Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise zum Baustein: IND.2.1 Allgemeine ICS-Komponente

1. Einleitung

Diese Umsetzungshinweise geben Hilfestellung bei der Umsetzung der spezifischen Sicherheitsanforderungen für ICS-Komponenten und vergleichbare Automatisierungsgeräte, die Teil einer ICS-Anlage bzw. der Operational Technology (OT) sind. ICS-Komponenten sind elektronische Komponenten zur Steuerung, Messung, Überwachung oder Regelung. Sie sind Teil einer Maschine oder Anlage.

Grundsätzlich beziehen sich der Baustein sowie die vorliegenden Umsetzungshinweise auf ICS-Komponenten aller Bauarten. Dabei ist jedoch zu beachten, dass sich nicht jede Maßnahme mit jedem Gerätetyp wortwörtlich umsetzen lässt. Es ist bezüglich der Begrifflichkeiten immer diejenige Interpretation zu wählen, die der Absicht der Anforderung am nächsten kommt. Dies betrifft insbesondere emulierte Soft-Komponenten.

2. Maßnahmen

Im Folgenden sind spezifische Maßnahmen für die Anforderungen des Bausteins IND.2.1 *Allgemeine ICS-Komponente* sowie für weitere Bausteinen aufgeführt, die hiermit im Zusammenhang stehen: ORP.4 *Identitäts- und Berechtigungsmanagement.*

Diese zusätzlichen Maßnahmen sollten bei der Umsetzung der genannten Bausteine berücksichtigt werden. Alle Maßnahmen (gekennzeichnet mit M) sind aufsteigend nummeriert und korrespondieren mit den entsprechenden Anforderungen (gekennzeichnet mit A).

2.1. Maßnahmen zum Baustein IND.2.1 Allgemeine ICS-Komponente

IND.2.1.M1 Einschränkung des Zugriffs für Konfigurations- und Wartungsschnittstellen (B)

Erzwingen der Authentifizierung an Konfigurations- und Wartungsschnittstellen

Das Gerät sollte für den Zugriff auf Schnittstellen zur Konfiguration und Wartung eine Authentifizierung erzwingen. Dies gilt sowohl für den Zugriff auf lokale Schnittstellen als auch auf Schnittstellen, die für den Fernzugriff nutzbar sind. Auf diese Weise soll ein unberechtigter Zugriff auf Konfigurations- sowie Wartungsschnittstellen verhindert werden.

Standardbenutzerkonten und -passwörter, Qualität der Passwörter

Viele Geräte werden werksseitig mit Standardbenutzerkonten und -passwörtern oder aufgedruckten Initialpasswörtern ausgeliefert, sodass diese vor der Inbetriebnahme geändert werden müssen, um einen Missbrauch zu verhindern (siehe auch IND.1.M7 *Etablieren einer übergreifenden Berechtigungsverwaltung zwischen der OT und in der Office-IT*, ORP.4.A2 *Regelung für Einrichtung, Änderung und Entzug von Berechtigungen*).

Dokumentation

Die Passwörter für Systemkonten sollten für Wartungs-, Diagnose- oder Notfallzugriffe im Rahmen der diesbezüglich bestehenden Regelungen sicher hinterlegt werden (siehe auch IND.1.M13 *Notfallplanung für OT*). Das Hinterlegen kann etwa in einem verschlossenen Umschlag, in einem Safe oder in einem geeigneten, organisationsintern freigegebenen Passwortmanager erfolgen. Das Verfahren zur Passworthinterlegung sollte praktikabel und auch in Notfallsituationen zuverlässig nutzbar sein.

IND.2.1.M2 Nutzung sicherer Übertragungs-Protokolle für die Konfiguration und Wartung (B)

Deaktivieren unsicherer Administrations-, Entwicklungs- und Wartungsschnittstellen

Sowohl durch unsichere, unverschlüsselte Protokolle für Administrationsschnittstellen (z. B. Telnet, FTP oder zu ungesicherten Weboberflächen) als auch durch unverschlüsselte proprietäre Protokolle für Konfigurations- und Wartungsschnittstellen können Zugangsdaten durch Dritte bei Zugang zum Übertragungsmedium bzw. zu den lokalen Geräteschnittstellen ausgelesen und für unbefugten Zugriff verwendet werden. Aus diesem Grund sollten unverschlüsselte Anwendungs-, Konfigurations- und Wartungsschnittstellen deaktiviert werden.

