Handbuch Grundschutz für «Operational Technology» in der Stromversorgung

OT_SCTY, Ausgabe Juli 2018

Verband Schweizerischer Elektrizitätsunternehmen
Association des entreprises électriques suisses
Associazione delle aziende elettriche svizzere

Telefon +41 62 825 25 25, Fax +41 62 825 25 26, info@strom.ch, www.strom.ch

Impressum und Kontakt

Herausgeber
Verband Schweizerischer Elektrizitätsunternehmen VSE
Hintere Bahnhofstrasse 10, Postfach
CH-5001 Aarau
Telefon +41 62 825 25 25
Fax +41 62 825 25 26
info@strom.ch
www.strom.ch

Autoren der Erstausgabe

Reto Amsler	Swissgrid AG	Autor
Mattia Bardelli	AET	Autor
Reto Bondolfi	EWZ	Autor
Daniel Caduff	BWL	Autor
Beate Fiedler	Alpiq Power AG	Autor
Olivier Hauert	Alpiq Power AG	Autor
Hendrik la Roi	VSE	Sekretär
Stefan Mattmann	CKW AG	Autor
Michele Paganini	Repower AG	Autor
Markus Rauber	BKW Energie AG	Autor
Daniel Rudin	MELANI	Autor
Daniel Schirato	Axpo WZ-Systems AG	Projektleitung
Wolfgang Sutter	KWO	Autor
Peter Waldegger	Axpo Power AG	Projektleitung

Verantwortung Kommission
Für die Pflege und die Weiterentwicklung des Dokuments zeichnet die VSE-Kommission EVU-TSO verantwortlich.

Chronologie

September 2016	Arbeitsaufnahme AG ICT-Security für kritische Infrastrukturen
Dezember 2017	Fertigstellung des Dokumentes
März/April 2018	Vernehmlassung in der Branche
11. Juni 2018	Genehmigung durch die Geschäftsleitung des VSE

Das Dokument wurde unter Einbezug und Mithilfe von VSE und Branchenvertretern erarbeitet.

Druckschrift Nr. 1047/d, Ausgabe 2018

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Vorwort

Beim vorliegenden Dokument handelt es sich um ein Branchendokument des VSE. Es ist Teil eines umfassenden Regelwerkes für die Elektrizitätsversorgung im offenen Strommarkt. Branchendokumente beinhalten branchenweit anerkannte Richtlinien und Empfehlungen zur Nutzung der Strommärkte und der Organisation des Energiegeschäftes und erfüllen damit die Vorgabe des Stromversorgungsgesetzes (StromVG) sowie der Stromversorgungsverordnung (StromVV) an die Energieversorgungsunternehmen (EVU).

Branchendokumente werden von Branchenexperten im Sinne des Subsidiaritätsprinzips ausgearbeitet, regelmässig aktualisiert und erweitert. Bei den Bestimmungen, welche als Richtlinien im Sinne des StromVV gelten, handelt es sich um Selbstregulierungsnormen. Die Branchendokumente sind grundsätzlich für diejenigen Beteiligten verbindlich, welche die Branchendokumente als Bestandteil eines konkreten Vertrags erklärt haben.

Die Dokumente sind hierarchisch in vier unterschiedliche Stufen gegliedert

- Grundsatzdokument: Marktmodell Elektrische Energie (MMEE)
- Schlüsseldokumente
- Umsetzungsdokumente
- Werkzeuge / Handbuch

Beim vorliegenden Dokument «Grundschutz für Operational Technology in der Stromversorgung» handelt es sich um ein Werkzeug / Handbuch.

