Bundesamt
für Sicherheit in der
Informationstechnik

IND: Industrielle IT

IND.1: Prozessleit- und Automatisierungstechnik

1 Beschreibung

1.1 Einleitung

Prozessleit- und Automatisierungstechnik (Operational Technology, OT) ist Hard- und Software, die physische Geräte, Prozesse und Ereignisse in der Institution überwacht und steuert.

In der Industrie, zu der unter anderem auch die Kritischen Infrastrukturen gehören, zählen dazu insbesondere industrielle Steuerungssysteme (Industrial Control Systems, ICS) und Automationslösungen, die dort Steuerungs- und Regelfunktionen aller Art übernehmen. Weitere Beispiele sind Laborgeräte, z. B. automatisierte Mikroskope oder Analysewerkzeuge, Logistiksysteme, wie Barcodescanner mit Kleinrechner, oder Gebäudeleittechnik.

Die in der Vergangenheit übliche physische Trennung der OT von anderen IT-Systemen und Datennetzen in Büroanwendungen ist heute aufgrund zunehmender Integrationsanforderungen nur in Ausnahmefällen bei erhöhtem Schutzbedarf anwendbar. Mehrstufige Produktionsschritte und deren übergreifende Steuerung sowie regulatorische Anforderungen machen es zunehmend notwendig, die OT auch über Organisationsgrenzen hinweg zu öffnen. Diese Entwicklung wird durch den Trend zur Optimierung von Fertigungsprozessen noch beschleunigt, vor allem im Rahmen der Industrie 4.0.

Da in der OT zunehmend auch IT-Komponenten aus der Office-IT eingesetzt werden, ist diese inzwischen ähnlich gefährdet. Gleichzeitig weist die OT gegenüber der klassischen IT aber wesentliche Unterschiede auf, die es erschweren, dort etablierte Sicherheitsverfahren anzuwenden. So kann es aufgrund von Herstellervorgaben oder gesetzlichen Anforderungen Beschränkungen geben, die Veränderungen an Komponenten verhindern oder erschweren, wie zum Beispiel das Einspielen von Sicherheitsupdates oder nachträgliche Härtungsmaßnahmen. Die OT unterliegt zudem in der Regel deutlich längeren Lebenszyklen, auch über die Herstellerunterstützung hinaus, sodass Sicherheitsupdates nicht durchgängig verfügbar sind.

Ein wesentlicher Unterschied ergibt sich für die OT auch aus den oft hohen Verfügbarkeits- und Integritätsanforderungen. Denn im Vergleich dazu ist bei der Office-IT die Vertraulichkeit eher von nachrangiger Bedeutung. Störungen von OT-Systemen können dagegen Gefährdungen von Leib, Leben und Umwelt nach sich ziehen und sind zumeist nicht durch einen Neustart zu beheben.

1.2 Zielsetzung

Ziel dieses Bausteins ist es, geeignete Anforderungen an die Informationssicherheit der OT aufzuzeigen.

Er enthält komponentenübergreifende, konzeptionelle und architektonische Sicherheitsanforderungen.

1.3 Abgrenzung und Modellierung

Der Baustein IND.1 *Prozessleit- und Automatisierungstechnik* ist auf jedes IT-System mit Prozessleit- und Automatisierungstechnik innerhalb des Informationsverbunds mindestens einmal anzuwenden.

Der Baustein ist übergreifend umzusetzen. Bestehen in den einzelnen Bereichen mit Prozessleit- und Automatisierungstechnik unterschiedliche Sicherheitsanforderungen an die Informationssicherheit, sollte der Baustein auf jedes IT-System getrennt angewandt werden.

Die Ausgestaltung der OT kann je nach Zweck, Branche, den eingesetzten IT-Systemen und der Technik sowie aufgrund des langen Einsatzzeitraums selbst bei vergleichbaren Anwendungsfällen stark variieren. Werden die Sicherheitsmaßnahmen auf Basis der Anforderungen aus diesem Baustein ausgewählt, sind diese Besonderheiten dabei zu berücksichtigen. Sie können wesentlichen Einfluss auf die Ausgestaltung des Sicherheitskonzepts nehmen. Auch der Risikoanalyse kann aus diesem Grund bereits bei der Erstellung eines Sicherheitskonzepts für den normalen Schutzbedarf eine hohe Bedeutung zukommen.

