Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise zum Baustein: IND.1 Prozessleit- und Automatisierungstechnik

1. Einleitung

Betriebstechnik (englisch: Operational Technology, OT) ist Hard- und Software, die Änderung durch die direkte Überwachung sowie Steuerung von physikalischen Geräten, Prozessen und Ereignissen in der Institution erfasst und bewirkt.

In der Industrie, zu der unter anderem auch die Kritischen Infrastrukturen gehören, zählen zur OT insbesondere industrielle Steuerungssysteme (Industrial Control Systems, ICS) mit Automatisierungslösungen, die Steuerungs- und Regelfunktionen aller Art übernehmen (siehe auch 3.1 *Wissenswertes*, Abschnitte *Begriffsbestimmungen*, *Grundcharakteristika der OT*). Weitere Beispiele für Betriebstechnik sind Laborgeräte (z. B. automatisierte Mikroskope oder Analysewerkzeuge), Logistiksysteme (z. B. Barcodescanner mit Kleinrechner) oder die Gebäudeleittechnik.

Die in der Vergangenheit übliche physische Trennung der OT von anderen IT-Systemen und Netzen in Büroanwendungen ist heute aufgrund zunehmender Integrationsanforderungen nur in Ausnahmefällen bei erhöhtem Schutzbedarf anwendbar. Mehrstufige Produktionsschritte und deren übergreifende Steuerung wie auch regulatorische Anforderungen erfordern eine zunehmende Öffnung auch über

Organisationsgrenzen hinweg. Diese Entwicklung wird durch den Trend zur Optimierung von Fertigungsprozessen zur Steigerung der Wettbewerbsfähigkeit im Rahmen von Industrie 4.0 beschleunigt.

Da neben OT-spezifischen Komponenten zunehmend IT-Komponenten und Techik aus der Büro-IT in der OT eingesetzt werden, ist die OT inzwischen vergleichbaren Gefährdungen ausgesetzt wie die Büro-IT. Zugleich weist die OT gegenüber der klassischen IT wesentliche Unterschiede auf, die das Anwenden dort etablierter Sicherheitsverfahren erschweren. So kann es Restriktionen aufgrund von Herstellervorgaben oder gesetzlichen Anforderungen geben, die Veränderungen an Komponenten verhindern oder erschweren. Beispiele hierfür sind die Anwendung von Sicherheitsupdates oder nachträgliche Härtungsmaßnahmen. Die OT unterliegt in der Regel auch deutlich längeren Lebenszyklen, häufig über die Herstellerunterstützung hinaus, sodass auch die Verfügbarkeit von Sicherheitsupdates nicht durchgängig gewährleistet werden kann.

Diese zunehmende Angleichung der OT- und der IT-Technik wird zukünftig eine vermehrte Zusammenarbeit zwischen den Wissensträgern beider Funktionsbereiche fordern. Das Know-how für IT, Kommunikation und Cyber-Defense liegt derzeit in den meisten Fällen bei den Abteilungen der Büro- und Gebäude-IT. Eine erfolgreiche Lösung muss aber die Gegebenheiten der OT-Infrastruktur weitestgehend berücksichtigen. Dies kann jedoch nur mit der Unterstützung der Zuständigen für die OT erfolgen.

2. Maßnahmen

Im Folgenden sind spezifische Maßnahmen für die Anforderungen des Bausteins IND.1 *Prozessleit- und Automatisierungstechnik* sowie für weitere Bausteine aufgeführt, die hiermit im Zusammenhang stehen: ORP.3 *Organisation und Personal*, OPS.1.1.4 *Schutz vor Schadprogrammen* sowie NET.1.2 *Netzmanagement*.

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.1 Prozessleit- und Automatisierungstechnik

IND.1.M1 Einbindung in die Sicherheitsorganisation (B)

Es muss ein Managementsystem für Informationssicherheit (ISMS) für die OT-Infrastruktur etabliert werden. Dieses OT-ISMS kann entweder als selbständiges ISMS oder als Teil eines Gesamt-ISMS existieren und sollte in seinem Geltungsbereich die Definition von Zielen und Werten, Prozessen, Zuständigkeiten (Rollen), sowie Vorgaben für die OT-Infrastruktur explizit umfassen.

Insbesondere sollte auf die besonderen Anforderungen der OT eingegangen werden, die sich aus den besonderen Rahmenbedingungen wie z. B. Regelungen zur Gewährleistung ableiten lassen. Hierbei sollten die alternativen Vorgehensweisen zur Büro- und Gebäude-IT skizziert werden.

Aufbau einer Sicherheitsorganisation

Die Institution muss eine Sicherheitsorganisation aufbauen, welche die Zuständigkeiten für die Informationssicherheit der OT, sowohl für die OT-Infrastruktur als auch für die OT-Komponenten, regelt. Dabei sollte die Sicherheitsorganisation alle an dem Betrieb von OT-Komponenten beteiligten Parteien berücksichtigen (z. B. Hersteller, Integrator bzw. Maschinenbauer, Outsourcing-Partner, Drittanbieter, Spezialisten für die physische Sicherheit, Produktions- und Instandhaltungsleiter).

Es muss eine Person bestimmt werden, die für die Informationssicherheit in der OT insgesamt zuständig ist. Diese Person muss innerhalb der Organisation bekannt sein. Im Folgenden wird dieser als ICS-Informationssicherheitsbeauftragter bezeichnet. In größeren Institutionen sollte zudem für jede Anlage, alternativ je Komponententyp, Schicht oder Zone ein Zuständiger für die Informationssicherheit bestimmt werden.

Dabei können sowohl eine Sicherheitsorganisation für die gesamte Institution aufgebaut und betrieben werden, welche die Bereiche der Büro- und Gebäude-IT sowie der OT umfasst, als auch getrennte

Sicherheitsorganisationen für die beiden Bereiche. Um Synergien zu nutzen und Fehlplanungen sowie Risiken zu vermeiden, muss eine enge Kooperation zwischen den OT-Experten und den Experten für die Büro- und Gebäude-IT stattfinden. Welche Struktur für eine Organisation geeignet ist, hängt stark von den vorhandenen Strukturen und eingespielten Prozessen in einer Institution ab. Entscheidend ist, dass ein Informations- und Wissensfluss in beide Richtungen stattfindet und die jeweils Zuständigen in ihren Bereichen ernst genommen werden. Dafür müssen beide Seiten offen für die jeweiligen Besonderheiten des anderen Bereichs sein und zur Vermeidung von Missverständnissen die Kultur und Sprache der anderen Seite berücksichtigen. Eine Doppelspitze (Informationssicherheitsbeauftragter (ISB) und ICS-Informationssicherheitsbeauftragter) kann in manchen Institutionen eine sinnvolle Lösung sein, wenn Aufgabenteilung und Schnittstellen eindeutig und schriftlich geklärt sind.

Beachtung gesetzlicher Rahmenbedingungen

Gesetzliche, regulatorische und sonstige besondere Vorgaben für die OT sowie für die jeweilige Branche bzw. den jeweiligen Sektor müssen bekannt sein und in ihren Auswirkungen für die Institution interpretiert werden. Dies gilt insbesondere für Institutionen, die kritische Infrastrukturen betreiben, aber auch zunehmend in anderen Bereichen. Neben den nationalen Vorgaben sind möglicherweise auch europäische und internationale Bestimmungen zu beachten. Es sollten Zuständigkeiten und Prozesse eingerichtet werden, um sicherzustellen, dass alle relevanten Anforderungen zeitnah den entscheidenden Stellen bekannt gegeben werden.

Festlegung und Einhaltung von Vorgaben

Es sollte ein Prozess existieren, wie konkrete Vorgaben für bestimmte Themenbereiche (Richtlinien) im ICS-Bereich verfasst, kommuniziert, fortgeschrieben, bewertet und umgesetzt werden. Diese können teilweise, wo angemessen und vorhanden, aus dem Bereich der Büro- und Gebäude-IT übernommen werden. Häufig sind jedoch Anpassungen notwendig, um die Besonderheiten der OT zu reflektieren.

Bei der Auswahl von Komponenten sollte eine Überprüfung von definierten (d. h. sowohl funktionalen als auch für die Informationssicherheit relevanten) Anforderungen durchgeführt werden. Dabei können einzelne Komponenten bis hin zur gesamten OT Prüfgegenstand sein.

Weiterführende Informationen

Weiterführende Informationen zu Aufbau und Gestaltung der Sicherheitsorganisation sind im Baustein ISMS.1 *Sicherheitsmanagement* dokumentiert.

IND.1.M2 ENTFALLEN (B)

Die zugehörige Anforderung ist entfallen.

Die Maßnahme wurde überführt in IND.1.ORP.3.M6 *Planung und Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit* (siehe 2.2 *Maßnahmen zum Baustein ORP.3 Organisation und Personal*).

IND.1.M3 Schutz vor Schadprogrammen (B)

Ein Konzept zum Schutz vor Schadprogrammen muss die bedrohten OT-Komponenten sowie alle möglichen Infektionswege betrachten, Risiken bewerten und wo notwendig geeignete technische und organisatorische Schutzmaßnahmen festlegen.

Zu den möglichen Infektionswegen gehören unter anderem:

- alle Außenschnittstellen inkl. Verbindungen zum Büro- und Gebäude-Netz, Internet und sonstigen Extranets,
- Wechseldatenträger,
- Service-Stationen und Programmiergeräte, auch von Dienstleistern, sowie
- neu beschaffte Komponenten, z. B. Festplatten, USB-Sticks oder Software. Diese können grundsätzlich Schadsoftware enthalten.

Virenscanner

Ist die Installation und der uneingeschränkte Betrieb von Virenschutzprogrammen auf OT-Komponenten möglich und durch den Hersteller oder Integrator freigegeben, sollten diese Systeme automatisiert mit aktuellen Viren-Signaturen versorgt werden.

Sichere Konfiguration von Virenschutzprogrammen

Aufgrund der hohen Verfügbarkeitsanforderungen in der OT sollte bei kritischen Systemen unter Umständen eine angepasste Konfiguration für Virenschutzprogramme verwendet werden. Dabei sollten Einstellungen deaktiviert werden, die zu einer unbeabsichtigten Beeinträchtigung der Produktion führen können (z. B. aufgrund einer hohen Systemlast durch einen Virensuchlauf). Oftmals geben Hersteller nur solche eingeschränkten Konfigurationen zum Betrieb von Virenschutzprogrammen auf den OT-Komponenten frei.

Virenschutzprogramme können gewöhnlich in zwei unterschiedlichen Modi operieren. Entweder kann vor dem Zugriff auf Anwendungen oder Dateien allgemein eine Überprüfung stattfinden oder der Scanvorgang wird manuell oder zeitgesteuert ausgelöst. Gewöhnlich sollte das Virenschutzprogramm automatisiert bei allen Zugriffen scannen.

Die Auswahl sollte dabei in Abhängigkeit von Empfehlung des Herstellers des Virenschutzprogramms und der OT-Komponente erfolgen. Sollte eine kontinuierliche Prüfung (z. B. aus Performance-Gründen) nicht möglich sein, sollten alternative Schutzmaßnahmen ergriffen werden.

Darüber hinaus sollte in regelmäßigen Abständen ein vollständiger Scan aller Daten durchgeführt werden. Ein zusätzlicher, vollständiger Scan mit aktuellen Signaturen sollte nach der Erstinstallation und nach Änderungen am System durchgeführt werden.

Grundsätzlich sollten folgende Einstellungen bei der Konfiguration der Virenschutzprogramme berücksichtigt werden:

- Manuelle Scans sollten ausschließlich bei Stillstand der Produktion durchgeführt und dann auch dokumentiert werden.
- Ausschließlich lokale Medien sollten geprüft werden.
- Netzlaufwerke sollten nicht gescannt werden, um parallele Scans durch mehrere IT-Systeme zu vermeiden. Vorgelagerte Sicherungssysteme sollten diese Aufgabe übernehmen (siehe auch *Virenschutz-Programm auf der Firewall (Virus-Wall)*).
- Nur Administratoren dürfen die Befugnisse haben, das Virenschutzprogramm zu konfigurieren oder zu deaktivieren.
- Das Virenschutzprogramm sollte Funde an eine zentrale Stelle melden. Eine automatische Terminierung der Prozesse und Programme kann bei einem False-Positive-Fund zu einem Ausfall der OT-Komponente führen und ist daher kritisch zu prüfen.

Der Installationsprozess sowie die Konfiguration sollten für jede OT-Komponente dokumentiert werden.

Zentraler Virensignatur-Verteilerdienst

Das OT-Netz sollte soweit möglich autark betrieben werden und nur zwingend notwendige Verbindungen in andere Netze erlauben. Ist eine Verbindung in andere Netze notwendig, so sollte diese nicht direkt erfolgen, sondern stets über einen Proxy-Server geführt werden.

Daher dürfen die Signaturen für das Virenschutzprogramm nicht direkt aus dem Internet, sondern nur über einen zentralen Virensignatur-Verteildienst in der DMZ bezogen werden. Dieser lädt die aktuellen Signaturen stellvertretend aus dem Internet und stellt sie den OT-Komponenten zur Verfügung. Somit sind keine direkten Verbindungen aus dem OT-Netz in das Internet erforderlich.

Zeitnahe Aktualisierung der Viren-Signaturen

Oftmals sind zeitnahe Updates der Virensignaturen und der Virenschutzprogramme auf OT-Komponenten nicht möglich. Daher sind hierbei folgende Aspekte zu berücksichtigen.

Die OT-Komponenten sollten gemäß ihres möglichen Aktualisierungsintervalls in Gruppen unterteilt werden. Zusätzlich sollten redundant ausgelegte OT-Komponenten getrennten Gruppen zugeordnet werden, um beispielsweise auf die Verteilung von fehlerhaften Virensignaturen in der Produktionsumgebung (z. B. False Positives) umgehend reagieren zu können.

Die Verteilung der Virensignaturen in die Gruppen mit redundanten ICS sollte mit einer Zeitverzögerung durchgeführt werden (z. B. 12 Stunden), um bei Problemen weiterhin den Betrieb mit dem zweiten System aufrecht erhalten zu können.

Aufgrund der hohen Verfügbarkeitsanforderungen sollten nur vom Hersteller bzw. Integrator der OT-Komponente freigegebene und als unkritisch klassifizierte Signaturen verteilt werden.

Virenschutzprogramm auf der Firewall (Virus-Wall)

Eine Virus-Wall untersucht den Datenverkehr zwischen zwei Netzen auf Schadprogramme. Auf diese Weise kann sie, stellvertretend für OT-Komponenten mit keinem oder eingeschränktem Virenschutzprogramm, übermittelte Daten prüfen. Dazu werden diese OT-Komponenten in ein separates Netzsegment platziert und der Datenverkehr zu und von diesem Netz durch ein Application Level Gateway (ALG) mit installiertem Virenschutzprogramm gefiltert und auf Schadprogramme untersucht (siehe auch IND.1.M16 *Stärkere Abschottung der Zonen*).