Konfiguration sicherer Administrations-, Entwicklungs- und Wartungsschnittstellen

Insbesondere für den Fernzugriff sollten die Geräte nur durch gesicherte Protokolle wie z. B. SSHv2, SNMPv3, HTTPS oder OPC UA erreichbar sein. Darüber hinaus sollte geprüft werden, ob für bestehende unverschlüsselte proprietäre Wartungsprotokolle und -verfahren Verschlüsselungsverfahren wie etwa TLS- oder VPN-Tunnel genutzt werden können. Weiterhin sollte geprüft werden, ob die Operatoren eine PKI betreiben, um mit den Komponenten mit Zertifikaten umgehen zu können.

Bei hohem Schutzbedarf sollte außerdem auf die Nutzung lokaler Funkschnittstellen wie Bluetooth oder NFC zur Konfiguration und Wartung verzichtet werden (siehe auch IND.2.1.M4 *Deaktivierung oder Deinstallation nicht genutzter Dienste, Funktionen und Schnittstellen*).

IND.2.1.M3 ENTFALLEN

Die zugehörige Anforderung ist entfallen.

IND.2.1.M4 Deaktivierung oder Deinstallation nicht genutzter Dienste, Funktionen und Schnittstellen (B)

Um die Angriffsfläche des Systems auf Netzebene zu reduzieren, sollten alle nicht benötigten Dienste deaktiviert werden. Ebenso sollten sämtliche nicht benötigten Programme und Funktionen in ICS-Komponenten deaktiviert werden. Gleiches gilt für nicht benötigte Schnittstellen.

Deaktivieren nicht benötigter Hardware- und Softwareschnittstellen

Moderne, vielfältig einsetzbare Automatisierungssysteme besitzen eine Vielzahl von Hard- und Software-Schnittstellen zur Anbindung weiterer Baugruppenelemente oder externer Geräte wie Sensoren und Aktoren. Beispiele hierfür sind Slots für Erweiterungsmodule, serielle Schnittstellen sowie Netz- und Funknetz-Schnittstellen wie Bluetooth, Tetra und WLAN.

Sowohl ICS-Komponenten als auch andere Automatisierungssysteme (z. B. IT-Systeme innerhalb eines ICS) beherrschen aufgrund ihrer Flexibilität und Vielseitigkeit in der Regel eine größere Anzahl an Kommunikationsprotokollen, die sich in ihren Sicherheitseigenschaften teilweise stark unterscheiden. So werden z. B. häufig Protokolle für den RS-232/485-Standard, Modbus, Modbus TCP, Profibus, Profinet, OPC, OPC UA sowie Protokolle, die von Webinterfaces genutzt werden, angeboten.

In der werksseitig ausgelieferten Konfiguration sind oftmals viele Hard- und Software-Schnittstellen, die die verschiedenen Protokolle nutzen, von vornherein aktiviert. Jedoch werden nicht alle Schnittstellen für den vorgesehenen Einsatzzweck benötigt. Die nicht erforderlichen Hard- und Softwareschnittstellen sollten daher deaktiviert werden.

Bei den übrigen, d. h. erforderlichen Hard- und Software-Schnittstellen, sollten angemessene Sicherheitsfunktionen aktiviert bzw. gleichwertige alternative Maßnahmen umgesetzt werden (siehe auch IND.2.1.M2 *Nutzung sicherer Übertragungs-Protokolle für die Konfiguration und Wartung*).

IND.2.1.M5 ENTFALLEN

Die zugehörige Anforderung ist entfallen.

IND.2.1.M6 Netzsegmentierung (B)

Als Grundlage für die Netzsegmentierung ist im Rahmen der Dokumentation (siehe auch IND.1.M5 *Entwicklung eines geeigneten Zonenkonzepts*) zu erfassen, mit welchen anderen Komponenten und Systemen die ICS-Komponente in Kommunikation steht. Sämtliche Kommunikationsprotokolle, die eingesetzt werden, und sämtliche Kommunikationsendpunkte sollen erfasst werden.