Das Betriebspersonal sollte in Bezug auf relevante Bedrohungen und Gefährdungen geschult und sensibilisiert werden. Hierfür ist der Baustein ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit* umzusetzen.

Zusätzlich zu diesem Baustein ist die umgebende Infrastruktur der OT, also Standorte, Anlagen, Gebäude oder Räume, durch möglichst spezifische Bausteine zu modellieren, um die Schutzwirkung dieses Bausteins zu ergänzen.

Für eine geeignete Protokollierung im Bereich der Prozessleit- und Steuerungstechnik ist der Baustein OPS.1.1.5 *Protokollierung* umzusetzen.

ICS-Systeme sollten grundsätzlich mit berücksichtigt werden, wenn der Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* umgesetzt wird.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein IND.1 *Prozessleit- und Automatisierungstechnik* von besonderer Bedeutung:

2.1 Beeinträchtigung durch schädliche Umgebungseinflüsse

ICS-Komponenten sind in industriellen Umgebungen häufig besonderen Bedingungen ausgesetzt, die den sicheren Betrieb beeinträchtigen können. Dazu zählen extreme Wärme, Kälte, Feuchtigkeit, Staub, Vibration oder auch ätzend oder korrodierend wirkende Umgebungen. Häufig treten auch mehrere Faktoren gleichzeitig auf. Durch solche schädlichen Einflüsse können ICS-Komponenten schneller verschleißen und früher ausfallen.

2.2 Ungeeignete Einbindung der OT in die Sicherheitsorganisation

Durch unterschiedliche Rahmenbedingungen, Kenntnisse und Vorgehensweisen in den Bereichen Office-IT und OT können bei übergreifenden Sicherheitsvorgaben Probleme bei der Umsetzung auftreten. Sicherheitsvorgaben aus dem Bereich der Office-IT können einerseits aufgrund technischer oder prozessualer Besonderheiten bei ICS-Systemen nicht umsetzbar sein. Andererseits könnte es sein, dass ICS-spezifische Informationssicherheits- und Safety-Aspekte, also Aspekte der funktionalen Sicherheit, den Informationssicherheitsbeauftragten der Office-IT nicht bekannt sind. So können Reibungsverluste in der Kommunikation und der Umsetzung entstehen. Außerdem könnten Risiken nicht erkannt oder unzureichend behandelt werden.

2.3 Ungeeignete Einbindung der OT in betriebliche Abläufe

Auch wenn sich OT und IT zunehmend annähern, gibt es Besonderheiten, die das Übertragen etablierter betrieblicher Abläufe erschweren. Betriebliche Eingriffe im Rahmen des Change- und Incident-Managements zur sicheren Konfiguration, Störungsbehebung oder zum Einspielen von Sicherheitsupdates können etwa eine erneute behördliche Freigabe oder den Verlust des Herstellersupports nach sich ziehen. Nicht autorisierte Änderungen können die Funktion einer Komponente beeinflussen und damit potenziell auch Auswirkungen auf deren Safety-Funktion haben.

Die OT dient der Überwachung, Steuerung und Automatisierung von technischen Abläufen. Störungen dieser Systeme können zu Produktionsausfällen, technischen oder personellen Schäden und Umweltschäden führen. Diese potenziellen Auswirkungen müssen bei betrieblichen Eingriffen berücksichtigt werden.

2.4 Unzureichender Zugangsschutz

Industrielle Steuerungsanlagen werden immer seltener vollständig autark von der Außenwelt betrieben. Moderne Fertigungs- und Erzeugungsprozesse erfordern einen Informationsaustausch mit vor- und nachgelagerten Produktionsschritten und sind häufig an die zentralen Produktionsplanungs- und Steuerungssysteme einer Institution angebunden. Um elektronisch Informationen auszutauschen, müssen die Produktionsanlagen außerdem mit Drittnetzen, wie der Office-IT oder den Netzen von Partnern und Dienstleistern, verbunden sein. Interaktive Zugriffe von Büro- oder Mobilarbeitsplätzen und der betrieblich bedingte elektronische Datenaustausch, etwa zur Bereitstellung von Software und Updates, bedeuten eine weitere Vernetzung mit der Außenwelt. Auch die Einrichtung von Fernzugängen für eine Rufbereitschaft oder für Dienstleister können den Zugriff von außen ermöglichen.