Alternativen für Virenscanner

Virenschutzprogramme können in der Regel nicht auf allen 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, sodass zumeist auch ergänzende oder alternative technische oder organisatorische Schutzmaßnahmen umgesetzt werden müssen.

Alternativ können z. B. die folgenden **technischen** Schutzmaßnahmen ergriffen werden:

- jeweils einheitliche Absicherung von Außenschnittstellen sämtlicher Gruppen von OT-Komponenten (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 *Virenschutzprogramm auf der Firewall (Virus-Wall)*)
- Einschränken des Einsatzes 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))
- Application Whitelisting (Beschränkung von ausführbaren Programmen auf ICS)
- Falls möglich regelmäßiges Scannen der OT-Komponenten von einem Boot-Medium oder einer USB-Einheit mit aktuellem Virenschutzprogramm und aktuellen Signaturen, beispielsweise während eines geplanten Wartungsfensters (auf diese Weise kann eine Infektion zumindest rückwirkend erkannt und dann beseitigt werden)

Alternative **organisatorische** Schutzmaßnahmen können sein:

- Regelungen zum Datenaustausch und Gebrauch von Wechseldatenträgern
- Verbot der Anbindung von Fremdgeräten
- Manuelle Virenprüfung mit speziellen offline-fähigen Antivirus-Lösungen in Wartungsfenstern

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.

Application Whitelisting

(Siehe IND.1.OPS.1.1.4.A3 *Auswahl eines Virenschutzprogramms*)

IND.1.M4 Dokumentation der OT-Infrastruktur (S)

Eine vollständige, aktuelle und praktisch nutzbare Dokumentation der OT ist für einen ordnungsgemäßen Betrieb unabdingbar.

Erst recht gilt dies für die Informationssicherheit, da nur auf dieser Grundlage Notwendigkeit, Angemessenheit und Umsetzungsgrad vieler weiterer Maßnahmen festgestellt und mögliche Schwachstellen und Angriffsvektoren systematisch gefunden werden können.

Die Tiefe der Dokumentation kann variieren. Beispielsweise kann man sich bei einem Prozessleitsystem (PLS), bei dem es sich um geschlossenes Industrial Control System (ICS) handelt, auf die Außenschnittstelle beschränken. Das PLS selbst hat in der Regel eine interne Verwaltung bzw. einen einheitlichen Soft- / Hardware-Stand in Abhängigkeit von der Systemversion des ICS. In anderen Fällen können sämtliche Komponenten dokumentiert werden.

Erstellen und Pflegen der Dokumentation

Die Form der Dokumentationsführung sollte sich an den Bedürfnissen der Zielgruppe orientieren und möglichst praktikabel gestaltet werden. Die Dokumentation kann in Form von einem oder mehreren Dokumenten, eingebettet in eine Website oder in spezifischen Dokumentationswerkzeugen (Tools) für IT-Umgebungen erfolgen. Zu beachten sind jedoch die bestehenden Anforderungen an die Verfügbarkeit der Dokumentation, welche insbesondere auch in Störungs- und Notfallsituationen zugänglich sein muss. Dies kann etwa durch Replikation auf Notsysteme oder als Ausdruck in Papierform am jeweiligen Arbeitsplatz sowie am Notfallstandort erfolgen. Gleichzeitig sollte bei der Ablage auch die Sensibilität der Dokumentation berücksichtigt sein, um unbefugten Zugriffen vorzubeugen.

Der Betreiber muss sicherstellen, dass betriebsrelevante Änderungen in der Anlagendokumentation erfasst werden. Durch regelmäßig durchgeführte Prüfungen auf Aktualität können Versäumnisse im Tagesgeschäft identifiziert und nachgeholt werden.

Anforderungsaustausch mit Integrator und Hersteller

Dort, wo wesentliche Teile einer OT-Infrastruktur von Dienstleistern (Integratoren sowie Maschinen- und Anlagenbauern) aufgebaut und gewartet werden, müssen Anforderungen, Nachweise und Dokumentationen in beide Richtungen weitergegeben werden. Sicherheitsanforderungen sollten möglichst schon im Rahmen der Ausschreibung, spätestens jedoch während der Umsetzung des Projekts an den Auftragnehmer kommuniziert werden.

Der Integrator sollte eine aktuelle und umfassende Dokumentation mitliefern oder erstellen, die Informationen zu Sicherheitsfunktionen, Schwachstellen, Konfigurationen und notwendigen Schutzmaßnahmen enthält. Der Integrator muss sicherstellen, dass die Dokumentation sämtlicher Einzelkomponenten aktuell und umfassend ist.

Bestandsverzeichnis

Um Inkompatibilitäten und Inkonsistenzen von Software in spezifischen Versionen sowie von Konfigurationen (z. B. IP-Adressen-Konflikte) zu vermeiden, sollte in einer Liste die Konfiguration der einzelnen OT-Komponenten dokumentiert sein. Darüber hinaus können auf diese Weise OT-Komponenten schnell identifiziert werden, wenn neue Updates verfügbar oder eine Konfigurationsänderung nötig sind. Auch wenn Updates nicht möglich sind, kann anhand einer solchen Bestandsverzeichnisses in Form einer Liste die potentielle Betroffenheit zeitnah bewertet werden.

Die Liste kann beispielsweise folgende Eigenschaften dokumentieren:

- Funktionaler Name,
- Name des IT-Systems,

- zuständiges Administrationspersonal mit hinterlegten Kontaktdaten (eventuell auch Servicezeiten),
- physischer Aufstellungsort,
- MAC-Adresse(n),
- IP-Adresse(n),
- DNS-Bezeichnung,
- Fully Qualified Domain Name (FQDN),
- Hersteller,
- Modell/Produkttyp
- Betriebssystem,
- installierte Anwendungen und Dienste unter Angabe von Ports und eingesetzten Protokollen,
- Patchstand jeder Software mit dem Datum der Einspielung des Patches (bei IT-Systemen wie SPSen und technisch verwandten Geräten ist es wichtig, Firmware-Stände jeder CPU und jedes Moduls vorzuhalten),
- Datum der letzten Virenprüfung (bzw. Intervall bei automatischer Wiederholung) und
- Backup-Intervall (vollständig und inkrementell), Umfang der Datensicherung und die zuletzt durchgeführte Datensicherung.

Netzplan bzw. Netzstrukturplan

Die Struktur des Netzes sollte in einem physischen und einem logischen Netzplan dokumentiert werden. Soweit für die Umgebung sinnvoll darstellbar, soll der physische Plan die Orte und OT-Infrastruktur, z. B. Kabel, Gebäude und Funkverbindungen darstellen. Der Plan könnte hierzu enthalten:

- Name bzw. Bezeichnung und Funktionalität der Systeme,
- mindestens ein technisches Merkmal, durch das das jeweilige System bzw. Netzsegment identifizierbar ist, z. B.
    - IP-Netzadressen und Netzmasken (z. B. 192.168.1.0/24),
    - IP-Adressen aller angeschlossenen Netzinterfaces (z. B. 192.168.1.54) sowie
    - MAC-Adressen (mindestens dann, wenn und wo nicht primär IP-Kommunikation eine Rolle spielt),
- (falls vorhanden) DNS-Name, bzw.
- (falls vorhanden) FQDN (Fully Qualified Domain Name).

Der logische Netzplan stellt nicht die physischen Gegebenheiten dar. Er fokussiert die strukturelle Sicht und die Sicherheitszonen.

Neben den Kommunikationsmöglichkeiten, die der Netzplan darstellt, sollten auch die Kommunikationsbeziehungen zwischen den Komponenten erfasst werden. Die dargestellten Kommunikationsbeziehungen sagen aus, welche Komponenten miteinander kommunizieren können müssen. Dies ist notwendig, um unbefugten Datenverkehr identifizieren und unterbinden zu können.

Redundanzen (gleichartige Systeme mit analoger Funktion, Konfiguration und gleichem Schutzbedarf) können im Netzstrukturplan zusammengefasst werden, da dies der Lesbarkeit dient. Bei hohem Verfügbarkeitsbedarf sollten die Redundanzen (Anzahl, Typ (etwa Hot-Standby, Failover, Load Balancing etc.)) jedoch aus dem Netzstrukturplan hervorgehen. Dies kann durch Annotierung der Objekte erfolgen, um den Plan selbst nicht aufzublähen.

Administrations- und Benutzerhandbücher

Für den sicheren und unterbrechungsfreien Betrieb ist es notwendig, dass das Service- und Wartungspersonal sowie Administratoren alle Funktionen der OT kennen und diese bedienen können.

Kommt es zu Ausfällen beim Personal (z. B. krankheitsbedingt oder aufgrund einer Kündigung), sollte sichergestellt sein, dass die benötigten Informationen weiterhin in der Institution verfügbar und für die Vertreter zugänglich sind.

Daher sollten für die OT und jede Anwendung ein Administrationshandbuch und ein Benutzerhandbuch verfügbar sein (möglicherweise auch ein Dokument, welches beide Themen abdeckt). Neben betrieblichen Regeltätigkeiten und Abläufen sollten die Dokumente auch Aspekte der Informationssicherheit abdecken, darunter:

- Notwendiges Firewall-Regelwerk (mit Dienst, Protokoll und Port),
- Anweisungen zur Härtung spezifischer Anwendungen,
- Anweisungen zur sicheren Konfiguration,
- spezifische Risiken (z. B. bei der Aktivierung einer bestimmten Konfiguration),
- Systemwiederherstellung (zur Notfallvorsorge).

Die Dokumentationslage sollte die Fortführung des Betriebs durch Dritte ermöglichen.

Energiewirtschaft und andere KRITIS-Sektoren

Für die Energiewirtschaft gelten aufgrund des IT-Sicherheitsgesetzes (IT-SiG) zusätzliche Anforderungen. Hier verlangt der IT-Sicherheitskatalog der Bundesnetzagentur gemäß §11 Absatz 1a des Energiewirtschaftsgesetzes (EnWG) neben der Errichtung eines ISMS, das den Anforderungen der DIN ISO/IEC 27001 in der jeweils geltenden Fassung genügt und bei dessen Implementierung die Normen DIN ISO/IEC 27002 und DIN ISO/IEC TR 27019 (DIN SPEC 27019) in der jeweils geltenden Fassung zu berücksichtigen sind, auch die Erstellung einer bestimmten Form des Netzstrukturplans. Der Netzbetreiber hat eine Übersicht über die vom Geltungsbereich des IT-Sicherheitskatalogs betroffenen Anwendungen, Systeme und Komponenten mit der gesamten verwendeten Technik, die von Bedeutung ist, sowie deren Verbindungen zu erstellen. Die Übersicht ist nach den "Technologiekategorien" „Leitsystem/Systembetrieb“, „Übertragungstechnik/Kommunikation“ und „Sekundär-, Automatisierungs- und Fernwirktechnik“ zu unterscheiden. Kapitel E.IV Tabelle 2 des IT-Sicherheitskatalogs enthält eine kurze Beschreibung zu den "Technologiekategorien" sowie einige Beispiele, welche in der Regel jedoch an die konkrete OT angepasst werden müssen. Im Geltungsbereich des ISMS wie im Netzstrukturplan müssen mindestens die Telekommunikations- und EDV-Systeme enthalten sein, die „für einen sicheren Netzbetrieb notwendig“ sind. Die Definition der letztgenannten Kategorie ist von der Institution vorzunehmen und zu begründen.

Auf andere KRITIS-Sektoren kommen zukünftig ebenfalls Sonderanforderungen zu. Hier muss die jeweilige Regulierung und Umsetzungspraxis beobachtet werden.

Wichtig ist, eine begründete Abgrenzung vorzunehmen, welche Systeme für den sicheren Betrieb der industriellen bzw. KRITIS-Funktionen notwendig sind. Dies kann z. B. im Netzplan geschehen und sollte mit dem Zonenmodell (siehe IND.1.M5 *Entwicklung eines geeigneten Zonenkonzepts*) kompatibel sein.

IND.1.M5 Entwicklung eines geeigneten Zonenkonzepts (S)

Das OT-Netz sollte aus mehreren Netzsegmenten mit individuellen Schutzbedarfen bestehen. Der Datenverkehr zwischen den verschiedenen Ebenen (siehe Abbildung 1: *Ebenen der Automatisierungspyramide*) sollte durch eine Datenflusskontrolle (z. B. mittels Firewall) auf das betrieblich notwendige Maß reglementiert werden.

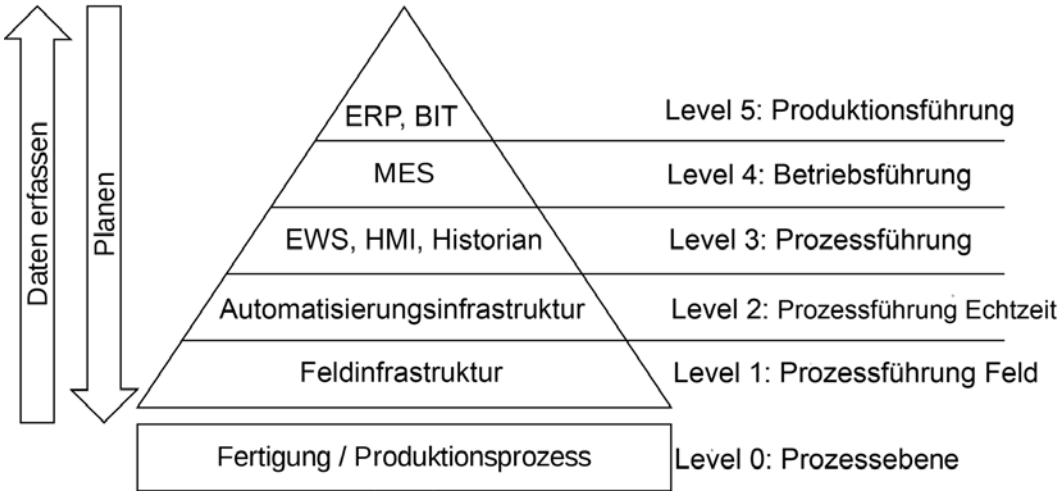

Abbildung 1: Ebenen der Automatisierungspyramide

Neben der Trennung von Netzen mit unterschiedlichen Funktionalitäten auf derselben Ebene sollten auch standortübergreifende Netze oder allgemein organisatorisch unabhängige Maschinen/Anlagen untereinander segmentiert werden (horizontale Segmentierung). So wird z. B. verhindert, dass sich Schadprogramme ungehindert auf alle Maschinen ausbreiten.

Der Verbindungsaufbau sollte grundsätzlich aus dem Netzsegment mit dem höheren Schutzbedarf in das Netzsegment mit dem niedrigeren Schutzbedarf aufgebaut werden.

Eine Umgehung der Netztrennung durch undokumentierte Verbindungen darf nicht stattfinden. Insbesondere sollten keine unkontrollierten Verbindungen zu Netzsegmenten mit unterschiedlichem Schutzbedarf zugelassen werden.