Auf Basis dieser Informationen kann eine Einschränkung der Kommunikationsverbindungen erfolgen anhand

1. der Kommunikationsprotokolle oder
2. der Kommunikationsendpunkte.

Netzbasierte lokale Zugriffskontrolle (Host-Firewall)

Die Kommunikationsbeziehungen in einer ICS-Umgebung sind in vielen Fällen deterministisch und nur selten Änderungen unterworfen. Durch eine Host-Firewall können nicht vorgesehene Kommunikationswege unterbunden und unzulässige Verbindungsversuche detektiert werden. Zu diesem Zweck sollte insbesondere der Zugriff auf administrative Dienste über die externe Schnittstelle auf berechtigte Netzbereiche und Gegenstellen beschränkt werden. Unzulässige und abgewiesene Verbindungen sollten als Grundlage für die Detektion von Anomalien protokolliert werden.

Die Erstellung des Regelwerks sollte gemäß den Vorgaben des Bausteins NET.3.2 *Firewall* erfolgen.

IND.2.1.M7 Erstellung von Datensicherungen (S)

Die Daten auf einer ICS-Komponente sollten gesichert werden. Sämtliche Steuerungsprogramme und Konfigurationen sollten gesichert werden. Diese Daten sollten bei jeder Änderung in einem Archiv hinterlegt werden.

Vor jeder Systemänderung an einer ICS-Komponente müssen zusätzlich Backups erstellt werden. Im Notfall sollte der unmittelbare Zugriff auf die Datensicherungen gewährleistet sein.

Es sollte regelmäßig geprüft werden, ob das Einspielen der Sicherungen funktioniert, um im Notfall schnell darauf zurückgreifen und ein fehlerfreies Einspielen der Sicherungen gewährleisten zu können (siehe auch IND.1.M13 *Notfallplanung für OT* sowie Baustein CON.3 *Datensicherungskonzept*).

IND.2.1.M8 Schutz vor Schadsoftware (S)

Virenschutzprogramme können nicht auf allen OT-Komponenten installiert werden. Mögliche Einschränkungen können sich aus einer fehlenden Herstellerfreigabe, nicht unterstützten Betriebsplattformen (z. B. Feldsysteme oder SPS), fehlenden Möglichkeiten zur Aktualisierung von Virensignaturen oder potentiellen Risiken in der Verfügbarkeit ergeben. So müssen folgende Fälle unterschieden werden:

Fall 1: Auf einer OT-Komponente kann ein eigenes Virenschutzprogramm installiert werden. Dann kann diese OT-Komponente in das allgemeine Konzept zum Schutz vor Schadprogrammen eingefügt werden (siehe IND.1.M3 *Schutz vor Schadprogrammen*).

Fall 2: Auf einer OT-Komponente kann **kein** eigenes Virenschutzprogramm installiert werden. Die Zone, in der sich die Komponente befindet, ist jedoch ausreichend abgesichert (siehe IND.1.M3 *Schutz vor Schadprogrammen*).

Fall 3: Auf einer OT-Komponente kann kein eigenes Virenschutzprogramm installiert werden und die Zone, in der sich die Komponente befindet, ist **nicht** ausreichend abgesichert. In diesem Fall müssen für die einzelne Komponente **alternative** technische oder organisatorische Schutzmaßnahmen umgesetzt werden.

Die folgenden **alternativen technischen** Schutzmaßnahmen können z. B. gewählt werden:

- Absicherung von Außenschnittstellen einer OT-Komponente (Standortanbindungen, Zugänge von Dienstleistern, Schnittstellen zum Office-Netz und dem Internet),
- Ausgliedern von bedrohten Systemen in abgesicherte Netzsegmente (mit einer Filterkomponente, falls eine Verbindung zu anderen Zonen notwendig ist (siehe Abschnitt *Virus-Wall* unten)),
- Einschränken des Gebrauchs von Wechseldatenträgern (z.B. USB-Datenträger):
    - Deaktivieren von Systemschnittstellen,
    - Einsatz einer Wechseldatenträgerschleuse,
- Etablieren von netzbasierten Zugangskontrollen im Benutzerbereich (Vermeidung von Fremdgeräten),
- Einsatz netzbasierter Schutzsysteme (Application Layer Gateways (ALG)) sowie
- physische Trennung.