Werden die erforderlichen Kommunikationskanäle zu weit gefasst oder unzureichend gesichert, können Angreifer diese Zugangswege ausnutzen, um auf diese zuzugreifen und um diese zu kompromittieren. Industrielle Steuerungsanlagen können einerseits von zielgerichteten Schadsoftware-Angriffen betroffen sein. Andererseits können sie auch von Schadprogrammen kompromittiert werden, die eigentlich auf die Manipulation der Office-IT abzielen. Durch eine fehlende Segmentierung oder Kontrolle des Datenverkehrs kann Schadsoftware auf die Systeme gelangen.

Aber auch der Einsatz von Virenschutz-Software kann ein Risiko für die OT darstellen. Etwa dann, wenn keine Herstellerfreigabe für die Umgebung vorliegt oder Fehlerkennungen und aktive Systemeingriffe den Betrieb gefährden. Ein vergleichbares Störungspotenzial kann sich auch aus dem Betrieb netzbasierter Intrusion Prevention Systeme (IPS) ergeben, weil dabei Verbindungen unterbrochen werden können.

2.5 Unsicherer Projektierungsprozess/Anwendungsentwicklungsprozess

Anpassungen und Weiterentwicklungen von IT-Systemen, Anwendungen und Steuerungsprogrammen können einen kritischen Eingriff in die Steuerungsanlage darstellen. Störungen können dabei aus funktionalen Fehlern bei unzureichenden Test- und Validierungsschritten, fehlerhaften oder manipulierten Projektierungsdaten oder Schwachstellen in der Software entstehen. Etwa dann, wenn wichtige Sicherheitsfunktionen wie Ein- und Ausgabe- oder Berechtigungsprüfungen unzureichend umgesetzt werden.

Weitere Gefahren können sich aus unsicheren Entwicklungsumgebungen, der ungeeigneten Ablage von Programmcode, Dokumentations- oder Projektdaten sowie aus den Datentransferschnittstellen ergeben.

2.6 Unsicheres Administrationskonzept und Fernadministration

Die Adminstration industrieller Steuerungssysteme erfolgt in bestimmten Fällen über Netzzugriffe. Dabei werden unterschiedliche öffentliche und private Netze wie z. B. Telefonnetze, Funknetze,

Mobilfunknetze und zunehmend das Internet genutzt. Sind diese Zugänge unzureichend geplant, unsicher konfiguriert oder werden diese nicht überwacht, können Angreifer unter Umständen unbefugt auf einzelne OT-Komponenten oder die Infrastruktur zugreifen. So können sie etwa die Sicherheitsmechanismen am Perimeter umgehen.

2.7 Unzureichende Überwachungs- und Detektionsverfahren

Eine wesentliche Funktion industrieller Steuerungssysteme ist es, den Betrieb eines automatisierten Prozesses zu überwachen. So wird etwa bei unterschrittenen Füllständen oder abweichenden Temperaturen oder Ventilstellungen eine entsprechende Warnung ausgegeben. Die unterstützende IT-Infrastruktur wird dagegen häufig nicht ausreichend überwacht.

Werden ungewöhnliche oder sicherheitsrelevante Ereignisse solcher Betriebsumgebungen nicht oder nur unzureichend kontrolliert, können Angriffsversuche, Netzengpässe oder absehbare Ausfälle nicht frühzeitig erkannt werden. Darüber hinaus kann auch eine mangelhafte Auswertung oder eine unübersichtliche Darstellung der Ereignisse dazu führen, dass Warnungen und Fehler verspätet erkannt werden.

2.8 Unzureichendes Testkonzept

Industrielle Steuerungsanlagen unterliegen oft hohen Verfügbarkeitsanforderungen. Denn Störungen oder technische Ausfälle können unter Umständen schwerwiegende Schäden und hohe Folgekosten nach sich ziehen. Aus diesem Grund sind OT-Systeme oft ausfallsicher konzipiert.

Werden Änderungen an einer solchen Umgebung nicht sorgfältig geplant, abgestimmt und in einer realitätsnahen Umgebung getestet, besteht die Gefahr, dass logische oder softwaretechnische Fehler übersehen werden und Störungen in der Anlage auftreten. Selbst vom Hersteller freigegebene Updates können bei der Modifikation oder Anpassung von Parametern Störungen an der Anlage verursachen.