Berücksichtigung institutionsspezifischer Anforderungen und Abhängigkeiten

Bei der Konzeption und Umsetzung des Zonenmodells müssen betriebliche Abhängigkeiten ermittelt und in ihren Auswirkungen untersucht werden. Damit wird die Betriebsstabilität im Rahmen der bestehenden Anforderungen gewährleistet und unter Berücksichtigung der Anforderungen der OT-Umgebung angemessen ausgestaltet. Für die Bewertung sind die Verfügbarkeitsanforderungen jeder Zone gemäß den Anforderungen der technischen Prozesse nach dem Maximalprinzip über alle Systeme der Zone zu bestimmen.

IND.1.M6 Änderungsmanagement im OT-Betrieb (S)

Über die gesamte Lebenszeit der OT gilt es, die Veränderungen an der Anlage und der möglichen neuen Gefährdungen laufend zu berücksichtigen und diesen entsprechend Rechnung zu tragen.

Dokumentation

Beim Betrieb der Anlage gilt es, in die bestehende Dokumentation Änderungen und Anpassungen zu übernehmen. Ziel ist es, stets über eine aktuelle Dokumentation zu verfügen, die den tatsächlichen Zustand der Systeme abbildet. Durch die kontinuierliche Fortschreibung entfallen aufwändige Bestandsanalysen.

Änderungsverwaltung

Administrative Änderungen an der bestehenden Infrastruktur oder an OT-Komponenten können die Informationssicherheit der Umgebung beeinflussen und sollten über einen verbindlichen Änderungsprozess geplant, geprüft, im Rahmen der Möglichkeiten angemessen getestet, durchgeführt und dokumentiert werden. Die Ausprägung des Prozesses ist dabei stark von der jeweiligen Organisation bzw. OT abhängig und sollte nachvollziehbar dokumentiert sein. In weniger komplexen Umgebungen mit einem kleinen Administrationsteam kann der Änderungsprozess im Wesentlichen aus Ablaufvorgaben (Planung, Informationspflichten bei Wartungsarbeiten, Bezug von Software-Updates, Ablauf von Tests (Testkonzept), Regelungen zum Einsatz von Dienstleistern) sowie aus Dokumentationsverpflichtungen (z. B. übergreifendes oder systemgebundenes Administrationsjournal) bestehen. In größeren Organisationen kann ein komplexerer Änderungsprozess bestehend aus Antrags-, Prüfungs-, Test- und Genehmigungsverfahren

bestehen und den Einsatz unterstützender Tools (Formulare, technisch gestützte Arbeitsabläufe, CMDB, etc.) erforderlich machen.

Zeitsynchronisation

Jeder Wechsel der Quelle sowie jede Unterbrechung der Verbindung zur Quelle für den Zeitgeber der Systemzeit müssen fortlaufend erfasst und im Änderungsmanagement lückenlos dokumentiert werden (siehe auch IND.1.NET.1.2.A8 *Zeitsynchronisation*).

IND.1.M7 Etablieren einer übergreifenden Berechtigungsverwaltung zwischen der OT und in der Office-IT (S)

Unter Berechtigungen sind folgende Privilegien von Personen zu verstehen:

- Zutritt (physikalischer Zugriff zu IT-Systemen)
- Zugang (Erreichbarkeit eines Systems über das Netz)
- Zugriff (Ausführbarkeit von Programmen und Funktionen sowie Nutzbarkeit von Daten)

Falsch gesetzte Berechtigungen können die Sicherheit einer OT-Umgebung wesentlich beeinträchtigen. Zu umfangreich oder zu Unrecht vergebene Rechte können durch Missbrauch oder Fehlhandlungen Störungen begünstigen, während zu gering gesetzte Rechte Regelabläufe erschweren und in kritischen Situationen die effektive Störungsbearbeitung behindern können.

Berechtigungen müssen daher bedarfsorientiert nach dem Minimalprinzip vergeben und in Bezug auf Änderungen aktiv gepflegt werden. Hierzu wird ein durchgängiger Prozess (Berechtigungsverwaltung) benötigt.

Die Berechtigungsverwaltung muss die folgenden grundlegenden Anforderungen erfüllen:

Bereitstellen eines Beantragungs-, Prüf- und Freigabeprozesses

Berechtigungen müssen formal beantragt und erfolgreich geprüft werden, bevor sie vergeben werden dürfen. Ein Berechtigungsantrag sollte von zumindest zwei Personen geprüft werden. Die Prüfung könnte durch den jeweiligen Vorgesetzten sowie durch den Zuständigen für die jeweilige Anwendung oder für das jeweilige System erfolgen.

Revisionssichere Pflege einer Bestandsübersicht und Historie

Das Berechtigungsmanagement muss eine vollständige Übersicht über die an eine Person vergebenen Berechtigungen besitzen. Diese Übersicht muss auch die Berechtigungshistorie einer Person sowie Informationen über den jeweils gestellten Berechtigungsantrag und durchgeführten Prüf- und Freigabeprozess umfassen.

Die Bestandsführung von Benutzerkonten und Berechtigungen muss in nutzbarer Form dargestellt und als Grundlage für einen Soll-Ist-Vergleich genutzt werden können.

Verifikation bestehender Zugänge

Die Berechtigungsverwaltung benötigt eine Schnittstelle zum Personalprozess, damit Statusänderungen in Beschäftigungsverhältnissen von Mitarbeitern zeitnah berücksichtigt werden können. Zugänge und Berechtigungen von befristeten und externen Mitarbeitern sollten stets zeitlich befristet für die Dauer des Arbeits- bzw. Beauftragungsverhältnisses angelegt werden.

Ergänzend sollte in einem festgelegten Zyklus (z. B. jährlich) eine manuelle Verifikation der eingerichteten Benutzerzugänge durchgeführt werden.

Bei IT-Berechtigungen sind zudem spezielle Vorgaben zur Berechtigungsverwaltung zu berücksichtigen.

Nutzung persönlicher Benutzerzugänge

Sofern vom System unterstützt, sollten Benutzerzugänge für die interaktive Systemnutzung durch Anwender und Administratoren als persönliche Konten erstellt und dem Besitzer fest zugeordnet werden. Ist

die Nutzung persönlicher Zugänge technisch nicht möglich oder im bestehenden Umfeld nicht sinnvoll umsetzbar, muss die Vergabe von Gruppenzugängen nachvollziehbar bleiben.

Rollenbasierte Berechtigungsvergabe an persönliche Zugänge

Berechtigungen sollten persönlichen Benutzerzugängen grundsätzlich über Berechtigungsgruppen zugeordnet werden. Zur Wahrnehmung einer Benutzerrolle kann ein Benutzerzugang Mitglied einer oder mehrerer Gruppen sein. Die für ein System zur Verfügung stehenden Berechtigungsgruppen werden durch die jeweiligen Systeme und Anwendungen vorgegeben.

Vergabe spezieller Zugriffsberechtigungen

Besondere netzseitige Zugangsberechtigungen, wie diese etwa durch Firewall-Freischaltungen oder Access Control Lists (ACL) auf Screening-Routern eingerichtet werden, werden typischerweise für die Arbeitsplatzrechner bestimmter Personen eingerichtet. Eine solche Zugriffsregel ist somit als Benutzerberechtigung zu verstehen und sollte in der Berechtigungsverwaltung geführt und im Rahmen der regelmäßigen Verifikation überprüft werden.

Die Verwaltung von Berechtigungen kann eigenständig für die OT durch die Institution erfolgen, oder in eine institutionsweite Berechtigungsverwaltung eingebunden sein.

Gruppen

Grundsätzlich ist die Nutzung persönlicher Benutzerzugänge aufgrund der höheren Nachvollziehbarkeit und Anwenderverantwortung zu bevorzugen. In bestimmten Fällen kann jedoch auch die Verwendung funktionaler Gruppenzugänge vertreten werden, wenn sich hierdurch betriebliche Vorteile oder eine verbesserte Verfügbarkeit erreichen lassen, welche mit anderen Mitteln nur aufwändig herzustellen wären. Jeder Gruppenzugang muss separat dokumentiert werden. Die Personen, die Zugriff auf den Gruppenzugang erhalten, müssen organisatorisch (z. B. über Schichtpläne) nachvollziehbar dokumentiert sein. Ein Beispiel könnte die Verwendung eines Zugangs „Bediener“ in einer Warte sein, welche rund um die Uhr besetzt ist und in der sich alle Personen mit Zutritt gegenseitig kennen. Die funktionalen Zugänge müssen ebenso wie andere Zugänge in den ordnungsgemäßen Prozess des Managements von Berechtigungen integriert sein. Es ist insbesondere darauf zu achten, dass jeweils nur die minimal benötigten Rechte erteilt werden. Im Zweifel können verschiedene Aufgaben auf verschiedene Zugänge verteilt werden, sodass idealerweise ein möglichst großer Teil des Personals nur lesenden Zugriff benötigt. Jeder Zugang muss einem Zuständigen zugeteilt sein.

Verantwortung für funktionale und technische Benutzerzugänge

Funktionale Zugänge sollten dem für die Anwendung Zuständigen zugeordnet sein. Technische Benutzer- und Dienstezugänge (etwa für Maschine- zu Maschine-Kommunikation bzw. die Integration mit anderen Anwendungen) sollten den für eine Komponente jeweilig Betriebsverantwortlichen zugeordnet sein.

Passwortverteilung und -management

Es sollte eine Passwortrichtlinie umgesetzt sein. Dabei können sowohl technische Lösungen als auch organisatorische Maßnahmen festgelegt werden. Die Passwortrichtlinie sollte folgende Punkte berücksichtigen:

- Der Benutzer sollte durch Komplexitätsanforderungen daran gehindert werden, schwache Passwörter zu wählen (z. B. Anforderungen an Länge und Zeichenraum, d. h. Alphabet und Zahlen sowie Sonderzeichen).
- Falls die individuellen Gegebenheiten oder der Schutzbedarf es erfordern, sollte das Passwort nach einem vordefinierten Zeitraum geändert werden. Dies gilt z. B. dann, wenn es sich um Geräte mit beschränkter Passwort-Zeichenanzahl, um lokale Passwörter oder um Gruppenpasswörter handelt. Ansonsten gelten die allgemeinen Passwort-Regeln (siehe ORP.4 *Identitäts- und Berechtigungsmanagement*).
- Die Anzahl fehlgeschlagener Anmeldeversuche sollte begrenzt werden (z. B. temporäre Sperrung des Benutzerzugangs).

Bei der Auswahl der Maßnahmen ist sicherzustellen, dass die Anlage stets bedienbar bleibt und gefährliche Zustände ausgeschlossen bleiben.

Eine mögliche Alternative zu Passwörtern stellen Smartcards dar.

Vermeidung von Missbrauch

Ein unbefugter Zugriff auf Systeme sollte verhindert werden. Es sollte erkennbar und dokumentierbar sein, welcher Benutzer aktiv war (siehe auch IND.1.M10 *Monitoring, Protokollierung und Detektion*).

Es gibt bestimmte Betriebssituationen, die einen unmittelbaren Bedienzugriff in die OT benötigen. Dabei ist eine Abmeldung oder Bildschirmsperre nicht akzeptabel. In diesen Fällen sollten die Systeme durch kompensierende Schutzmaßnahmen vor dem unbefugten Zugriff geschützt werden (z. B. besetzter Leitstand).

In weniger kritischen Bereichen sollte die Bedienung gesperrt werden und lediglich eine Anzeige der aktuellen Informationen erfolgen. Auf diese Weise ist eine Beobachtung weiterhin möglich, der ungehinderte Zugriff jedoch verhindert.

Zur Authentisierung können Lösungen unter Nutzung von Chip- oder RFID-Karten mit Benutzer-PIN genutzt werden, um die Eingabe von komplexen Passworten zu vermeiden.

IND.1.M8 Sichere Administration (S)

Die Verwaltung von aktiven Systemkomponenten wie Serversystemen, Netz- oder OT-Komponenten erfolgt entweder an der lokalen Konsole, über eine serielle Schnittstelle oder bei vernetzten Komponenten nach der Ersteinrichtung typischerweise per netzbasiertem Fernzugriff.

Sichere Inbetriebnahme

Für die Erstkonfiguration einer Komponente sollte eine Anleitung bzw. Prüfliste erstellt werden, die gewährleistet, dass sicherheitsrelevante Einstellungen personenunabhängig durchgesetzt werden. Die jeweilig vorzunehmenden Einstellungen sind komponentenabhängig. Sie können beispielsweise folgende Maßnahmen umfassen (Aufzählung nicht vollständig):

- Deaktivieren von
    - nicht erforderlichen oder unsicheren administrativen Schnittstellen (SNMP, HTTP, Service-Ports, usw.) sowie
    - entbehrlichen Standardbenutzerkonten.
- Deinstallation nicht erforderlicher Funktionen.
- Aktivieren von Sicherheitsfunktionen, z. B.
    - Konfiguration sicherer Fernadministrationsschnittstellen (SSH, HTTPS),
    - Logon-Banner,
    - Session-Timeouts oder Sitzungszeitbeschränkungen,
    - Mindestanforderungen an die Passwortsicherheit,
    - Beschränkung administrativer Zugriffe auf Administrationsnetze (Access Control Lists),
    - verschlüsselte Speicherung von Passwörtern,
    - Zeitsynchronisierung,
    - Aktivieren der Systemprotokollierung sowie Konfiguration von Protokollierungsservern,
    - Prüfen auf und Ändern von potentiell vorhandenen Standardpasswörtern,
    - Einbindung in zentrale Verwaltungs- oder Authentisierungssysteme,
    - sicheres Hinterlegen von Administrationspasswörtern sowie
    - eventuell lokale Firewall oder Integritätsprüfungen.

Die Erstkonfiguration kann auch auf Basis einer initial erstellen Referenzkonfiguration durchgeführt werden. Die Erstkonfiguration sollte möglichst in einer sicheren Umgebung erfolgen und auch stets das

Einspielen der verfügbaren Sicherheitsaktualisierungen (Patches) umfassen, bevor eine Komponente in Betrieb genommen wird. Vor der Integration in das OT-Netz wird empfohlen, die Echtheit der Komponente zu prüfen und auf kompromittierendes Verhalten zu testen.

Sichere Konfigurationen an der lokalen Konsole

Die Konfiguration von OT-Komponenten an der lokalen Konsole beschränkt sich bei vielen Komponenten auf die Erstkonfiguration bei der Inbetriebnahme, sodass die Verwaltung im Betrieb über netzbasierte Fernzugriffe erfolgen kann. Die Konfiguration nicht vernetzter Komponenten erfolgt auch weiterhin über die lokale Konsole. Die lokale Konsole wird zudem oftmals als alternative Konfigurationsmöglichkeit im Störungsfall der Netzinfrastruktur beibehalten und nicht deaktiviert.