Falls möglich, regelmäßiges Scannen der OT-Komponenten von einem Boot-Medium oder USB-Device mit aktuellem Virenschutzprogramm und aktuellen Signaturen, beispielsweise während eines geplanten Wartungsfensters (auf diese Weise kann eine Infektion unter Umständen zumindest rückwirkend erkannt und dann beseitigt werden).

Alternative organisatorische Schutzmaßnahmen können sein

- Regelungen zum Datenaustausch und Gebrauch von Wechseldatenträgern sowie
- Verbot der Anbindung von Fremdgeräten.

Um einen wirksamen Schutz der OT vor Schadprogrammen zu erreichen, sind daher abgestimmte und angemessene Sicherheitsmaßnahmen unter Berücksichtigung der umgebungsspezifischen Besonderheiten auszuwählen und umzusetzen. Auf dieser Basis ist ein Virenschutzkonzept zu erstellen, aus dem hervorgeht, wie der Schutz vor Schadprogrammen erreicht wird (siehe IND.1.M3 *Schutz vor Schadprogrammen*).

IND.2.1.M9 ENTFALLEN

Die zugehörige Anforderung ist entfallen.

IND.2.1.M10 ENTFALLEN

Die zugehörige Anforderung ist entfallen.

IND.2.1.M11 Wartung der ICS-Komponenten (S)

Die zum Teil sehr hohen Anforderungen an die Verfügbarkeit erfordern einen speziellen Umgang bei Änderungen an den ICS-Komponenten. Veränderungen an den Komponenten, wie der Austausch von Steuerprogrammen oder ein Update der Firmware, sind daher nur in Wartungsfenstern durchführbar.

Daher sollte in diesem Zeitraum auch das Einspielen von Sicherheits-Updates oder die Aktualisierung von Security-Einstellungen eingeplant werden.

Spezielle Wartungsfenster sollten kurzfristig berücksichtigt werden können, falls ein kritisches Sicherheits-Update von einem Hersteller bereitgestellt wird und im Rahmen der Risikoanalyse festgestellt wird, dass es erforderlich ist, dieses schnell zu berücksichtigen. Es muss dann kurzfristig in den Produktionsvorgang eingeplant werden oder die betroffene Komponente muss bis zum Einspielen des kritischen Sicherheitsupdates von der Außenwelt abgeschottet werden (siehe IND.2.1.M6 *Netzsegmentierung*).

IND.2.1.M12 ENTFALLEN

Die zugehörige Anforderung ist entfallen.

IND.2.1.M13 Geeignete Inbetriebnahme der ICS-Komponenten (S)

Vor der Inbetriebnahme müssen Automatisierungsgeräte in eine sichere Grundkonfiguration gebracht werden. Hierzu bietet es sich an, eine sichere Referenzkonfiguration zu erstellen, diese als Konfigurationsvorlage für einen bestimmten Gerätetyp zu hinterlegen und die Einstellungen zu dokumentieren. Weitere Systeme können daraufhin auf Basis dieser Referenzkonfiguration in Betrieb genommen werden.

Die auf den Systemen vorhandenen Sicherheitsfunktionen sollten grundsätzlich aktiviert werden, sofern daraus keine negativen Implikationen auf den Betrieb entstehen. Diese Maßnahmen umfassen insbesondere:

Integritätsprüfungen

Bei verfügbaren Funktionen zur Selbstdiagnose und Integritätsprüfung sicherheitsrelevanter Systemmodule und -konfigurationen sollten diese aktiviert und das Verhalten beim Fehlschlagen der Integritätsprüfung festgelegt werden (z. B. ob bei Integritätsverletzungen automatisierte Eingriffe notwendig sind). Festgestellte Fehler und Integritätsverletzungen sollten protokolliert und möglichst aktiv signalisiert werden. Insofern dies möglich und sinnvoll ist, sollte das System seine Funktion bis zu einem manuellen Eingriff weiterhin wahrnehmen.

Festgestellte Integritätsverletzungen sollten bis zur Entkräftung grundsätzlich als Sicherheitsvorfall eingestuft und nach den organisationsinternen Regelungen bearbeitet werden. Ein solches Ereignis sollte im Reaktionsplan für Störungen berücksichtigt sein.