2.9 Mangelnde Life-Cycle-Konzepte

Neben spezifischen ICS-Komponenten werden zunehmend Komponenten und Software aus der Office-IT eingesetzt. Aufgrund der sehr langen Lebenszyklen in der OT werden diese Komponenten in der Regel deutlich länger betrieben als in der Office-IT üblich, teilweise auch über die Hersteller-Support-Zyklen hinaus.

Dies hat zur Folge, dass nach dem Ablauf der Herstellerunterstützung keine Updates gegen Schwachstellen mehr zur Verfügung gestellt werden. Dem gegenüber stehen oftmals öffentlich dokumentierte Schwachstellen sowie Werkzeuge, die diese Schwachstellen ausnutzen. Dies ermöglicht auch nicht versierten Angreifern ein erfolgreiches Eindringen in die OT-Systeme. Das gilt auch, wenn Updates nicht oder nur mit sehr großer Verzögerung eingespielt werden.

Die langen Einsatzzeiten können zudem zu Problemen bei der Beschaffung von Ersatzteilen führen, etwa wenn diese nicht mehr produziert werden. Dies gilt auch für mögliches Know-how zur Pflege und Wartung von Alt-Systemen, über das neue Mitarbeiter nicht mehr verfügen.

Zudem enthalten ICS-Komponenten häufig detaillierte Informationen über den geregelten oder überwachten Prozess. Auch aus sonstigen übertragenen Werten, wie Mess- oder Steuerungsdaten, lassen sich diese Informationen teilweise rekonstruieren. Gleiches gilt für Steuerungsprogramme oder -parameter. Angreifer könnten so an Geschäftsgeheimnisse gelangen.

2.10 Unzureichende Sicherheitsanforderungen bei der Beschaffung

Aufgrund nicht ausreichender Sicherheitsanforderungen und aus Kostengründen wird bei der Beschaffung häufig die Informationssicherheit nicht berücksichtigt. Dadurch können in ICS-Komponenten mitunter schwerwiegende Schwachstellen, z. B. in Hardware oder Software enthalten sein, die sich später nur sehr aufwändig beheben lassen.

2.11 Einsatz unsicherer Protokolle

Die ICS-Komponenten kommunizieren untereinander über verschiedene Netzprotokolle und Standards. Neben Protokollen und Standards aus der Office-IT wie Ethernet, TCP/IP, WLAN oder GSM werden OT-spezifische Protokolle eingesetzt. Diese sind nicht immer unter dem Gesichtspunkt der Informationssicherheit entwickelt worden und bieten demgemäß teilweise keine oder nur eingeschränkte Sicherheitsmechanismen. Informationen werden häufig im Klartext und ohne Integritätssicherung oder Authentisierung übertragen.

Ein Angreifer mit Zugang zum Netz könnte die Inhalte der Kommunikation auslesen oder verändern und auf diese Weise die Prozesse beeinflussen, etwa indem Sensordaten vorgetäuscht oder Steuerungsbefehle gefälscht werden. Dies trifft in besonderem Maße auf Protokolle zu, die für die Kommunikation über frei zugängliche Gebiete eingesetzt werden, etwa bei Funkprotokollen oder im Rahmen der Standortvernetzung.

2.12 Unsichere Konfigurationen von ICS-Komponenten

In der Standardkonfiguration von ICS-Komponenten werden Sicherheitsmaßnahmen nicht immer aktiviert. Dadurch können Unbefugte leicht Zugriff erlangen. Der Betrieb unsicher konfigurierter Komponenten kann darüber hinaus auch die Sicherheit anderer Komponenten der Umgebung bedrohen, etwa wenn Zugangsdaten zu diesen ausgelesen werden können oder sie in einer Vertrauensstellung zu anderen Systemen stehen.

Beispielsweise könnten Standardpasswörter gebraucht, Klartextprotokolle zur Systemverwaltung genutzt, nicht erforderliche Dienste betrieben, ungesicherte Schnittstellen wie z. B. USB- oder Firewire-Ports verwendet oder Sicherheitsfunktionen deaktiviert werden.

2.13 Abhängigkeiten der OT von IT-Netzen

Die OT wird mittlerweile immer weniger völlig autark betrieben. Bestehen Abhängigkeiten zu anderen Systemen, Netzen oder Diensten, wirken sich Ausfälle oder Sicherheitsvorfälle im IT-Netz auch auf die OT aus.

Insbesondere wenn diese Systeme und Netze nicht unter der direkten Kontrolle des Betreibers stehen, kann die Verfügbarkeit der OT und seiner Prozesse stark beeinträchtigt werden. Darüber hinaus kann ein Vorfall oder Fehler in der Regel nur mit externer Unterstützung behoben werden.