Der physische Zugang zu aktivierten Systemkonsolen muss daher auf geeignete Weise beschränkt werden, etwa durch gesicherte Räumlichkeiten oder abschließbare Serverschränke. Des Weiteren sollte der Zugriff auf die Konsole durch ein Passwort gesichert und auf autorisierte Zugänge beschränkt sein.

Sichere Fernwartung

Die Fernwartung sollte grundsätzlich durch sichere Protokolle wie zum Beispiel TLS-gesicherte Verbindungen, SSH oder SNMPv3 erfolgen. Klartextprotokolle sind zu vermeiden. Falls möglich, sollten ein dediziertes Administrationsnetz bzw. Zugriffsbeschränkungen (ACLs) eingerichtet werden, um vor unbefugtem Zugriff schützen.

Die Sicherheit der IT-Systeme für die Wartung ist für den sicheren Betrieb der Anlage unverzichtbar. Diese müssen daher angemessen vor Kompromittierung oder Missbrauch geschützt werden. Als Grundlage hierfür sollten die einschlägigen Bausteine des IT-Grundschutzes für die Wartungssysteme angewendet werden. Besonderes Augenmerk sollte in diesem Zusammenhang auf die Aspekte Zutritt, netzbasierter Zugang, Nutzung des Systems und Außenschnittstellen wie Internet, E-Mail oder die Nutzung von Wechseldatenträgern gelegt werden. Der Betrieb eines aktuellen Virenscanners kann in Abhängigkeit von der Bedrohungslage erforderlich bzw. vermeidbar sein.

Sichere Support-Zugriffe

Extern erreichbare Fernwartungszugänge müssen angemessen geplant und wirksam vor Missbrauch gesichert werden. Geeignete Maßnahmen hierzu sind:

- Zugangsbeschränkungen (Der Zugang zu Fernwartungszugängen sollte nach Möglichkeit auf bekannte, vordefinierte Netzbereiche beschränkt werden.)
- Sichere Authentisierung (Der externe Verbindungsaufbau sollte sicher authentisiert werden. Dies kann beispielsweise mittels eines zusätzlichen Tokens oder Client-Zertifikats erreicht werden. Bei Einwahlverbindungen kann ein Call-Back-Verfahren an eine hinterlegte Rufnummer eingerichtet werden.)
- Einsatz sicherer Protokolle (Der externe Zugriff auf OT-Umgebungen darf ausschließliche über verschlüsselte und integritätsgesicherte Protokolle erfolgen.)
- Nutzung von Sprungservern (Der externe Fernwartungszugriff auf OT-Komponenten sollte nicht direkt, sondern über gehärtete Sprungserver in einer DMZ-Infrastruktur erfolgen (vgl. IND.1.M16 *Stärkere Abschottung der Zonen*). Der Sprungsserver kann bestmöglich gegen Angriffe geschützt werden und auf dem aktuellen Patch-Stand sein, während die OT-Komponente wegen Verfügbarkeitsanfoderungen oder fehlender Updates noch auf einem veralteten Stand ist. Auf diese Weise kann die Komponente vor unberechtigten oder schädlichen Zugriffen geschützt werden. Außerdem können Datentransfers unterbunden, Prüfungen auf Schadprogramme erzwungen und Sitzungszeitbeschränkungen oder Verbindungsabbrüche bei Inaktivität durchgesetzt werden.)
- Bedarfsabhängige Aktivierung (Wenn Fernzugänge nur unregelmäßig benötigt werden, sollten die externen Zugänge standardmäßig deaktiviert sein und nur im Bedarfsfall aktiviert werden.)
- Protokollierung von Zugriffen (Fernzugriffe sollten durch eine geeignete Protokollierung nachvollziehbar bleiben. Bei sehr hohem Schutzbedarf sollte erwogen werden, die Administrationssitzung mittels geeigneter Verfahren aufzuzeichnen.)

Bei der Konzeption des Fernzugangs sollte darauf geachtet werden, die Nutzung unerwünschter Verbindungen zur Umgehung von Sicherheitsmaßnahmen zu unterbinden. Durch solche Tunnel könnten Komponenten und Dienste der OT-Komponenten unerwünscht zugänglich werden.

IND.1.M9 Restriktiver Einsatz von Wechseldatenträgern und mobilen Endgeräten in ICS-Umgebungen (S)

Wechselmedien einerseits (z. B. USB-Stick) und mobile Endgeräte anderseits (z. B. Service-Laptop) haben sich zu Haupteinfallstoren für Angriffe entwickelt, da diese Komponenten häufig die sorgsam konstruierten Zonengrenzen überqueren und so missbraucht werden können, um Schadsoftware oder Befehle hinein oder sensible Informationen hinaus zu transportieren.

Regelungen zum Thema Wechselmedien und mobile Endgeräte

Die Regelung sollte auf den Anwendungsbereich eingehen und mögliche definierte Ausnahmen und abweichende Regelungen dokumentieren. Es sollten Vorgänge dokumentiert werden, in denen Wechseldatenträger genutzt werden.

Eine Nutzung von privaten Wechseldatenträgern oder anderen mobilen Endgeräten zum Datentransport oder Anschluss an OT-Komponenten sollte generell ausgeschlossen werden.

Einschränkung der Nutzung

Auf den OT-Komponenten sollte die Nutzung auf bestimmte Geräte eingeschränkt werden (Device Control). Dies ist meist mit Funktionen des Betriebssystems oder über zusätzliche Software möglich.

Ist der Transport von Medien oder Geräten zwischen verschiedenen Zonen notwendig, so muss ein Prozess existieren, mit dem die Medien bzw. Geräte abgesichert und geprüft werden. Für Dienstleister sollte ein gleichwertiger Prozess gelten.

Bei der Neuplanung von Anlagen und Systemen sollte auf die Nutzung verzichtet werden oder ein restriktiver Umgang und eine sichere Nutzung von Wechselmedien forciert werden.

Wechseldatenträgerschleuse (Quarantäne-PC)

Ein Quarantäne-PC kann, stellvertretend für die einzelnen OT-Komponenten, OT-Speichermedien auf Schadprogramme prüfen. Hierzu müssen die Mitarbeiter angewiesen werden, Speichermedien aus einer nicht vertrauenswürdigen Quelle (z. B. USB-Sticks) mittels des Quarantäne-PCs auf Schadprogramme zu überprüfen, bevor solche Datenträger in das OT-Netz eingebracht oder an OT-Komponenten mit keinem oder eingeschränktem Virenschutzprogramm angeschlossen werden.

Der Quarantäne-PC sollte einen aktuellen Patchstand der Virenschutzprogramme aufweisen und mit aktuellen Schadsoftware-Signaturen bespielt sein. Daher müssen die Signaturen von Quarantäne-PCs immer auf dem aktuellsten Stand sein.

Zusätzlich zu einer möglicherweise automatisierten Überprüfung der Speichermedien durch den Quarantäne-PC sollte immer auch eine manuelle Prüfung für den Datenträger durchgeführt werden, z. B. durch eine gezielte Überprüfung von Logdaten oder durch Einsatz einer Datenschleuse (siehe auch SYS.4.5.A16 *Nutzung dedizierter Systeme zur Datenprüfung*).

Nutzung mobiler Endgeräte

Auf Service-Laptops, Programmiergeräte und ähnliche Endgeräte, die speziell im Bereich der OT eingesetzt werden, kann in der Regel nicht verzichtet werden. Solche mobilen Endgeräte, die nicht in der Hoheit des Betreibers stehen, werden häufig von externen Auftragnehmern genutzt. So kommen z. B. externe mobile Endgeräte zum Einsatz, wenn Hersteller Konfigurationsdateien auf die ICS-Komponenten des Betreibers aufspielen, wenn Integratoren Wartungsdienstleistungen im Auftrag eines Betreibers übernehmen oder wenn eine ICS-Anwendung nicht gekauft, sondern nur gemietet und extern betreut wird. Hier sind daher besondere Überlegungen notwendig, damit die Sicherheit der OT-Infrastruktur nicht durch Schwachstellen in diesen Clients oder in deren Nutzung gefährdet wird.

Smartphones, Tablets und andere Mobilgeräte, welche nicht ausschließlich im OT-Netz verwaltet werden, sollten in der Regel nicht mit dem OT-Netz verbunden werden. Ist dies doch erwünscht, so sind diese

angemessen abzusichern. Zur Absicherung dieser Geräte sollten zudem die einschlägigen IT-Grundschutz-Bausteine angewendet werden.

Einsatz von mobilen Endgeräten zu Wartungszwecken

In ICS kommen häufig mobile Endgeräte zum Einsatz, wenn Wartungsarbeiten durchzuführen sind, und es muss vorab sichergestellt werden, dass der Wartungsmitarbeiter aufgrund seiner Ausbildung und Kenntnisse zur Durchführung dieser Arbeiten in der Lage ist.

Bei Arbeiten an Anlagen mit hohem Schutzbedarf (SIL, GMP etc.) ist durch Zusatzmaßnahmen sicherzustellen, dass keine unbeabsichtigten Änderungen vorgenommen werden. Dann sind technische Sicherungsmaßnahmen (z. B. Schutz der Konfigurationsdaten des Feldgerätes mittels entsprechender Brücke) oder alternativ organisatorische Maßnahmen (Vier-Augen-Prinzip) anzuwenden.

Interne Geräte zu Wartungszwecken

Über organisatorische Maßnahmen ist sicherzustellen, dass auf internen Wartungsgeräten ausschließlich Software installiert ist, die für Wartungszwecke erforderlich ist. Es sollte eine Systemhärtung durchgeführt werden. Darüber hinaus sollten diese Geräte regelmäßig aktualisiert und auf Schadprogramme untersucht werden.

Externe mobile Geräte zu Wartungszwecken

Für den Einsatz externer Wartungsgeräte empfiehlt sich zunächst der Abschluss eines entsprechenden Vertrages mit dem externen Anbieter. In dem Vertrag können die informationssicherheitsrelevanten Themen (speziell Verhaltensregeln für die externen Mitarbeiter) vertraglich geregelt werden.

Vor dem Einsatz eines externen Wartungsgerätes ist eine Bestandsaufnahme erforderlich. Zu klären sind folgende Fragen:

- Welche Software ist installiert (inkl. Betriebssystem und Patches)?
- Welche Schnittstellen sind vorhanden und aktiv (z. B. UMTS/GPRS/GSM)?
- Welcher Schutz für Schadprogramme ist installiert? (Sind aktuelle Signaturen vorhanden?)

Ist diese Inventarisierung abgeschlossen und hat keine negativen Erkenntnisse geliefert, ist im nächsten Schritt eine Untersuchung auf Schadprogramme unter Nutzung eines den institutionsseitigen Festlegungen genügenden Virenschutzprogramms durchzuführen. Ist dieser Test erfolgreich abgeschlossen, so kann Zugang zur OT gewährt werden.

In diesem Zusammenhang hat sich bei verschiedenen Anwendern die Nutzung individueller Firewalls (USB-betriebene Kompaktgeräte) bewährt. Diese werden zwischen die jeweilige OT-Komponente und das Wartungsgerät geschaltet und sollen ungewollte Aktivitäten unterbinden.

IND.1.M10 Monitoring, Protokollierung und Detektion (S)

Durch das frühzeitige Erkennen von sicherheitsrelevanten Ereignissen kann zeitnah auf diese reagiert und somit ein möglicher Schaden begrenzt werden. Daher sollte im Vorfeld in einem Security-Incident-Response-Plan eine Strategie entwickelt werden, wie sicherheitsrelevante Ereignisse erfasst und erkannt werden, welche Reaktionen erforderlich sind und wie ein sicherer Zustand wiederhergestellt werden kann. Der Security-Incident-Response-Plan sollte die Phasen Planung, Reaktion und Wiederherstellung berücksichtigen und hierfür Prozesse z. B. zur Klassifizierung der Ereignisse, Benachrichtigung, Dokumentation, Untersuchung des Ereignisses und den daraus abgeleiteten Aktionen definieren.

Insbesondere sollten die Zuständigkeiten (Rollen) sowie das weitere Vorgehen (z. B. Meldung an Behörden oder Veröffentlichung) festgelegt werden. Hier ist auch der Datenschutzbeauftragte einzubinden.

Der Plan sollte in regelmäßigen Abständen und mindestens jährlich erprobt, auf Aktualität geprüft und bei Bedarf überarbeitet werden.

Protokollierung

Logging dient dem frühen Erkennen von Fehlern und sicherheitsrelevanten Vorfällen wie beispielsweise unbefugten Zugriffsversuchen auf Daten oder zur Identifikation von Übertragungsengpässen.

Die Protokollierungsdaten sollten auf einem zentralen Server gespeichert werden. So können die Protokollierungsdaten von verteilten Systemen und Komponenten zentral gesammelt, analysiert und in Zusammenhang gebracht werden.

In einem OT-Netz sollten mindestens die folgenden Ereignisse protokolliert und zentral gesammelt werden, soweit diese verfügbar sind:

- lokale Ereignisse, z. B. der Betriebssysteme, wie
    - Neustart von Diensten,
    - Systemstarts und Reboots,
    - erfolgreiche und erfolglose Anmeldungen am System (Betriebssystem und Anwendungssoftware),
    - fehlgeschlagene Berechtigungsprüfungen,
- Ereignisse von Domänen-Controllern (z. B. Einrichtung oder Änderungen von Benutzern, Gruppen und Berechtigungen),
- Firewall-, Router-, Switch- sowie Server-Ereignisse, vor allem blockierte Datenströme (Verstöße gegen ACLs oder Firewall-Regeln),
- Ereignisse der Virenschutzprogramme,
- sonstige sicherheitsrelevante Fehlermeldungen (z. B. Hardwaredefekte, Überschreitung von Kapazitätsgrenzen) sowie
- Ereignisse des Intrusion-Detection- oder Intrusion-Prevention-Systems (IDS/IPS).

Zusätzlich sollten zu den vorher genannten Ereignissen folgende Daten aufgezeichnet werden:

- Datum und Zeit (Wird für alle ICS eine gemeinsame Zeitquelle kontrolliert genutzt? Siehe IND.1.M6 *Änderungsmanagement im OT-Betrieb* sowie IND.1.NET.1.2.M8 *Zeitsynchronisation*)
- Beschreibung des Ereignisses
- Einstufung der Kritikalität (Wie kritisch ist das Ereignis im Hinblick auf eine unterbrechungsfreie Prozess-Fortführung?)
- Quelle des Ereignisses (z. B. Anwendung, Betriebssystem)

Außerdem ist auf die geltenden Datenschutzbestimmungen zu achten.

Monitoring und Auswertung

Zur Gewährleistung des sicheren Wirkbetriebs sollte eine geeignete Infrastruktur für die betriebliche Überwachung des ICS konzipiert, implementiert und betrieben werden. Die Überwachung sollte neben der betrieblichen Verfügbarkeits- und Auslastungsüberwachung von Diensten, Systemen und Netzen auch die Auswertung sicherheitsrelevanter Ereignisse umfassen.