Aktivierung der Systemprotokollierung

Die Protokollierung sicherheitsrelevanter Ereignisse ist eine wichtige Grundlage für die Detektion von Anomalien und muss daher für jede ICS-Komponente aktiviert werden (siehe IND.1.A18 *Protokollierung* sowie IND.1.M10 *Monitoring, Protokollierung und Detektion*).

Initiales Patchen

Vor der Inbetriebnahme sollten die Automatisierungsgeräte zudem auf den aktuellen, intern freigegebenen Firmware-, Software- und Patch-Stand gehoben werden, da in der Regel Updates im Betrieb nicht immer zeitnah erfolgen können.

IND.2.1.M14 ENTFALLEN

Die zugehörige Anforderung ist entfallen.

IND.2.1.M15 ENTFALLEN

Die zugehörige Anforderung ist entfallen.

IND.2.1.M16 Schutz externer Schnittstellen (S)

Alle nach außen sichtbaren, physischen Anschlüsse der ICS-Komponente (Hardware-Schnittstellen, z. B. Ethernet, Feldbus, USB) sollten geschützt werden. Dies kann z. B. durch ein Schloss erfolgen. Alternativen können Siegel sein, die in regelmäßigen Abständen kontrolliert werden.

IND.2.1.M17 Nutzung sicherer Protokolle für die Übertragung von Mess- und Steuerdaten (S)

Für IP-basierte Protokolle kann auf etablierte Transportprotokolle wie z. B. TLS zurückgegriffen werden, um den Schutz zu realisieren. Alternativ kann der Schutz durch das Anwendungsprotokoll erfolgen. Eine mögliche Lösung ist die Nutzung der Schutzmechanismen zur Verschlüsselung und Signatur von OPC UA.

Bei dem Einsatz sind die Anforderungen an sichere kryptographische Verfahren zu beachten.

Bei Feldbussen bzw. ähnlichen Systemen mit sehr kurzen Reaktionszeiten und Echtzeitanforderungen sollte entsprechend dem Schutzbedarf der übertragenen Steuerungsinformationen entschieden werden, wie ein Schutz erfolgen kann bzw. ob dieser notwendig ist.

IND.2.1.M18 Kommunikation im Störfall (H)

Die Sicherheitskonfiguration darf hierbei die Handlungsfähigkeit in Störungs- und Notfallsituationen nicht beeinträchtigen. Daher sollte eine lokale und im Bedarfsfall auch über den Fernzugriff nutzbare Out-Of-Band-Schnittstelle vorgesehen sein. Eine solche Schnittstelle kann über eine lokale Administrationsschnittstelle realisiert werden, z. B. über eine serielle Schnittstelle, über eine Kernel-basierte virtuelle Maschine (KVM) für den Fernzugriff sowie über einen redundanten netzbasierten Administrationsweg.

IND.2.1.M19 Security-Tests (H)

Richtlinien und Prozesse dienen der Vermeidung von Schwachstellen. Wenn höherer Schutzbedarf insbesondere bezüglich Integrität (Manipulationssicherheit gegenüber Angriffen), aber auch Bedenken in Bezug auf Denial-of-Service (Verfügbarkeit) oder Wissensabfluss (Vertraulichkeit) bestehen, empfiehlt es sich, die in diesem Umsetzungshinweis beschriebenen vorbeugenden und ermittelnden Maßnahmen für Schadensfälle mit realistischen, praktischen Tests des tatsächlichen, effektiven Sicherheitsniveaus zu ergänzen. Die Tests sollen mögliche Regelungslücken, Fehler oder Unaufmerksamkeiten aufdecken und diese einer geeigneten Beseitigung (auch für die Zukunft) zuführen. Denn nicht alle Schwachstellen können durch Konfiguration, Richtlinien oder Prozesse entdeckt und geschlossen werden.

Zu diesem Zweck kann ein technisches Audit durchgeführt werden, das die Automatisierungsgeräte in den Geltungsbereich mit einschließt.