Beispiele für Abhängigkeiten zu anderen Systemen und Netzen sind Internetanbindungen, gemeinsam genutzte Infrastrukturkomponenten, eine Betriebsführung und Überwachung durch Dienstleister oder die Nutzung von Cloud-Diensten.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins IND.1 *Prozessleit- und Automatisierungstechnik* aufgeführt. Grundsätzlich ist der ICS-Informationssicherheitsbeauftragte (ICS-ISB) für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeit	**Rolle**
Grundsätzlich zuständig	ICS-Informationssicherheitsbeauftragter

Weitere Zuständigkeiten	Mitarbeiter, Planer, IT-Betrieb, OT-Betrieb (Operational Technology, OT)

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein IND.1 *Prozessleit- und Automatisierungstechnik* vorrangig erfüllt werden:

IND.1.A1 Einbindung in die Sicherheitsorganisation (B)

Ein Managementsystem für Informationssicherheit (ISMS) für den Betrieb der OT-Infrastruktur MUSS entweder als selbständiges ISMS oder als Teil eines Gesamt-ISMS existieren.

Ein Gesamtverantwortlicher für die Informationssicherheit im OT-Bereich MUSS benannt werden. Er MUSS innerhalb der Institution bekannt gegeben werden.

IND.1.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

IND.1.A3 Schutz vor Schadprogrammen (B)

Beim Einsatz von Virenschutz-Software auf OT-Komponenten MUSS berücksichtigt werden, ob und in welcher Konfiguration der Betrieb von Virenschutz-Software vom Hersteller unterstützt wird. Ist dies nicht der Fall, MUSS der Bedarf an alternativen Schutzverfahren geprüft werden.

Die Virensignaturen DÜRFEN NICHT von OT-Systemen direkt aus dem Internet bezogen werden.

IND.1.A18 Protokollierung [OT-Betrieb (Operational Technology, OT)] (B)

Jede Änderung an ICS-Komponenten MUSS protokolliert werden. Außerdem MÜSSEN alle Zugriffe auf ICS-Komponeten protokolliert werden.

IND.1.A19 Erstellung von Datensicherungen [Mitarbeiter, OT-Betrieb (Operational Technology, OT)] (B)

Programme und Daten MÜSSEN regelmäßig gesichert werden. Auch nach jeder Systemänderung an OT-Komponenten MUSS eine Sicherung erstellt werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein IND.1 *Prozessleit- und Automatisierungstechnik*. Sie SOLLTEN grundsätzlich erfüllt werden.

IND.1.A4 Dokumentation der OT-Infrastruktur (S)

Alle sicherheitsrelevanten Parameter der OT-Infrastruktur SOLLTEN dokumentiert sein. In einem Bestandsverzeichnis SOLLTEN alle Software- und Systemkomponenten geführt werden. Hieraus SOLLTEN die eingesetzten Produkt- und Protokollversionen sowie die Zuständigkeiten hervorgehen. Zu den eingesetzten Komponenten SOLLTEN eventuelle Restriktionen der Hersteller oder regulatorische Auflagen bestimmt sein. Diese Dokumentation und ein Systeminventar SOLLTEN beispielsweise in einem Leitsystem geführt werden.

Zusätzlich SOLLTE ein aktueller Netzplan Zonen, Zonenübergänge (Conduits), eingesetzte Kommunikationsprotokolle und -verfahren sowie Außenschnittstellen dokumentieren. Bei den Schnittstellen SOLLTEN aktive Netzkomponenten und manuelle Datentransferverfahren, z. B. durch Wechseldatenträger, berücksichtigt werden. Zonen und Conduits schützen die OT-Infrastrukur, indem die Automatisierungslösung in Zellen und Kommunikationskanälen strukturiert werden SOLLTE.

IND.1.A5 Entwicklung eines geeigneten Zonenkonzepts [Planer] (S)

Die OT-Infrastruktur SOLLTE auch horizontal in unabhängige Funktionsbereiche, wie etwa Anlagen, segmentiert werden. Die einzelnen Zonen SOLLTEN, so weit wie möglich, im Betrieb voneinander

unabhängig sein. Insbesondere die Zonen, in denen der technische Prozess gesteuert wird, SOLLTEN bei einem Ausfall der anderen Zonen für einen gewissen Zeitraum weiter funktionstüchtig sein. Auch SOLLTE die Abkopplung nach einem Angriff weiter funktionieren. Dieser Zeitraum SOLLTE geeignet definiert und dokumentiert werden. Das Netz SOLLTE manipulations- und fehlerresistent konzipiert werden.