Dies wird in der Regel nicht erfolgen, wenn die Logs auf eine Vielzahl von Systemen verteilt sind. Daher sollte ein zentraler Protokollserver eingerichtet werden. Dieser muss geeignet in das Zonenkonzept eingebettet werden (siehe IND.1.M5 *Entwicklung eines geeigneten Zonenkonzepts*). Gegebenenfalls sind mehrere Protokollserver notwendig, um die Trennung der Zonen aufrechterhalten zu können.

Die auflaufenden Protokolle müssen systematisch ausgewertet werden, damit nötigenfalls die geeignete Reaktion ausgelöst werden kann. Bei einer überschaubaren Anzahl von Systemen kann dies stichprobenartig erfolgen, hierfür ist mindestens eine (Rollen-)Verantwortung und eine Frequenz (je nach Schutzbedarf, z. B. wöchentlich) festzulegen. Bei einer größeren OT-Infrastruktur wird ausschließlich eine zumindest teilautomatisierte Auswertung erlaubt, um kritische Ereignisse zu erkennen.

Auf Grundlage von auftretenden Ereignissen und Grenzüberschreitungen bei überwachten Werten sollte ein Alarm ausgelöst werden, der den IT-Betrieb der Komponente über das Ereignis informiert.

Die folgende Liste veranschaulicht mögliche Beispiele für solche Ereignisse und Muster:

- Auffälliges Verhalten, welches typisch für Schadprogramme ist (z. B. erhöhter Netzverkehr, Abnahme der Performance, zunehmende Fehler in Anwendungen und Integritätsverletzungen),
- Hardware-Defekte wie fehlerhafte Sektoren bei Datenspeichern (z. B. Festplatte) oder ausfallende Komponenten aufgrund von Hardware-Fehlern,
- Verlust der Netzverbindung,
- ungewöhnlicher Anstieg der CPU-Last und des Speicherverbrauchs.

Implementierung von Intrusion-Detection- bzw. Intrusion-Prevention-Systemen

Mithilfe von Intrusion-Detection-Systemen (IDS) und Intrusion-Prevention-Systemen (IPS) lassen sich Angriffsversuche in einer frühen Phase erkennen, sodass der IT-Betrieb frühzeitig alarmiert wird (IDS) oder bereits eine automatisierte Reaktion auf den Angriff eingeleitet wird (IPS).

Hierzu arbeiten IDS/IPS auf der Grundlage von Heuristiken, um Angriffsversuche von gewöhnlichen, gewünschten Verhalten und Daten zu unterscheiden. Demgemäß müssen diese Heuristiken regelmäßig aktualisiert werden. Bei der Aktualisierung der Heuristiken sollten die Hinweise zur Aktualisierung von Virensignaturen berücksichtigt werden. Darüber hinaus müssen die Heuristiken auf die OT und ihre individuellen Gegebenheiten angepasst werden. Typische Vorfälle und Ereignisse, die durch ein solches System erkannt werden können, sind z. B. unbefugte Zugriffe auf Systeme und die unbefugte Installation von Software oder Manipulationen von Daten. Zudem können hierdurch auch unbeabsichtigte und versehentliche Änderungen (z. B. in Konfigurationsdateien) bemerkt werden.

Ein IDS/IPS kann einzelne Server überwachen (Hostbasierte IDS/IPS: HIDS/HIPS) oder durch Sensoren im Netz den Datenverkehr prüfen (netzbasiertes IDS/IPS: NIDS/NIPS).

Wird ein NIDS/NIPS verwendet, so sollten die Sensoren im Netz zur Überwachung des Datenverkehrs insbesondere bei externen Schnittstellen platziert werden (z. B. DMZ). Von externen Schnittstellen geht gewöhnlich eine höhere Bedrohung durch Angriffe aus (z. B. Internet). Ebenso sollte ein HIDS auf allen OT-Komponenten installiert werden. Die Protokolldaten des HIDS sollten in ein zentrales Logging integriert werden.

IDS/IPS sollten als zusätzliche Schutzmaßnahme angesehen werden und ersetzen kein Monitoring der Systeme und des Netzes (z. B. durch ein Security Information Event Management (SIEM)).

Der Einsatz und der Betrieb eines IDS können nur größeren Institutionen empfohlen werden, da die Einrichtung, die Pflege und die Sichtung der Meldungen (insbesondere in der Anfangsphase) mit einem nicht unerheblichen Aufwand verbunden sind. In kleineren Anlagen ist der Aufwand und der Nutzen vorab zu prüfen und es sind eventuell alternative Härtungs- und Schutzmaßnahmen umzusetzen.

Bei der Umsetzung eines IPS ist zudem zu beachten, dass bei der Planung auch sehr spezielle Situationen berücksichtigt werden, damit diese legitimen Übertragungen nicht verhindert werden. Vor einer Aktivierung dieser Funktionen ist daher eine sehr sorgfältige Probephase zu absolvieren.

Die Effektivität eines IDS/IPS ist stark abhängig von einer angepassten und individuellen Konfiguration. So kann die Effektivität beispielsweise durch eine hohe Anzahl an immer wiederkehrenden False Positives beeinträchtigt werden. Insbesondere IPS sollten mit Bedacht eingesetzt werden. Vorrangig ist hier der laufende Betrieb, der durch ein fehlerhaftes Eingreifen des IPS gestört werden könnte.

Daher erfordert nicht nur die initiale Konfiguration des IDS/IPS ein geschultes Fachpersonal, sondern auch im Betrieb muss mindestens eine Person im Notfall einen gemeldeten Angriffsversuch von einem False Positive unterscheiden können. Diese Person sollte ständig erreichbar sein, sodass nach der Klassifizierung der Meldung entsprechende Gegenmaßnahmen eingeleitet werden können.

IND.1.M11 Sichere Beschaffung und Systementwicklung (S)

Entwicklung und Integration

OT-Komponenten werden als Verbund von Hard- und Software ausgeliefert. Die Anpassung auf die individuellen Gegebenheiten und Bedürfnisse wird durch die Konfiguration realisiert. In vereinzelten Fällen kann es notwendig sein, eigene Software zu entwickeln (z. B. Skripte, Batch-Dateien zur Stapelverarbeitung),

um gewisse Automatismen oder Funktionen nachträglich zu integrieren. Werden eigene Programme oder auch Skripte entwickelt, so sollte sowohl die sichere Erstellung der Programme (Secure-Coding-Guidelines) als auch die sichere Integration in die bestehende Umgebung durch eine interne Softwareentwicklungsrichtlinie geregelt werden.

Vertraulichkeitsvereinbarung mit den Herstellern, Lieferanten und externen Betreibern

Die Institution sollte mit Vertragspartnern (Herstellern, Lieferanten oder externe Betreibern) Vertraulichkeitsvereinbarungen treffen. Diese sollten insbesondere Mitarbeiter des Vertragspartners mit relevanten Informationen und Kenntnissen der Informationssicherheit über die OT der Institution berücksichtigen (z. B. für den Fall, dass Mitarbeiter des Vertragspartners die Position oder Firma wechseln).

Darüber hinaus sollte geregelt werden, wie die Verfügbarkeit der OT erhalten werden kann, falls der Vertragspartner keine Wartungsdienste oder Dienstleistungen mehr anbietet (z. B. wegen Insolvenz des Vertragspartners). So sollte der Institution beispielsweise der notwendige Zugriff auf diese Systeme auch weiterhin möglich und ausreichend Dokumentation zur Wartung und zum Betrieb der OT verfügbar sein.

Im Fall der Geschäftsaufgabe eines Vertragspartners sollte vertraglich geregelt sein, dass ausgehändigte, vertrauliche Informationen an die Institution zurückzugeben sind.

Langfristige Gewährleistung der Informationssicherheit

Die Institution, Integratoren und Hersteller sollten bereits bei der Planung des OT-Systems oder seiner Teile eine Strategie erarbeiten, wie langfristig die Informationssicherheit der Anlage gewährleistet werden kann. Dies gilt für die gesamte Laufzeit der Anlage und umfasst auch die weitere Nutzung von abgekündigter Software. Es sollten daher bereits frühzeitig alternative Schutzmaßnahmen berücksichtigt werden.

Kompatibilität

Die zu beschaffende OT und deren Komponenten sollten gängigen Technik-Standards entsprechen und infolgedessen kompatibel zu anderen Systemen sein. Dazu sollten diese nach Möglichkeit etablierte, marktübliche Informationssicherheitsmechanismen unterstützen.

Verzicht auf überflüssige Produktfunktionen

Falls OT-Komponenten Dienste oder Schnittstellen besitzen, die nicht für den Betrieb benötigt werden, sollten diese nach Möglichkeit entfernt oder zumindest deaktiviert werden. Die durchgeführten Änderungen an der OT sollten nachvollziehbar dokumentiert werden.

Mitteilung der Informationssicherheitsanforderungen an den Integrator und den Hersteller

Die Informationssicherheitsanforderungen der Institution an die OT, die sich aus der Risikoanalyse ergeben, sollten dem Hersteller und dem Integrator, der die Anlage realisiert, mitgeteilt werden. Dieses sollte als Bestandteil des Lastenhefts erfolgen.

Die Anforderungen sollten auf Basis der konkreten Anwendungen formuliert werden. So können sie sich auf geforderte Eigenschaften oder Informationen beziehen. Es sollten keine Lösungen, sondern Anforderungen beschrieben werden. Der Erfüllungsgrad der Anforderungen sollte bei der Wahl der Lösung und des Integrators berücksichtigt werden.

Berücksichtigung der Informationssicherheitsspezifikationen des Herstellers und Integrators

Die Institution muss die Informationssicherheitsspezifikation, die der Hersteller und der Integrator bereitstellt, im Zyklus der Risikoanalyse berücksichtigen. Aufbauend auf den Informationen des Herstellers und des Integrators können weitere Maßnahmen durch die Institution definiert werden.

Robustheit der Produkte

Neben der Hardware (z. B. IT-System) sollte auch die Software (z. B. OT-Anwendungen, Protokollstack) robust auf ungültige Eingaben reagieren. So sollten beispielsweise ungültige Netzpakete nicht zum Absturz oder zu Fehlern der Software führen, sondern von dem Protokollstack ignoriert und bei Bedarf protokolliert werden.

Die Robustheit der Komponenten sollte bereits durch die Hersteller sichergestellt werden. Diese Anforderung sollte bereits bei der Anschaffung neuer Komponenten durch die Institution gefordert werden.

Unterstützung von Virenschutz-Lösungen

Falls notwendig sollten die zu beschaffenden OT-Komponenten mit einem Schadsoftwareschutzprogramm ausgestattet sein oder zumindest den Betrieb von solchen Schutzprogrammen unterstützen. In der Regel unterstützt der Hersteller ausgewählte Produkte (siehe auch IND.1.M3 *Schutz vor Schadprogrammen*).

Abnahmetests und Integrationstests

Im Rahmen der Abnahme- und Integrationstests sollte die Umsetzung der Sicherheitsanforderungen sowie die Interoperabilität geprüft und verifiziert werden.

Im besonderen Fokus sollte die Handhabung und Wirksamkeit von Backup- und Recovery-Maßnahmen stehen.

IND.1.M12 Etablieren eines Schwachstellen-Managements (S)

Fehler in der Software stellen ein Problem dar, sobald sie es einem Angreifer ermöglichen, Zugriff auf das System erlangen oder den Ablauf der Software zu stören. Daher gilt grundsätzlich, dass diese Fehler behoben werden sollten oder aber ihre negativen Auswirkungen anderweitig begrenzt werden müssen.

Schwachstellen

Wie bei allen IT-Systemen enthalten OT-Komponenten, -Systeme, -Anwendungen und -Protokolle Schwachstellen. Da diese die Sicherheit grundsätzlich bedrohen, ist ein Prozess zum Umgang mit ihnen notwendig.

Dabei ist für eine Komponente (Produkt, System, Anwendung) zwischen den folgenden Fällen zu unterscheiden:

Fall 1: **Es sind keine Schwachstellen öffentlich bekannt**. Dies kann sich jederzeit ändern. Außerdem können Schwachstellen nur bestimmten Parteien bekannt sein, die diese aus unterschiedlichen Gründen nicht veröffentlichen möchten. Die Ausnutzung einer Schwachstelle, bevor die Schwachstelle öffentlich bekannt gegeben wurde, ist ein sogenannter Zero Day Exploit, bzw. ein Zero Day Exploit Attack (ZETA).

Fall 2: **Es sind Schwachstellen bekannt**.

- **Fall 2.1**: Der Hersteller hat **Patches bereitgestellt**. Diese werden vom Integrator oder Maschinen- bzw. Anlagenbauer wie folgt behandelt:
    - Die Patches werden freigegeben.
    - Die Patches werden nicht freigegeben.
- **Fall 2.2**: Der Hersteller hat **noch keine Patches** bereitgestellt.
    - Der Hersteller plant, Patches bereitzustellen.
    - Der Hersteller plant nicht, Patches bereitzustellen. (In diesem Fall muss das Risiko des Weiterbetriebs betrachtet und es müssen entsprechende technische oder organisatorische Maßnahmen getroffen werden. Ansonsten müssen solche Komponenten (Hardware wie Software) ausgetauscht werden.)

Ziel des Schwachstellen-Managements

In sämtlichen Fällen sollte das Schwachstellen-Management Vorgehensweisen liefern können. Dieses sollte grundsätzlich in die sonstigen Vorgehensweisen zum sicheren Betrieb der Betriebs- und Steuerungstechnik integriert werden (siehe IND.1.M6 *Änderungsmanagement im OT-Betrieb*).

Das Schwachstellen-Management muss Lücken in Software, Komponenten, Protokollen und Außenschnittstellen der Umgebung identifizieren und mögliche Handlungsbedarfe und -möglichkeiten (z. B. ein Patchmanagement) ableiten, bewerten und umsetzen.

Bestandsanalyse

Bei der Ersteinführung des Schwachstellen-Managements muss einmal eine Schwachstellenanalyse der Ausgangslage zum Ableiten von Handlungsbedarfen durchgeführt werden. Auf Grundlage der

Bestandsinfrastruktur muss die Institution dafür alle bestehenden Schwachstellen aller verbauten Komponenten (Produkte, Anwendungen, Systeme, Protokolle, Außenschnittstellen) identifizieren. Grundlage hierfür sollten Schwachstellenmeldungen (Advisories) von Herstellern und öffentlich verfügbare CERT-Meldungen sein. Ergänzend hierzu können organisatorische und technische Audits zur Schwachstellenanalyse durchgeführt werden. Dies ist insbesondere bei höherem Schutzbedarf und bei besonderer Exponiertheit (z. B. Schnittstellen zum Internet) zu empfehlen.

Ein Einspielen sicherheitsrelevanter Updates im Rahmen eines systematischen Patchmanagements kann eine Möglichkeit sein, bestimmte Schwachstellen zu schließen. Hierfür muss ein geeignetes Verfahren für die jeweilige Umgebung bestimmt werden, ob, wie und wann Patches ausgebracht werden können.