Bestandteile eines technischen Audits in der OT

Ein technisches Audit kann folgende Prüfungen umfassen:

- **Konfigurationsreview**
  Prüfung der tatsächlich auf den Systemen vorzufindenden Konfiguration und Abgleich mit dem Soll-Zustand (idealerweise aus der Dokumentation, sinnvollerweise zusätzlich mit Best Practices, sofern die Dokumentation von diesen abweicht bzw. unvollständig ist).
- **Code-Review**
  Dies dürfte im Bereich Automatisierungsgeräte seltener vorkommen, da große Teile des Codes wie die Firmware in der Regel nicht frei verfügbar sind. Immerhin lassen sich öffentlich verfügbare Teile des Codes wie etwa HTML- und JavaScript-Code einer Weboberfläche auf Schwachstellen untersuchen. Grundsätzlich kann auch der Code von Anwendungsprogrammen einem Review unterzogen werden, insofern diese Sicherheitsfunktionen realisieren oder unterstützen.

- **Penetrationstest**
  Hierbei handelt es sich um tatsächliche absichtliche Angriffsversuche, deren Auswertung Rückschlüsse auf Schwachstellen ermöglicht, die teilweise mit keiner anderen Methode gefunden werden können. Penetrationstests (kurz Pentests) können mit unterschiedlichem Tiefgang und mit variabler Aggressivität durchgeführt werden.

Planung und Durchführung eines technischen Audits in der OT

Für sämtliche Arbeiten an einem ICS sollten dringend für die jeweilige Arbeit **qualifizierte Fachkräfte** eingesetzt werden, die dafür tiefgehend geschult oder aber eingekauft werden können.

Die ersten Security-Tests werden idealerweise bereits frühzeitig durchgeführt. Ein sinnvoller Zeitpunkt ist vor der Abnahme des Systems bzw. bei der Integration in die Anlage (System Acceptance bzw. Factory Acceptance Test). Hier kann gleichzeitig die Security überprüft werden.

Es bietet sich an, weitere Tests mit den erforderlichen Wartungsmaßnahmen zu koordinieren, um die Folgen möglicher Beeinträchtigungen abzumildern.

Die Tests sollten gründlich geplant und regelmäßig durchgeführt werden, um die sich weiterentwickelnden Angriffsmethoden und -tools berücksichtigen zu können.

Die Ergebnisse des Audits sollten nachvollziehbar dokumentiert werden und in eine priorisierte Liste empfohlener Maßnahmen münden. Dafür ist üblicherweise ein Bewertungsschema entlang des Schweregrads nützlich. Letzterer kann sich etwa aus Komplexität der Ausnutzung einer Schwachstelle und möglicher Schadenshöhe zusammensetzen. Eine Bewertung von Eintrittswahrscheinlichkeiten ist in der Regel nicht zielführend, da zu wenig verlässliche Daten hierzu vorliegen, insbesondere für seltene, aber kritische Ereignisse.

Penetrationstests in der OT

Für Penetrationstests in der OT sollten einige Besonderheiten beachtet werden. Aufgrund der Unterschiede zur Büro-IT sollten für Sicherheitstests sogenannte **Whitebox-Tests** gewählt werden. Um das Risiko von Ausfällen und sonstigen Störungen zu mindern, sollten die Tests mit möglichst viel Vorinformation durchgeführt werden.

Blackbox-Tests ohne weiteres Vorwissen sind nicht nur risikoreicher, sondern auch ineffektiver, da viel Zeit mit vergeblicher Suche verschwendet wird. Unter bestimmten Rahmenbedingungen können Blackbox-Tests jedoch nötig sein.

Die **„Aggressivität" des Tests** ist angemessen zu wählen und zwischen Betreiber und Testpersonal abzustimmen. Hierbei können im Lauf des Tests Anpassungen notwendig werden, wenn Störungen aufgetreten sind oder aber der Test sehr stabil verläuft und nicht schnell genug voranschreitet. Parameter, die in die Bestimmung der optimal angemessenen Aggressivität eingehen sollten, sind u. a.

- Schutzbedarf des gesteuerten Prozesses,
- Alter und Sicherheits-Reifegrad der IT-Komponenten der Automatisierungsgeräte,
- Erfahrung der Tester sowie
- Typ und Funktion weiterer Geräte im Netzsegment.