IND.1.A6 Änderungsmanagement im OT-Betrieb (S)

Für Änderungen an der OT SOLLTE ein eigener Änderungsprozess definiert, dokumentiert und gelebt werden.

IND.1.A7 Etablieren einer übergreifenden Berechtigungsverwaltung zwischen der OT und in der Office-IT (S)

Die Institution SOLLTE einen Prozess zur Verwaltung von Benutzerzugängen und zugeordneten Berechtigungen für den Zugriff auf die OT etablieren. Die Berechtigungsverwaltung SOLLTE den Prozess, die Durchführung und die Dokumentation für die Beantragung, Einrichtung und den Entzug von Berechtigungen umfassen.

Die Berechtigungsverwaltung SOLLTE gewährleisten, dass Berechtigungen nach dem Minimalprinzip vergeben und regelmäßig überprüft werden. In der Berechtigungsverwaltung SOLLTEN die Zugriffe auf IT-Systeme für Mitarbeiter, Administratoren und Dritte geregelt sein. Jeder Beteiligte SOLLTE regelmäßig zu den einzuhaltenden Regelungen sensibilisiert werden. Die Einhaltung SOLLTE überprüft werden. Fehlverhalten SOLLTE sanktioniert werden.

IND.1.A8 Sichere Administration [IT-Betrieb] (S)

Für die Erstkonfiguration, Verwaltung und Fernwartung in der OT SOLLTEN entweder sichere Protokolle oder abgetrennte Administrationsnetze mit entsprechendem Schutzbedarf genutzt werden. Der Zugang zu diesen Schnittstellen SOLLTE auf die Berechtigten eingeschränkt sein. Es SOLLTE nur der Zugriff auf die Systeme und Funktionen gewährt sein, die für die jeweilige Administrationsaufgabe benötigt werden.

Die Systeme und Kommunikationskanäle, mit denen die Administration oder Fernwartung durchgeführt wird, SOLLTEN das gleiche Schutzniveau aufweisen wie die verwaltete OT-Komponente.

IND.1.A9 Restriktiver Einsatz von Wechseldatenträgern und mobilen Endgeräten in ICS-Umgebungen (S)

Für die Nutzung von Wechseldatenträgern und mobilen Endgeräten SOLLTEN Regelungen aufgestellt und bekannt gegeben werden. Der Einsatz von Wechseldatenträgern und mobilen Endgeräten in ICS-Umgebungen SOLLTE beschränkt werden. Für Medien und Geräte von Dienstleistern SOLLTEN ein Genehmigungsprozess und eine Anforderungsliste existieren. Die Vorgaben SOLLTEN jedem Dienstleister bekannt sein und von diesen schriftlich bestätigt werden.

Auf den OT-Komponenten SOLLTEN alle nicht benötigten Schnittstellen deaktiviert werden. An den aktiven Schnittstellen SOLLTE die Nutzung auf bestimmte Geräte oder Medien eingeschränkt werden.

IND.1.A10 Monitoring, Protokollierung und Detektion [OT-Betrieb (Operational Technology, OT)] (S)

Betriebs- und sicherheitsrelevante Ereignisse SOLLTEN zeitnah identifiziert werden. Hierzu SOLLTE ein geeignetes Log- und Event-Management entwickelt und umgesetzt werden. Das Log- und Event-Management SOLLTE angemessene Maßnahmen umfassen, um sicherheitsrelevante Ereignisse zu erkennen und zu erheben. Es SOLLTE zudem einen Reaktionsplan (Security Incident Response) enthalten.

Der Reaktionsplan SOLLTE Verfahren zur Behandlung von Sicherheitsvorfällen festlegen. Darin abgedeckt sein SOLLTEN die Klassifizierung von Ereignissen, Meldewege und Festlegung der einzubeziehenden Organisationseinheiten, Reaktionspläne zur Schadensbegrenzung, Analyse und Wiederherstellung von Systemen und Diensten sowie die Dokumentation und Nachbereitung von

Vorfällen.