Bewertung von Schwachstellen

Um relevante Schwachstellen zeitnah, systematisch, fachlich angemessen und wirtschaftlich bewerten und die richtigen Schlussfolgerungen ziehen zu können, ist die Festlegung eines Verfahrens zur Bewertung von Schwachstellen notwendig. Hierbei sollte definiert werden, wer (d. h. welche Rolle(n)) wann (in welcher Frequenz) welche Informationsquellen (Nachrichten, Advisories, E-Mail-Verteiler, Datenbanken etc.) abonniert, sichtet und auswertet. In kleineren Organisationen bietet es sich an, diese Aufgaben beim ICS-Informationssicherheitsbeauftragten zu bündeln. In größeren Strukturen mit vielen System- und Anwendungstypen wird eine Aufgabenteilung notwendig sein. Aus den möglichen Auswirkungen einer Schwachstelle (gefolgert aus dem Schutzbedarf) und der Exponiertheit (Einfachheit der Ausnutzbarkeit) sollte eine Kritikalität abgeleitet werden, welche die Priorität für das weitere Vorgehen vorgibt. Es kann ein standardisierter Bewertungsmaßstab wie CVSS verwendet werden. Für kleinere Organisationen reicht in der Regel eine zwei- oder dreistufige qualitative Skala:

- unkritisch (geringe Auswirkungen oder vernachlässigbare Exponiertheit): Weiter zu beobachten
- mittel (maximal mittlere Auswirkungen oder Exponiertheit): Behandlung im Rahmen der nächsten regulären Softwarepflege
- kritisch (kritische Auswirkung oder hohe Exponiertheit): Prioritäre außerplanmäßige Behandlung (Informationssicherheitsbeauftragter entscheidet über das weitere Vorgehen)

An den Bewertungsprozess angeschlossen sein sollte ein Vorgehen zur Software-Pflege: Je nach Bereich (z. B. nach Zone) können unterschiedliche Vorgaben definiert sein, wann, wie oft und wie Schwachstellen ab einem bestimmten Schweregrad gepatcht werden bzw. welche alternativen Maßnahmen in Kraft sein müssen, damit auf das Patchen verzichtet werden kann. Bei jeder neuen Art von Schwachstelle und jeder Fortentwicklung von Angriffstechniken ist zu prüfen, ob die etablierten Ersatzmaßnahmen weiterhin ausreichen oder ob diese ergänzt werden müssen.

Patchen

Wo Patchen möglich ist, dessen Risiken abgeschätzt sind und tragbar erscheinen, sollte ein Patchprozess mit rollenspezifischen Zuständigkeiten definiert werden, welcher neben den vom Hersteller freigegebenen Patches und Updates ebenso zusätzliche Drittanbieter-Software berücksichtigt (z. B. Büroanwendungen, PDF-Reader). Der Prozess sollte mindestens folgende Elemente beinhalten:

- Regelmäßige Prüfung auf neue Schwachstellenmeldungen bei den Herstellern der OT-Komponenten oder Drittanbieter-Software
- Bewertung des Schweregrads von Patches, beispielsweise mit Common Vulnerability Scoring System (CVSS),
- Beziehen der Patches und Updates,
- Testen (dies sollte auf einer Testumgebung (baugleiche Komponente) erfolgen),
- Freigabeprozess,
- Umgang mit Hersteller-Freigaben von Patches und
- Umgang mit dem Patchen von zusätzlicher Software.

Bezugsquellen für die Meldung von Schwachstellen sind die Hersteller oder auch CERTs.

Das CVSS ist eine Methodik zur Bewertung und Klassifizierung von Schwachstellen in Abhängigkeit des individuellen Risikos des einzelnen Betriebs. In die Basis-Bewertung (Base Score) fließt unter anderem ein, wie die Schwachstelle ausgenutzt werden kann (z. B. lokal oder entfernt) und welche Konsequenzen drohen (z. B. Denial of Service oder Code-Ausführung). Ein zweiter Wert (Temporal Score) bewertet über die Zeit veränderbare Rahmenbedingungen. Dazu zählt z. B. die Verfügbarkeit von Exploit-Code. Eine dritte Komponente stellt den Bezug zur lokalen Umgebung des Anwenders her. Dieser muss anhand seiner Umgebung einschätzen, was diese Schwachstelle für ihn bedeutet. Die ersten beiden Informationen werden auf verschiedenen Webseiten zu Schwachstellen zur Verfügung gestellt (z. B. CVE MITRE).

Das Einspielen von Patches und Updates erfordert gewöhnlich die Freigabe durch den Hersteller der OT-Komponente. Daher können in der Regel z. B. bereits im Internet verfügbare Patches und Updates durch die Institution nicht eingespielt werden, da ein Funktionsverlust möglich wäre und durch den Hersteller keine Garantie übernommen würde.

Aus diesem Grund sollte die Institution mit dem Hersteller vertraglich Zeiträume zur Freigabe und Bereitstellung von Patches und Updates oder alternativen Workarounds für Schwachstellen festlegen, insbesondere dann, wenn solche Eingriffe Auswirkungen auf die Zulassung eines Systems haben können. Die Zeiträume sollten möglichst kurz gewählt werden, da in diesem Zeitfenster das betroffene System durch die Schwachstelle einem erhöhten Risiko ausgesetzt ist.

Sofern die Möglichkeit besteht, kann die Institution vor der Installation eigenständig Tests durchführen. Alternativ sollten die Updates sequenziell installiert und getestet werden. Hierbei sollten zuerst redundante Systeme bespielt werden. Vor dem Einspielen von Patches und Updates wird empfohlen, für jedes System eine Datensicherung durchzuführen. Dies betrifft insbesondere OT-Systeme, die notwendig für die Produktion sind. OT mit keiner oder geringer Bedeutung für die Produktion können auch ohne vorherige Datensicherung und umfangreiche Tests gepatcht werden.

Zudem sollte geprüft werden, ob ein Neustart nach dem Patch durchgeführt wird oder erforderlich ist. Dies muss bei der Planung berücksichtigt werden.

Insgesamt sollte das Einspielen von Patches in die Betriebszyklen der Anlage integriert werden. So können Wartungsfenster an der Anlage genutzt werden, um Patches zu installieren. Bei redundant ausgelegten Komponenten kann ein schrittweises Vorgehen gewählt werden, um den Zeitpunkt der Installation nicht zu lange aufzuschieben.

Alternativen zum Patchen

Steht kein Patch zur Verfügung, sollten in einer Sicherheitsbetrachtung alternative Maßnahmen betrachtet und ergriffen werden, um die Ausnutzung der Schwachstelle zu verhindern. Lösungen können zum Beispiel zusätzliche Tools sein, die eine Ausnutzung von Schwachstellen verhindern oder Änderungen verhindern. Als alternative Maßnahme ist es beispielsweise möglich, die betroffene OT in ein separates Netzsegment zu platzieren und den Datenverkehr zu diesem Netzsegment mittels einer Firewall zu filtern (siehe IND.1.M5 *Entwicklung eines geeigneten Zonenkonzepts*).

Umgang mit End-Of-Support / End-Of-Life (EOS/EOL)

Falls für OT-Komponenten oder darin verwendeter Software der End-of-Support erreicht wird, führen diese Komponenten zu einem erhöhten Betriebsrisiko. Dies gilt im Speziellen für Software aus dem IT-Umfeld (z. B. Betriebssysteme). In diesen Fällen ist es möglich, dass weiterhin Schwachstellen entdeckt werden, diese jedoch nicht mehr geschlossen werden. Dann sind möglicherweise zusätzliche Schutzmaßnahmen notwendig, z. B. die Migration auf eine neue Software- oder Firmware-Version oder auf eine Hardware-Revision.

Hierfür sollte eine Sicherheitsbetrachtung durchgeführt werden und darauf aufbauend sollten in Abhängigkeit der Funktion der OT und Bedeutung für die Produktion angemessene Informationssicherheitsmaßnahmen identifiziert werden. So kann beispielsweise eine Separierung der OT mit ungepatchten Schwachstellen in ein eigenes Netzsegment und einer restriktiven Firewall zur Filterung des Datenverkehrs die Systeme schützen.

Langfristiges Ziel sollte der Austausch der betroffenen OT-Komponenten durch solche Komponenten sein, die vom Hersteller unterstützt werden. Ohne Support durch den Hersteller können zukünftig auftretende

Fehler und Ausfälle die Produktion stark beeinträchtigen, da die Erarbeitung von Lösungen ohne Hilfe durch den Hersteller aufwendiger ist.

Es sollte insbesondere bei der Anschaffung darauf geachtet werden, dass keine Komponenten zum Einsatz kommen, die bereits durch den Hersteller abgekündigt wurden.

IND.1.M13 Notfallplanung für OT (H)

Notfallmanagement

Viele Organisationen verfügen aufgrund unterschiedlicher Anforderungen bereits über ein Notfallmanagement, das bestimmte Szenarien abdeckt. Im Bereich der OT sollten diese um Notfallpläne mindestens für folgende Szenarien ergänzt werden:

- Komplettausfall der Internetanbindung inklusive Fernwartung für längere Zeit (> 1 Woche)
- Komplettausfall der Büro- und Gebäude-IT für eine bestimmte Zeit (z. B. 2 Tage)
- temporärer Ausfall kritischer IT-Komponenten im OT-Bereich für einen Zeitraum, der mit Standardbetriebsprozessen nicht auffangbar ist
- Kompromittierung kritischer IT-Komponenten im OT-Bereich durch einen unbekannten Angreifer bzw. durch Schadprogramme

Falls bereits ein Business Continuity Management (BCM) besteht, kann das Notfallmanagement für die OT-Infrastruktur in dieses integriert werden. Andernfalls sollte ein BCM eingerichtet werden, etwa nach IT-Grundschutz (Baustein DER.4 *Notfallmanagement* bzw. BSI-Standard 100-4), das die OT-Infrastruktur umfasst.

Systemsicherung und -wiederherstellung

Für die OT sollte ein Sicherungs- und Wiederherstellungskonzept erstellt werden. Grundlage hierfür können die bewährten Verfahren der Büro- und Gebäude-IT (siehe Baustein CON.3 *Datensicherungskonzept*) sein. Darüber hinaus können ergänzende system- bzw. komponentenspezifische Sicherungsverfahren für Systeme erforderlich werden, die nicht in klassische Sicherungslösungen eingebunden werden können.

Die Sicherungsinfrastruktur der OT sollte möglichst unabhängig von der Infrastruktur der Büro- und Gebäude-IT-Lösung betrieben werden. Bei der Nutzung einer gemeinsamen Infrastruktur sollten die durch die Abhängigkeiten entstehenden Risiken betrachtet und angemessen berücksichtigt werden. Dies gilt insbesondere auch für die Ablage von Systemsicherungen oder Projektdaten auf Dateiservern der Büro- und Gebäude-IT.

Wiederherstellungsplan

In einem Wiederherstellungsplan sollte festgelegt werden, wie grundlegende Funktionen in der OT nach einer signifikanten Störung wieder aufgenommen werden können. Es sollten im Vorfeld Aktionen abgeleitet werden, die nach Eintritt einer Produktionsstörung oder eines Sicherheitsvorfalls den Wiederanlauf der Produktion in einer angemessenen Zeit sicherstellen. Dazu zählen beispielsweise Prozesse zur Datensicherung, Wiederherstellung und zum regelmäßigen Testen von Backups, Prozeduren zur Systemwiederherstellung, Reparatur defekter Komponenten und Vorhalten von Ersatzteilen sowie auch alternative Kommunikations- und Steuerungsmöglichkeiten bei Ausfällen.

Der Plan sollte in regelmäßigen Abständen und mindestens jährlich auf Aktualität geprüft und bei Bedarf überarbeitet werden.

Notfallplan und -vorgehensweisen müssen mit geltenden Gesetzen und anderen regulatorischen Anforderungen kompatibel sein. Die Notfallplanung für die OT-Infrastruktur lässt sich entweder in ein bestehendes Notfallmanagement integrieren oder aber als eigenständiges Notfallmanagement für die OT etablieren. In letzterem Fall kann das OT-Notfallmanagement auch Teil eines bereits bestehenden OT-Krisenmanagements sein.

Die Organisation muss Notfallpläne für zu definierende Kategorien von Ausfällen und anderen Krisen entwickeln. Für den Fall des Ausfalls der gesamten oder Teile der OT oder wichtiger

Kommunikationsverbindungen müssen vordefinierte Maßnahmen ausgeführt werden (z. B. den gesteuerten Prozess sicher herunterfahren oder letzten Betriebszustand vor dem Ereignis aufrechterhalten).

Wiederherstellung der OT-Infrastruktur in einen sicheren Zustand bedeutet, dass

- alle Systemparameter (Standardparameter und organisationsspezifische Parameter) auf sichere Werte gesetzt sind,
- sicherheitskritische Updates (wieder) installiert sind,
- sicherheitsrelevante Einstelllungen wiederhergestellt sind,
- Systemdokumentationen und Bedienungsanleitungen verfügbar sind,
- aktuelle, verifizierte Backups wiederhergestellt sind und
- das Gesamtsystem voll getestet und funktional ist.

Evaluierung des Notfallmanagements

Das OT-Notfallmanagement muss regelmäßig (z. B. einmal jährlich) evaluiert werden. Dafür sollte die Organisation ein Testverfahren auswählen (z. B. vollumfängliche Simulation oder Table-Top-Exercise), dessen Testtiefe und -abdeckung der Wichtigkeit der OT-Infrastruktur angemessen ist.

Redundanz

Bezüglich Redundanzen als wichtige Maßnahme der Business Continuity gilt im OT-Bereich grundsätzlich dasselbe wie für Büro- und Gebäude-IT. Die Ausgestaltung und Dimensionierung der Redundanzen hat dabei immer den Schutzbedarf zu beachten und muss alle betriebskritischen Elemente der OT-Umgebung abdecken, also auch Stromeinspeisung, Versorgungsleitungen, Datenkabel, aktive Netzkomponenten etc.

Wenn sehr hoher Verfügbarkeitsbedarf besteht, so sollte ein alternatives Kontrollzentrum (z. B. Warte oder Leitstand) aufgebaut werden, das bei Ausfall des Hauptkontrollzentrums in einem gewissen Zeitrahmen, welcher von der Organisation mithilfe des Schutzbedarfs zu definieren ist, einsatzbereit ist (sogenannter Notfallstandort). Dieser Notfallstandort sollte

- geographisch getrennt sein, sodass ein Einwirken einer Naturkatastrophe auf beide Standorte unwahrscheinlich ist,
- im Notfall erreichbar sein (auch bei regionalen Ausfällen von Strom und anderen Diensten),
- über notwendige Dienstleisterverträge mit der angemessenen Priorität abgedeckt sein und
- ständig so weit konfiguriert sein, dass er im gesetzten Zeitrahmen einsatzfähig ist.