Im Zweifel sollte mit einer niedrigeren Aggressivität begonnen werden, die in stetiger Abstimmung mit dem Betreiber gesteigert werden kann.

Viele **Tools für Penetrationstests in der OT** senden eine sehr große Zahl unterschiedlichster Pakete, um aufgrund der Reaktionen Rückschlüsse auf Schwachstellen zu ziehen. Dies betrifft vor allem Schwachstellenscanner, aber auch bestimmte Portscanner bzw. deren Betriebsmodi. Teilweise kann jedoch allein die Anzahl an Paketen einer bestimmten Art vor allem ältere Geräte im Segment instabil werden lassen.

Pentest-Tools müssen daher mit Bedacht eingesetzt werden, um Ausfälle des ICS zu vermeiden. In der Regel hat im industriellen Umfeld die Verfügbarkeit von Mess-, Steuer-, Regel- und Konfigurationsdaten für die Automatisierungsaufgabe die höchste Priorität. Geeignete Pentest-Tools können zum einen sogenannte

Baseline Analyzer sein, die Systemkonfigurationen auslesen und mit einem Sollzustand abgleichen. Zum anderen handelt es sich um Scans mit Schwachstellenscannern, bei denen diese (idealerweise administrative) Zugangsdaten zu den zu testenden Systemen erhalten. Derartige „credentialed scans“ können jedoch nicht alle Tests ersetzen, da nicht alle Arten von Schwachstellen aus dem System verlässlich auszulesen sind. U. a. betrifft dies alle Schwachstellen, die nur durch Fuzzing gefunden werden können.

- **Lauschen**: Noch weniger mögliche Störungen verursacht das reine Belauschen des Netzverkehrs. Sogenannte passive Schwachstellenscanner können bestimmte Arten von Schwachstellen durch reine Beobachtung des Netzverkehrs erkennen, ohne aktiv einzugreifen. Diese Scanart kann bei besonders sensiblen Geräten und Zonen oder zur anfänglichen Informationssammlung eingesetzt werden. Die Zahl der Schwachstellen, die so gefunden werden können, ist allerdings prinzipiell begrenzt.
- **Testsystem**: Bei einigen Betreibern existiert ein Testsystem oder sogar eine Test-Anlage, auf der der Sicherheitstest durchgeführt werden kann. In der Regel unterscheiden sich solche Testsysteme jedoch mehr oder weniger stark vom Produktivsystem, manchmal in Patchstand oder Konfiguration, in der Regel aber zumindest in fehlenden Außenanbindungen. Daher können die Ergebnisse des Tests nicht komplett übertragen werden. Es bietet sich allerdings an, wenn vorhanden, die Testparameter zunächst am Testsystem auszuprobieren und danach auf das Produktivsystem überzugehen.
- **Spezialisierte Tools**: Neben Standard-Pentest-Tools existieren auch auf ICS-spezialisierte Tools oder Erweiterungspakete. Diese haben den Vorteil, dass sie in der Regel mehr ICS-spezifische Schwachstellen kennen als Standardtools. Dies erhöht einerseits das Risiko von Störungen und fordert daher besondere Vorsicht. Andererseits verschicken derartige Tools ggf. weniger willkürliche Pakete und tragen daher ein etwas geringeres Risiko, alte, instabile Legacy-Geräte in Mitleidenschaft zu ziehen.

Für optimale Ergebnisse sollten mehrere Tools, allgemeine wie spezialisierte, kombiniert werden.

IND.2.1.M20 Vertrauenswürdiger Code (H)

Über Updates von Firmware oder anderer Software kann bösartiger Code in Automatisierungsgeräte gelangen. Um wirksam zu verhindern, dass Angreifer unbemerkt Schadprogramme oder -routinen einspielen können, sind zusätzliche Maßnahmen notwendig.

Firmwareupdates sollten vom Hersteller kryptographisch abgesichert sein und vom Gerät überprüft werden. Dies erfordert, dass der Hersteller eine entsprechende Signatur-Infrastruktur betreibt und für jedes Update nutzt.

