔ Konfiguration eines VLAN für einen industriellen Anwendungsfall

4 Ausblick

Fortbildungs- und Qualifizierungsmaßnahmen im Kontext Cyber-Sicherheit für Industrial Control Systems sind zunehmend seitens der Betreiber im Bereich Fabrikautomation und Prozesssteuerung gefragt. Dieses Dokument sollte als Orientierungshilfe für die dabei relevanten Inhalte verwendet werden. Als weitere Grundlage für die Ausgestaltung solcher Trainings können die Veröffentlichungen und Hilfsmittel des BSI[1] in diesem Bereich dienen.

Für Feedback, Anregungen und die Mitarbeit bei der Ausgestaltung von Empfehlungen für weitere Zielgruppen steht das BSI unter der E-Mail Adresse ics-sec@bsi.bund.de zur Verfügung.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.

1 Sicherheit von Industrial Control Systems, BSI, https://www.bsi.bund.de/ICS