IND.1.M14 Starke Authentisierung an OT-Komponenten (H)

Soweit möglich sollte die Nutzung aller OT-Komponenten eine Authentisierung der Benutzer und Dienste erfordern, sodass eine Bedienung der Systeme nur im authentisierten Zustand möglich ist. Dazu zählen neben gewöhnlichen IT-Systemen auch Router, Switches und SPS.

Zur Authentisierung können unterschiedliche Verfahren und Merkmale eingesetzt werden. Es wird zwischen den Authentisierungsmerkmalen Wissen (z. B. Passwort, PIN), Besitz (z. B. Token, Smartcard, Zertifikat) und körperliche Merkmale (z. B. Fingerabdruck, Iriserkennung) unterschieden. Auch der Aufenthaltsort des Zugreifenden kann indirekt als Merkmal betrachtet werden, wenn sichergestellt ist, dass dieser nur mittels eines oder mehrerer weiterer Merkmale an diesen Ort gelangen konnte. Ein Beispiel ist eine Warte, die nur mit einem Schlüssel oder nach einer (beiläufigen) Gesichtskontrolle durch Kollegen betreten werden kann.

Mehrfaktorauthentisierung

Bei erhöhtem Schutzbedarf sollten mehrere Merkmale zur Authentisierung herangezogen werden und so ein höheres Informationssicherheitsniveau etablieren (z. B. Zwei-Faktor-Authentisierung mittels Token und Passwort). Hierbei sollten Merkmale aus unterschiedlichen Klassen (Wissen, Besitz, Biometrie, Ort) kombiniert werden.

Bei der Auswahl der Authentisierungsmethoden ist eine Sicherheitsbetrachtung durchzuführen. Diese muss mit weiteren Anforderungen (z. B. Störfallverordnung) und organisatorischen Rahmenbedingungen (z. B. Zugangsrestriktionen) abgeglichen werden, um zu einer geeigneten Auswahl zu kommen.

Zentrale Verwaltung von Authentisierung

Die Verwaltung der genannten Anforderungen sollte vorzugsweise über eine zentrale Management-Lösung realisiert werden (z. B. in einem Verzeichnisdienst). Dabei sollte keine zusätzliche Abhängigkeit von anderen Zonen eingeführt werden. Dies kann dadurch erreicht werden, dass der Verzeichnisdienst innerhalb der Zone betrieben wird, für die er benötigt wird. Informationen aus einem Verzeichnisdienst in einer anderen Zone können bei Bedarf repliziert werden.

Nicht alle hier genannten Maßnahmen sind voll umfassend auf alle OT-Komponenten sinnvoll anwendbar. So kann beispielsweise ein Angreifer durch provozierte, fehlgeschlagene Anmeldeversuche den Benutzerzugang sperren. Somit wäre ein Zugriff auf das betroffene System durch den legitimen Benutzer nicht mehr möglich. Daher muss der Sicherheitszugewinn durch die jeweilige Maßnahme und mögliche Einschränkungen sonstiger Anforderungen an die OT-Komponenten (z. B. erforderlicher, unmittelbarer Zugriff) gegeneinander abgewogen werden. Es sollte immer ein Notfallprozess existieren, durch den im Fall der Störung der Authentisierung der Betrieb aufrechterhalten werden kann. In diesem Zusammenhang sollten die für den automatisierten Betrieb erforderlichen technischen Benutzer- und Dienstezugänge möglichst nicht von einem Verzeichnisdienst abhängig sein.

IND.1.M15 Überwachung von weitreichenden Berechtigungen (H)

Notwendige Grundlage für diese Maßnahme ist, dass IND.1.M7 *Etablieren einer übergreifenden Berechtigungsverwaltung zwischen der OT und in der Office-IT* ordnungsgemäß umgesetzt wurde. Im Fall des erhöhten Schutzbedarfs werden die Anforderungen an die Berechtigungsverwaltung folgendermaßen erhöht. Ziel ist, dass ein Missbrauch einfacher und schneller verhindert oder zumindest erkannt werden kann.

Revisionssichere Pflege einer Bestandsübersicht und Historie

Nach IND.1.M7 *Etablieren einer übergreifenden Berechtigungsverwaltung zwischen der OT und in der Office-IT* gilt: Das Berechtigungsmanagement muss eine vollständige Übersicht über die an eine Person vergebenen Berechtigungen besitzen. Diese Übersicht muss auch die Berechtigungshistorie einer Person sowie Informationen über den jeweils gestellten Berechtigungsantrag und durchgeführten Prüf- und Freigabeprozess umfassen.

Dies stellt also eine Zuordnung von Benutzern zu (Mengen von) Rechten dar. Zusätzlich soll die Bestandsübersicht jedoch umgekehrt darüber Auskunft geben können, welche Zugriffsrechte auf bestimmten Systeme und Anwendungen gelten, also die Zuordnung der Anwendung bzw. des Systems zu Anwendern und Rechten. Zumindest für alle kritischen OT-Infrastrukturen sollte dies vorliegen und aktuell sein. Idealerweise werden hier die effektiven Berechtigungen dargestellt, also die tatsächlich im System technisch gesetzten anstelle der aus der historischen Setzung und Löschung ableitbaren. Dies hat den Vorteil, dass eine Chance besteht, illegitim am Berechtigungsprozess vorbei hinzugefügte Berechtigungen zu erkennen.

Automatisierte Auswertung

Es bietet sich an, die Zusammenstellung der effektiven Berechtigungen automatisiert vorzunehmen und dabei gleichzeitig eine Auswertung durchzuführen. So könnten Änderungen (Deltas) gemeldet werden oder Abweichungen von einem Standard- oder Sollzustand besonders dargestellt werden.

Protokollierung kritischer Tätigkeiten

Kritische Berechtigungen können auf folgende Arten missbraucht werden:

1. durch Innentäter
2. durch Social Engineering
3. unabsichtlich durch Fehlhandlungen

4. unbewusst durch einen kompromittierten Client oder Kommunikationskanal

Zum ersten Fall lässt sich die Wahrscheinlichkeit mindern, zu den anderen zumindest die Nachvollziehbarkeit und Aufklärung verbessern, wenn kritische administrative Tätigkeiten protokolliert werden. Dies sollte zentral erfolgen und Bedarf einer systematischen Auswertung (siehe auch IND.1.M10 *Monitoring, Protokollierung und Detektion*). Um in den Fällen 1 und eventuell auch 4 effektiv sein zu können, dürfen die Protokolle nicht einfach durch dieselbe Rolle gelöscht oder manipuliert werden können, deren Handlung protokolliert wurde. Zumindest sollte eine Löschung oder Manipulation an eine weitere, unabhängige Rolle gemeldet werden. Noch besser ist, die Löschung oder Manipulation technisch zu verhindern und Versuche der Löschung oder Manipulation automatisch an eine unabhängige Rolle zu melden.

IND.1.M16 Stärkere Abschottung der Zonen (H)

Schnittstellen zu Zonen mit hohem oder sehr hohem Schutzbedarf können eine stärkere Abschottung erfordern, als dies durch Layer-4-Firewall-Systeme oder durch die oft eingeschränkten Absicherungsmöglichkeiten von OT-Komponenten möglich ist. Insbesondere bei Außenschnittstellen der OT und des Office-Netzes sollten die Schnittstellen einer Sicherheitsbewertung unterzogen werden.

Die Sicherheitsbewertung sollte unter Berücksichtigung der Ausgestaltung der jeweiligen Schnittstelle auf Basis der Elementaren Gefährdungen erfolgen. Bei dieser Vorgehensweise sind zunächst die relevanten elementaren Gefährdungen zu bestimmen und die jeweilige Schnittstelle auf angemessenen Schutz zu untersuchen. Aus dieser Betrachtung heraus kann es erforderlich werden, Schnittstellen zu verwerfen oder diese gegen die ermittelten Bedrohungen zusätzlich abzusichern, wenn die etablierten Sicherheitsmaßnahmen die ermittelten Gefährdungen nicht hinreichend abdecken.

Die jeweils erforderlichen Schutzmaßnahmen ergeben sich aus der Risikobetrachtung und können auch Anpassungen an den kommunizierenden OT-Komponenten wie Härtung, Virenschutzprogramme, Patch-Management oder Vergabe minimaler Rechte erfordern. Aufgrund der dort häufig eingeschränkten Handlungsmöglichkeiten können solche Schutzmaßnahmen auch auf einem Schnittstellensystem realisiert werden. Zu diesem Zweck kann der Aufbau einer DMZ in Betracht gezogen werden.

Die Kommunikation zwischen den betrachteten Sicherheitsbereichen (etwa externer Zugriff in die OT) wird in dieser DMZ durch Application-Layer-Gateways (ALG) wie etwa Proxy- oder Datentransfer-Server terminiert. Dabei können auf dem Gateway spezifische Inhaltsprüfungen wie etwa Prüfung auf Schadprogramme oder Datenformatprüfungen (z. B. XML-Prüfung durch eine Web Application Firewall oder Protokollprüfungen durch Industrie-Firewalls) vorgenommen werden. Die Firewall-Systeme gewährleisten, dass lediglich vordefinierte Kommunikationswege möglich sind und die erwünschte Kommunikationsrichtung des Verbindungsaufbaus beachtet wird. Die ALGs können speziell gehärtet werden und die für die Zone erforderlichen Sicherheitsanforderungen durchsetzen, ohne dass Anpassungen an den OT-Komponenten notwendig sind. Eine solche DMZ-Infrastruktur kann je nach Umgebungsanforderungen pro Schnittstelle oder für mehrere Schnittstellen genutzt werden.

IND.1.M17 Regelmäßige Sicherheitsüberprüfung (H)

Organisation interner und externer Audits

OT-Infrastrukturen werden oftmals noch seltener auditiert als die Büro- und Gebäude-IT. Neben mangelndem Sicherheitsbewusstsein ist dies häufig den hohen Verfügbarkeitsanforderungen solcher Umgebungen geschuldet.

Vor diesem Hintergrund sollte ein geeigneter Überprüfungsprozess für die Umgebung entwickelt werden, der unter Berücksichtigung der Gegebenheiten geeignete Überprüfungsverfahren auf Basis manuell oder automatisiert durchgeführter Richtlinienkonformitätsprüfungen (Konfigurations- und Richtlinienprüfungen) umfasst. Besonderes Augenmerk sollte hierbei auf exponierte Systeme mit Außenschnittstellen sowie auf Systeme mit direktem Benutzerzugriff gelegt werden, da diese einer erhöhten Bedrohungslage ausgesetzt sind.

Bei der Planung sollte zudem berücksichtigt werden, dass sich bestimmte Schwachstellen prinzipbedingt nur durch praktische Schwachstellenprüfungen (Vulnerability Assessment, häufig auch als Penetrationstest

bezeichnet) wirtschaftlich aufdecken lassen. Durch eine solche Maßnahme kann grundsätzlich die Verfügbarkeit der Umgebung zeitweise vermindert werden.

Sowohl interne als auch externe Audits sollten stets in Abstimmung mit den zuständigen Administratoren während der Betriebszeiten durchgeführt werden.

Für die Tests werden umfangreiche Fähigkeiten und Erfahrungen benötigt, welche bei Bedarf von extern bezogen werden können. In größeren Institutionen lohnt eventuell auch der Aufbau eigener Kompetenz. Je nach Schutzbedarf empfiehlt sich ein Audit pro System und Jahr bis hinunter zu einem Audit vor Produktivsetzung sowie bei größeren Änderungen in der Umgebung. Dies kann umfassen, bleibt aber nicht beschränkt auf

- Erweiterungen der Anlagen (Hard- und Software),
- Einrichtung neuer Außenanbindungen,
- Ersatzinstallationen sowie
- substanzielle Upgrade-Vorgänge und System- bzw. Software-Migrationen.

IND.1.M18 Protokollierung (B)

Es liegen keine Hinweise zur Umsetzung vor. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.bund.de entgegengenommen.

IND.1.M19 Erstellung von Datensicherungen (B)

Es liegen keine Hinweise zur Umsetzung vor. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.bund.de entgegengenommen.

IND.1.M20 Systemdokumentation (S)

Es liegen keine Hinweise zur Umsetzung vor. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.bund.de entgegengenommen.

IND.1.M21 Dokumentation der Kommunikationsbeziehungen (S)

Es liegen keine Hinweise zur Umsetzung vor. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.bund.de entgegengenommen.

IND.1.M22 Zentrale Systemprotokollierung und -überwachung(S)

Es liegen keine Hinweise zur Umsetzung vor. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.bund.de entgegengenommen.

IND.1.M23 Aussonderung von ICS-Komponenten (S)

Es liegen keine Hinweise zur Umsetzung vor. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.bund.de entgegengenommen.

IND.1.M24 Kommunikation im Störfall (H)

Es liegen keine Hinweise zur Umsetzung vor. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.bund.de entgegengenommen.

2.2. Maßnahmen zum Baustein ORP.3 Organisation und Personal

IND.1.ORP.3.M6 Planung und Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit (B)

Die Umsetzung der notwendigen Sensibilisierung und Wissensbildung des Personals kann auf unterschiedliche Art erfolgen. Es kann sich um spezielle Schulungsveranstaltungen handeln oder um Online-Schulungen. Inhalte und Häufigkeit sollten sich an den Aufgaben der Mitarbeiter und den

Bedrohungsszenarien orientieren. Eine einmalige Information ist mindestens für alle Mitarbeiter durchzuführen.

Betriebspersonal sollte auf die an einem OT-spezifischen Arbeitsplatz relevanten Bedrohungen oder Probleme hingewiesen werden. Dies kann z. B. der Umgang mit Wechseldatenträgern oder Smartphones sein.

Der ICS-Informationssicherheitsbeauftragte und die jeweils zuständigen Rollen in der OT sollten spezifischer hinsichtlich der Bedrohungslage und notwendiger Handlungsbedarfe geschult werden.

Für KMUs bietet es sich in der Regel an, die Schulung durch Externe durchführen zu lassen, da diese stets aktuelles Praxiswissen mitbringen können. Bei größeren Institutionen lohnt sich eventuell die Errichtung eines eigenen Kursprogramms.

Vorschläge für genauere Fortbildungspläne können z. B. dem Dokument *Empfehlungen für Fortbildungs- und Qualifizierungsmaßnahmen im ICS-Umfeld* [BSI-CS 123] entnommen werden.

Zusätzlich ist zu empfehlen, die Sensibilisierung bezüglich Social Engineering regelmäßig und mit Nachdruck voranzutreiben, etwa durch Aufklärungskampagnen oder durch mit Datenschutz und Betriebsrat abgestimmte sorgsame Tests, welche niemanden persönlich bloßstellen dürfen.