Bei dieser Signatur-Infrastruktur sollten folgende Funktionen eingesetzt werden:

- kryptographisch sichere Funktionen, zumindest eine sichere digitale Signatur (Checksummen genügen nicht, da diese vom Angreifer leicht berechnet werden können) sowie
- eine sichere Hashfunktion, um aus der gesamten Firmware bzw. Software einen zu signierenden Fingerabdruck zu berechnen (z. B. SHA-2).

Der Hersteller sollte Mechanismen in die Automatisierungsgeräte einbauen, die die genannten Funktionen verlässlich korrekt überprüfen. Jedes Automatisierungsgerät sollte einen Vertrauensanker enthalten, um die Vertrauenskette überprüfen zu können, z. B. ein Zertifikat bzw. einen öffentlichen Schlüssel, der nicht verändert werden kann. Bei einer Verletzung der Integrität sollten die Automatisierungsgeräte geeignet reagieren, z. B. mit einer deutlichen Warnung. Die korrekte Reaktion auf eine solche Warnung muss dokumentiert sein.

Um die Funktionalität robust gegen Veränderungsversuche zu machen, sollte sie in schwer zu manipulierende Hardware wie etwa ein HSM (Hardware-Sicherheitsmodul) integriert sein.

Ggf. kann diese oder eine ähnliche Infrastruktur auch für Anwendungsprogramme genutzt werden. Dies ist allerdings komplex zu implementieren, da hierfür der Betreiber Signaturschlüssel benötigt, die von den Automatisierungsgeräten überprüft werden.

Eine weitere Möglichkeit, Vertrauenswürdigkeit durch den Code zu schaffen, ist die Verschlüsselung zentraler Bestandteile, die geschäftskritisches Know-how beinhalten. Hierfür muss das Automatisierungsgerät in der Lage sein, bei Bedarf die Entschlüsselung eigenständig vorzunehmen. Damit

die dafür notwendigen Schlüssel nicht leicht entwendet werden können, sollten sich auch diese in sicherer Hardware (HSM) befinden.

2.2. Maßnahmen zum Baustein ORP.4 Identitäts- und Berechtigungsmanagement

IND.2.1.ORP.4.M2 Regelung für Einrichtung, Änderung und Entzug von Berechtigungen (B)

Für den Betrieb entbehrliche Konten sollten entweder entfernt oder deaktiviert werden. Dies betrifft insbesondere auch Zugangsdaten für Verwaltungsschnittstellen wie eine Web-Oberfläche oder SNMP. Das Entfernen von Benutzerkonten kann Einfluss auf den Betrieb eines Geräts haben und steht unter dem Vorbehalt der Herstellerfreigabe. Verbleibende aktivierte und deaktivierte Konten sollten auf unsichere Standard- oder Initialpasswörter geprüft (letztere zum Schutz bei versehentlicher Reaktivierung) und es sollten unter Berücksichtigung der geltenden Regelungen zum Passwortgebrauch neue Passwörter gesetzt werden.

3. Weiterführende Informationen

3.1. Wissenswerte

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind.

Weiterführende Literatur

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen im Personalbereich finden sich unter anderem in folgenden Veröffentlichungen:

Mit dem *ICS-Security-Kompendium* bietet das Bundesamt für Sicherheit in der Informationstechnik (BSI) Maßnahmen für die IT-Sicherheit von ICS.

Mit dem *ICS-Security-Kompendium für Hersteller und Integratoren* bietet das Bundesamt für Sicherheit in der Informationstechnik (BSI) Maßnahmen für die IT-Sicherheit in ICS für Hersteller und Integratoren von ICS.

Der Bundesverband der Energie- und Wasserwirtschaft e. V. (BDEW) und Österreichs E-Wirtschaft bietet mit dem Dokument *Whitepaper: Anforderungen an sichere Steuerungs- und Telekommunikationssysteme* eine Hilfestellung zum sicheren Betrieb von Steuerungs- und Telekommunikationssystemen.

Das National Institute of Standard and Technology (NIST) gibt mit der Veröffentlichung *Guide to Industrial Control Systems (ICS) Security: NIST Special Publication 800-81* Empfehlungen und Hilfestellungen zur Verankerung der Informationssicherheit im ICS-Umfeld.

3.2. Quellenverweise

Für den Umsetzungshinweis UH_IND.2.1 *Allgemeine ICS-Komponente* sind keine Quellenverweise vorhanden.