IND.1.A11 Sichere Beschaffung und Systementwicklung (S)

Sollen OT-Systeme beschafft, geplant oder entwickelt werden, SOLLTEN Regelungen zur Informationssicherheit getroffen und dokumentiert werden. Die Unterlagen SOLLTEN Teil der Ausschreibung sein.

Bei Beschaffungen, Planungen oder Entwicklungen SOLLTE die Informationssicherheit in dem gesamten Lebenszyklus berücksichtigt werden. Voraussetzungen und Umsetzungshinweise für einen sicheren Betrieb von ICS-Komponenten von Herstellern SOLLTEN frühzeitig eingeplant und umgesetzt werden. Für ICS-Komponenten SOLLTEN einheitliche und dem Schutzbedarf angemessene Anforderungen an die Informationssicherheit definiert werden. Diese SOLLTEN berücksichtigt werden, wenn neue ICS-Komponenten beschafft werden. Die Einhaltung und Umsetzung SOLLTE dokumentiert werden.

Die Institution SOLLTE dokumentieren, wie sich das System in die Konzepte für die Zoneneinteilung, das Berechtigungs- und Schwachstellen-Management sowie für den Virenschutz einfügt und diese gegebenenfalls anpassen. Es SOLLTE geregelt sein, wie der Betrieb aufrechterhalten werden kann, falls einer der Kooperationspartner keine Dienstleistungen mehr anbietet.

IND.1.A12 Etablieren eines Schwachstellen-Managements (S)

Für den sicheren Betrieb einer OT-Umgebung SOLLTE die Institution ein Schwachstellen-Management etablieren. Das Schwachstellen-Management SOLLTE Lücken in Software, Komponenten, Protokollen und Außenschnittstellen der Umgebung identifizieren. Außerdem SOLLTEN sich daraus erforderliche Handlungen ableiten, bewerten und umsetzen lassen.

Grundlage dafür SOLLTEN Schwachstellenmeldungen von Herstellern oder öffentlich verfügbare CERT-Meldungen sein. Ergänzend hierzu SOLLTEN organisatorische und technische Audits zur Schwachstellenanalyse durchgeführt werden.

IND.1.A20 Systemdokumentation [Mitarbeiter, OT-Betrieb (Operational Technology, OT)] (S)

Es SOLLTE eine erweiterte Systemdokumentation erstellt werden. Darin SOLLTEN Besonderheiten im Betrieb und die Möglichkeiten zur Systemverwaltung festgehalten werden. Außerdem SOLLTE dokumentiert werden, wenn ICS-Komponenten verändert werden.

IND.1.A21 Dokumentation der Kommunikationsbeziehungen [OT-Betrieb (Operational Technology, OT)] (S)

Es SOLLTE dokumentiert werden, mit welchen Systemen eine ICS-Kompnente welche Daten austauscht. Außerdem SOLLTEN die Kommunikationsverbindungen neu integrierter ICS-Komponenten dokumentiert werden.

IND.1.A22 Zentrale Systemprotokollierung und -überwachung [OT-Betrieb (Operational Technology, OT)] (S)

Die Protokollierungsdaten von ICS-Komponenten SOLLTEN zentral gespeichert werden. Bei sicherheitskritischen Ereignissen SOLLTE automatisch alarmiert werden.

IND.1.A23 Aussonderung von ICS-Komponenten [OT-Betrieb (Operational Technology, OT)] (S)

Wenn alte oder defekte ICS-Komponenten ausgesondert werden, SOLLTEN alle schützenswerten Daten sicher gelöscht werden. Es SOLLTE insbesondere sichergestellt sein, dass alle Zugangsdaten nachhaltig entfernt wurden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein IND.1 *Prozessleit- und Automatisierungstechnik* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende

Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

IND.1.A13 Notfallplanung für OT (H)

Notfallpläne für den Ausfall und für die Kompromittierung jeder Zone SOLLTEN definiert, dokumentiert, nach jeder größeren Änderung getestet und regelmäßig geübt sein.

Zudem SOLLTE ein wirksames Ersatzverfahren für den Ausfall der (Fern-) Administrationsmöglichkeit definiert, dokumentiert und getestet sein.

IND.1.A14 Starke Authentisierung an OT-Komponenten (H)

Zur sicheren Authentisierung von privilegierten Benutzern in Steuerungssystemen SOLLTE ein zentraler Verzeichnisdienst eingerichtet werden (siehe Baustein ORP.4 *Identitäts- und Berechtigungsmanagement*). Die Authentisierung SOLLTE durch den Einsatz mehrerer Faktoren wie Wissen, Besitz oder Biometrie zusätzlich abgesichert werden.