2.3. Maßnahmen zum Baustein OPS.1.1.4 Schutz vor Schadprogrammen

IND.1.OPS.1.1.4.M3 Auswahl eines Virenschutzprogramms (B)

Es besteht die Möglichkeit, mittels spezieller Sicherheitssoftware zur Applikationskontrolle, das Ausführen von Programmen zu überwachen und einzuschränken. Anders als bei gängigen Virenschutzprogrammen wird nicht versucht, unerwünschte Software zu blockieren, sondern es wird der Ansatz verfolgt, ausschließlich erwünschten Programmen die Ausführung zu erlauben.

Demzufolge können zwei unterschiedliche Ansätze unterschieden werden, um Anwendungen und unerwünschtes Verhalten eines Systems zu erkennen und zu verhindern (z. B. im Fall von Schadprogrammen):

1. Bei dem **Blacklist-Ansatz** gewöhnlicher Virenschutzprogramme geschieht dies auf der Grundlage bekannter Signaturen und Heuristiken unerwünschter Anwendungen. Diese Herangehensweise weist einige Schwachstellen auf, wie z. B. dass sich neuartige Schadprogramme selbstständig bei jeder neuen Kopie verändern können und somit eine neue, noch unbekannte Signatur aufweisen. So ist der erfolgreiche Schutz von der Aktualität und Verfügbarkeit der Signaturen abhängig.
2. Beim **Application Whitelisting** werden nur solche Anwendungen und solches Verhalten erlaubt, die explizit freigegeben wurden. Alles andere ist verboten. Auf diese Weise besteht keine Abhängigkeit zu aktuellen Signaturen. Insbesondere bei Systemen wie im OT-Umfeld, die nur geringfügigen Änderungen durch Softwareinstallationen unterliegen, eignet sich dieses Verfahren. Daher sollte, soweit möglich, eine Applikationskontrolle stets nach dem Whitelist-Ansatz erfolgen.

Application Whitelisting

Um das Ausführen von unerlaubter Software zu verhindern, kann eine Schutzsoftware nach dem White-List-Ansatz beispielsweise auf folgende unterschiedliche Attribute zurückgreifen:

- Zertifikate (Signieren von vertrauenswürdiger Software z. B. durch eine zentrale Stelle),
- Dateisystempfad (bestimmte Bereiche werden als vertrauenswürdig deklariert),
- Hashes (die Anwendungen und möglicherweise unbefugte Änderungen werden anhand eines Hashwertes der Dateien identifiziert),
- System- und Benutzerverhalten (z. B. Nutzung gewisser TCP-Ports, Bedienung nur zu bestimmten Zeiten).

2.4. Maßnahmen zum Baustein NET.1.2 Netzmanagement

IND.1.NET.1.2.M8 Zeitsynchronisation (B)

Eine Vielzahl an Prozessen, aber auch administrative Tätigkeiten, beruhen in der OT auf einer genauen und abgestimmten Zeit (z. B. die Nachvollziehbarkeit verteilter Protokolldaten, Beigabe von Zusatzstoffen in der Produktion zum richtigen Zeitpunkt etc.). Es muss aufgrund der Applikationsanforderungen abgewogen werden, wie die Zeitsynchronisation erfolgt.

Für die Synchronisation kann das Network Time Protocol (NTP) oder IEEE 1588 genutzt werden.

Das Zeitsignal für die Systeme sollte aus einer vertrauenswürdigen Quelle stammen. z. B. sollten Zonen hoher Kritikalität (im Hinblick auf eine unterbrechungsfreie Prozess-Fortführung in Echtzeit) ihre Zeit nicht aus einer weniger geschützten Zone beziehen, wenn das Signal möglicherweise manipuliert werden könnte. Die Clients auf den OT-Komponenten sollten die Zeit in einem einheitlichen, standardisierten Format interpretieren (z. B. unter Berücksichtigung von Zeitzonen, Winter- und Sommerzeit).

3. Weiterführende Informationen

3.1. Wissenswertes

In Abgrenzung zur allgemeinen Büro- und Gebäude-IT sind in der Betriebstechnik einige weitere OT-spezifische Begriffe gebräuchlich. Diese Begriffe werden im Folgenden in den *Begriffsbestimmungen* definiert (siehe auch [BSI-ICS SK]).

Darüber hinaus werden unter *Grundcharakteristika der OT* grundlegende Aspekte der Betriebstechnik erläutert. Insbesondere wird beschrieben, inwiefern sich die OT in diesen Aspekten von der allgemeinen Büro- und Gebäude-IT unterscheidet.

Begriffsbestimmungen

Für eine ausführliche Beschreibung typischer OT-Infrastrukturen wird auf das ICS-Security-Kompendium verwiesen (siehe Kapitel 2.3 *Hierarchische Gliederung von ICS* und Kapitel 2.5 *Kommunikationsvorgänge*). Dort werden insbesondere auch die Level (Zonen) 1-5 (siehe IND.1.M5 *Entwicklung eines geeigneten Zonenkonzepts*) genauer dargestellt.

- **OT (Operational Technology)**: Betriebstechnik ist Hard- und Software, die Änderung durch die direkte Überwachung sowie Steuerung von physischen Geräten, Prozessen und Ereignissen in der Institution erfasst und bewirkt.
- **ICS (Industrial Control System)**: ICS ist ein Oberbegriff für Automatisierungslösungen zur Steuerung technischer Prozesse im industriellen Umfeld und ein Teil der OT.
- **PLC (Programmable Logic Controller), SPS (Speicherprogrammierbare Steuerung), PNK (Prozessnahe Komponente); MTU (Main Terminal Unit), Controller**: Diese Begriffe bezeichnen (abhängig von der sie einsetzenden Branche) eine Automatisierungskomponente mit Verarbeitungsfunktion. Diese werden zur Steuerung oder Regelung in einer Maschine oder Anlage eingesetzt und auf digitaler Basis programmiert.
- **Sensor, Messwertaufnehmer, Endschalter, Taster/Schalter, Initiator, Grenztaster:** Dies sind Komponenten zur Erfassung physikalischer Größen und deren Wandlung in ein Einheitssignal. Als Interfaces kommen dabei analoge Standardschnittstellen wie 4...20 mA Stromschnittstelle, 0-10V, 24V-Gleichspannung usw. aber auch digitale Kommunikationsprotokolle wie Feldbusse (z. B. PROFIBUS PA) oder digitale Punkt-zu-Punkt-Verbindungen (z. B. IO-Link) zum Einsatz.
- **Aktuator, Aktor**: Ein Aktor wandelt eine Steuergröße (z. B. elektrisches, hydraulisches oder pneumatisches Signal) in die Stellgröße zum Beeinflussen des Prozessgeschehens um. Bezüglich der Anbindung kommen die gleichen Techniken zum Einsatz wie bei Sensoren.

- **HMI (Human Machine Interface); BUB (Bedien- und Beobachtungskomponenten), ABK (Anzeige- und Bedienkomponente)**: Diese Komponenten dienen der Verwirklichung von Anzeige- und Bedienfunktionen. Typische Anwendungen sind z. B. die Darstellung und Bedienung des Prozesses über Prozessfließbilder, Standard-Bedienbilder (Faceplates), Trendbilder, Ablaufsprachenbilder, Gruppenbilder. Darüber hinaus stehen Funktionen für die Alarmverwaltung, die Datenarchivierung und Auswertung sowie die Systemdiagnose und Dokumentation.
- **Programmier- und Testgerät, Service-Rechner, Engineering Workstation**: Diese Komponenten ermöglichen die Konfiguration und Inbetriebnahme von Automatisierungskomponenten.
- **DCS (Digital Control System), PLS (Prozessleitsystem)**: DCS werden meist für größere verfahrenstechnische Anlagen eingesetzt. Sie können eine Vielzahl von Merkmalen, wie Alarmsysteme, Anlagenvisualisierung (Kurvenaufzeichnung von Messwerten), Benutzerverwaltung, zentrale Datenhaltung sowie Wartungs- und Entwicklungswerkzeuge aufweisen.

Grundcharakteristika der OT

Die OT umfasst alle Technik, die der Interaktion mit der physischen Welt dient. Ein Teilbereich sind Industrial Control Systems (ICS). Diese werden überall dort eingesetzt, wo technische Prozesse automatisiert werden. Sie werden für das Messen, Steuern, Regeln und Bedienen von industriellen Abläufen benutzt. Beispiele hierfür sind die Verfahrens- und Prozesstechnik, die Fertigungsautomatisierung, die Ver- und Entsorgungsnetze (z. B. Strom, Wasser, Abwasser, Gas, Fernwärme) oder die Betriebstechnik für Transport und Verkehr (z. B. Schienen- und Straßenverkehr). Darüberhinaus gehören zur OT auch Labor- und Analysegeräte oder die Gebäudeautomation.

Die individuellen Anforderungen an die OT einer Institution werden unmittelbar durch die betrieblichen Anforderungen der Produktionsprozesse bestimmt.

Garantierte Antwortzeiten

Regelkreise gewährleisten im Hinblick auf ihr Zeitverhalten definierte Reaktionszeiten. Kommt es aufgrund von (temporären) Modifikationen im Bereich der Software zu Änderungen am Zeitverhalten der OT, kann dies zu Störungen im Produktionsprozess führen und etwa eine erhöhte Ausschussquote zur Folge haben.

Spezielle gesetzliche Auflagen und Beschränkungen

Es gibt viele Anwendungen, in welchen der Betrieb der Anlagen an behördliche Auflagen gebunden ist (z. B. CE-Zertifizierung von Geräten, Safety-Richtlinien, Richtlinien bei der Produktion von pharmazeutischen Produkten). In diesen Fällen bedürfen wesentliche Änderungen, worunter auch Softwareänderungen an den eingesetzten OT-Komponenten fallen können, eines dedizierten Genehmigungsprozesses. Aufgrund des vorgeschriebenen Prüfprozesses sind hier beispielsweise die Möglichkeiten zum zeitnahen Einspielen von Sicherheitsupdates begrenzt bzw. nicht gegeben.

Software in der OT

Bei OT-Software-Komponenten ist zwischen Firmware, Anwendungssoftware und Software zur Parametrierung zu unterscheiden.

Die Firmware wird von den Herstellern nur bei auftretenden Fehlfunktionen aktualisiert. Änderungen bei den Anwenderprogrammen erfolgen nur, wenn die Anlagen geändert oder erweitert werden. Parametrierungen erfolgen im normalen Betrieb.

Änderungen und Updates in der OT

Das Ändern von Systemkonfigurationen oder das Einspielen von Updates in OT-Komponenten bereiten, im Gegensatz zum Einspielen von Updates in der Büro-IT, häufig größere Probleme. Vor der Maßnahme sind mögliche Auswirkungen auf das Zeitverhalten oder andere Auswirkungen auf die OT-Systeme zu prüfen. Bei der Durchführung kann es zu Einschränkungen der Verfügbarkeit (z. B. durch einen notwendigen Neustart) kommen. Nach Abschluss der Maßnahme ist eine Abnahme (etwa bzgl. Safety-Aspekten) zu erneuern. Dies führt dazu, dass Änderungen und Updates in der Regel nur im Rahmen von geplanten Anlagenstillständen eingebracht werden.

Lange Lebenszyklen von OT-Hardware

Im Gegensatz zur Büro-IT werden ICS häufig mit sehr langlebigen Hardware-Komponenten (Gerätetypen) sowie auch langlebigen Software-Komponenten, z. B. überholten Windows-Betriebssystemen, betrieben. Dies führt dazu, dass möglicherweise aktuelle Software, Firmware oder Protokolle nicht unterstützt werden.

Spezielle Normen, Standards und Richtlinien

Im Bereich der OT gibt es eine Vielzahl von Normen, Standards und Richtlinien, die stringente Anforderungen an die Betriebstechnik in einer Institution stellen (z. B. IEC 61508-3 im Bereich der Softwareentwicklung). Weitere Quellen führt das ICS-Security-Kompendium [BSI-ICS SK] (siehe Kapitel 4 *Organisationen, Verbände und deren Standards*) auf.

3.2. Weiterführende Literatur

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27019 *Information technology – Security techniques - Information security controls for the energy utility industry* Vorgaben für die Absicherung von Energieversorgern.

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.

Die Bundesnetzagentur (BNetzA) formuliert im *IT-Sicherheitskatalog gemäß §11 Absatz 1a Energiewirtschaftsgesetz* für Betreiber Schutzziele für die Informationssicherheit von Strom- und Gasnetzen und Anforderungen für die Umsetzung dieser Schutzziele.

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

Mit der Ergänzung *ICS-Security-Kompendium - Testempfehlungen und Anforderungen für Hersteller von Komponenten* gibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) Hilfestellungen für den Test von OT-Komponenten.

Die Allianz für Cyber-Sicherheit bietet mit der BSI-Veröffentlichung *Empfehlungen für Fortbildungs-und Qualifizierungsmaßnahmen im ICS-Umfeld* Hilfestellungen zur organisatorischen Verankerung der Informationssicherheit in Institutionen.

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.

Gartner IT Glossary: Operational Technology (OT)

Folgende **internationale** und **nationale Normen** und **Richtlinien** stellen weitere Hilfsmittel zur Verfügung:

- IEC 62443-2-1:2010 *Industrial communication networks - Network and system security,* Part 2-1: *Establishing an industrial automation and control system security program*: International Electrotechnical Commission (IEC), 2010
- Richtlinie VDI/VDE 2182: Blatt 1, *Informationssicherheit in der industriellen Automatisierung - Allgemeines Vorgehensmodell*, Januar 2011
- Richtlinie VDI/VDE 2182: Blatt 2.1, *Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomation für Hersteller - Speicherprogrammierbare Steuerung (SPS)*, Februar 2013
- Richtlinie VDI/VDE 2182 : Blatt 3.1, *Informationssicherheit in der industriellen Automatisierung - Anwenderbeispiel des Vorgehensmodells in der Prozessautomation für Hersteller - Prozessleitsystem einer LDPE-Anlage*, September 2013

- DIN ISO/IEC 27001:2013 + Cor. 1:2014 + 2:2015 *IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen*, letzte Ausgabe: 2017-06
- DIN ISO/IEC 27002:2013 + Cor 1:2014 + Cor 2:2015 *IT-Sicherheitsverfahren - Leitfaden für das Informationssicherheitsmanagement*, letzte Ausgabe: 2017-02
- DIN ISO/IEC TR 27019:2015-03 (DIN SPEC 27019:2015-03) *Informationstechnik - Sicherheitsverfahren - Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002 (ISO/IEC TR 27019:2014)*

3.3. Quellenverweise

[BSI-CS 123] *Empfehlungen für Fortbildungs-und Qualifizierungsmaßnahmen im ICS-Umfeld*: BSI-Veröffentlichungen zur Cyber-Sicherheit, Version 2, Juli 2018, https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_123.html , zuletzt abgerufen am 14.04.2021

[BSI-ICS SK] *ICS-Security-Kompendium*: Bundesamt für Sicherheit in der Informationstechnik (BSI), November 2013, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.html, zuletzt abgerufen am 14.04.2021