Bei der Planung SOLLTE darauf geachtet werden, dass daraus entstehende Abhängigkeiten in der Benutzerauthentisierung bekannt sind und bei der Umsetzung der Lösung berücksichtigt werden.

Es SOLLTE sichergestellt werden, dass die Authentisierung von betrieblich erforderlichen technischen Konten auch in Notfällen durchgeführt werden kann.

IND.1.A15 Überwachung von weitreichenden Berechtigungen (H)

Die Institution SOLLTE ein Bestandsverzeichnis führen, das alle vergebenen Zutritts-, Zugangs und Zugriffsrechte auf kritische Systeme enthält. Das Verzeichnis SOLLTE beinhalten, welche Rechte ein bestimmter Benutzer effektiv hat und wer an einem bestimmten System über welche Rechte verfügt.

Alle kritischen administrativen Tätigkeiten SOLLTEN protokolliert werden. Der IT-Betrieb SOLLTE NICHT die Protokolle löschen oder manipulieren können.

IND.1.A16 Stärkere Abschottung der Zonen (H)

Bei hoch schutzbedürftigen oder schlecht absicherbaren ICS-Umgebungen SOLLTEN vorbeugend Schnittstellensysteme mit Sicherheitsprüffunktionen eingesetzt werden.

Durch Realisierung einer oder mehrerer Anbindungszonen (DMZ) in P-A-P-Struktur SOLLTEN durchgängige Außenverbindungen terminiert werden. Erforderliche Sicherheitsprüfungen SOLLTEN so erfolgen, dass die ICS-Anlage nicht angepasst werden muss.

IND.1.A17 Regelmäßige Sicherheitsüberprüfung (H)

Die Sicherheitskonfiguration von OT-Komponenten SOLLTE regelmäßig und bedarfsorientiert bei plötzlich auftretenden neuen, bisher unbekannten Gefährdungen überprüft werden. Die Sicherheitsüberprüfung SOLLTE zumindest die exponierten Systeme mit Außenschnittstellen oder Benutzerinteraktion umfassen. Auch das realisierte Sicherheitskonzept SOLLTE regelmäßig überprüft werden. Die Sicherheitsüberprüfung SOLLTE als Konfigurationsprüfung oder auch durch automatisierte Konformitätsprüfungen erfolgen.

IND.1.A24 Kommunikation im Störfall [Mitarbeiter, OT-Betrieb (Operational Technology, OT)] (H)

Alternative und unabhängige Kommunikationsmöglichkeiten SOLLTEN aufgebaut und betrieben werden.

4 Weiterführende Informationen

4.1 Wissenswertes

Das BSI hat mit dem Dokument „Empfehlungen für Fortbildungs- und Qualifizierungsmaßnahmen im ICS-Umfeld“ entsprechende Hilfestellungen zur Absicherung im ICS-Umfeld veröffentlicht.

Mit dem „ICS Security Kompendium“ gibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) Hilfestellungen für den Test der Komponenten und Maßnahmen für die IT-Sicherheit in ICS für Hersteller und Integratoren von ICS.

Die International Organization for Standardization (ISO) macht 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 Oesterreichs E-Wirtschaft bietet mit dem Dokument „Whitepaper: Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“ eine Hilfestellung zum sicheren Betrieb von Steuerungs- und Telekommunikationssystemen.

Die internationale Norm 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, legt fest, was zur Einrichtung von IT-Sicherheit in Netzen und Systemen notwendig ist.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein IND.1 *Prozessleit- und Automatisierungstechnik* von Bedeutung.

G 0.5 Naturkatastrophen

G 0.6 Katastrophen im Umfeld

G 0.9 Ausfall oder Störung von Kommunikationsnetzen

G 0.11 Ausfall oder Störung von Dienstleistern

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.36 Identitätsdiebstahl

G 0.37 Abstreiten von Handlungen

G 0.39	Schadprogramme
G 0.41	Sabotage
G 0.42	Social Engineering
G 0.46	Integritätsverlust schützenswerter Informationen
G 0.17	Verlust von Geräten, Datenträgern oder Dokumenten
G 0.22	Manipulation von Informationen
G 0.25	Ausfall von Geräten oder Systemen