Dokumentstruktur

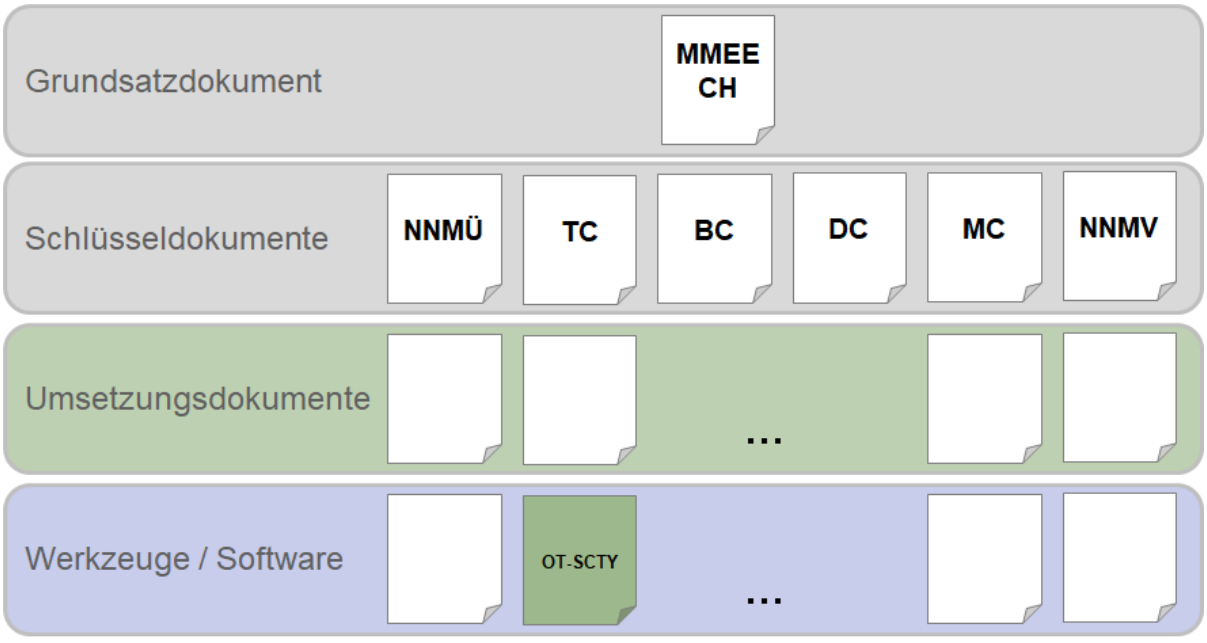

Abbildung 1 Dokumentstruktur

Haftungsausschluss

Das vorliegende Dokument mit Empfehlungen zur Verbesserung der Sicherheit von industriellen Steuerungssystemen mit der Defense-in-Depth Strategie, wurde von den beteiligten Personen und Stellen nach bestem Wissen und Gewissen erstellt. Alle Angaben erfolgen ohne Gewähr auf Vollständigkeit oder Richtigkeit. Weder der VSE noch die beteiligten Bundesstellen übernehmen eine Haftung für Schäden, die durch die Verwendung von Informationen aus diesem Dokument oder durch das Fehlen von Informationen entstehen.

Zusammenfassung

Automatisierung hat in kommerziellen und in industriellen Umgebungen lange unabhängig voneinander stattgefunden. Die Standardisierung (z.B. X86 basierte Geräte) und Vernetzung (z.B. Internet) in der Wirtschaftsinformatik haben in den letzten Jahren jedoch zunehmend auch Einzug in die Industrieinformatik gehalten. Damit werden aber industrielle Systeme auch denselben "Cyber-Bedrohungen" ausgesetzt, wie sie in der Wirtschaftsinformatik hinlänglich bekannt sind.

Industrielle Steuerungssysteme (ICS) bilden heutzutage einen integralen Bestandteil kritischer Infrastrukturen wie Strom, Öl und Gas, Wasser, Transport, Produktion und Chemie und erleichtern deren Betrieb. Die zunehmende Frage der Cybersecurity und ihre Auswirkungen auf das ICS heben grundlegende Risiken für die kritische Infrastruktur einer Nation hervor. Eine effiziente Bewältigung der ICS-Cybersicherheitsprobleme erfordert ein klares Verständnis der aktuellen Sicherheitsherausforderungen und spezifischer defensiver Gegenmassnahmen.

Das vorliegende Dokument adressiert Verteilnetzbetreiber der Netzebenen 1 bis 4 und Energieerzeugungsanlagen (Produzenten) und stellt eine Empfehlung dar, wie die Cyber-Risiken in der kritischen Infrastruktur der Stromversorgung auf ein akzeptables Mass reduziert werden können. Kern der Empfehlung ist die Implementierung einer sogenannten „Defense-in-Depth“-Strategie, welche heutzutage als die anerkannte defensive Strategie gegenüber Cyber-Bedrohungen gilt. Die Strategie basiert auf dem militärischen Prinzip, dass es für einen Feind schwieriger ist, ein komplexes und vielschichtiges Abwehrsystem zu überwinden als eine einzige Barriere. Die Strategie beinhaltet Informations- und Kommunikations-Technologien (IKT), welche durch den Menschen in effektiven und effizienten Prozessen eingesetzt werden sollen. Zum anderen verweist dieses Handbuch auf verschiedene Hilfsmittel und bietet insbesondere ein Framework mit einem begleitenden Excel Tool, das Unternehmen erlaubt, die eigenen Fähigkeiten zu erfassen, zu beurteilen und zu vergleichen sowie gezielt weiterzuentwickeln.

Dieses Handbuch wendet sich an Personen, die in der Gesamtverantwortung der Informatik Sicherheit beziehungsweise der Sicherheit von Prozess- und Netzleitsystemen der Energieversorgung stehen. Dies können Chief Information Officer (CIO), Chief Information Security Officer (CISO), Security Manager, Projektleiter oder Berater in IKT Sicherheit mit Führungsverantwortung sein. Aber auch Experten und Spezialisten in Cybersecurity finden hier wertvolle Informationen in der branchenspezifischen Anwendung von IKT Security Standards und Richtlinien. In kleineren Energieversorgungsunternehmen sind hier sicher auch Chief Operating Officer (COO) und jene Leute angesprochen, die die Gesamtverantwortung über den Betrieb der Energieversorgung haben, der ja zunehmend durch Informatikmittel überhaupt ermöglicht wird.

Mit der vorliegenden, ersten Version wird das Rüstzeug geliefert, um einen konkreten Grundschutz in der Operational Technology der Stromversorgung gewährleisten zu können. Der Umsetzungsgrad obliegt jedem Netzbetreiber der Netzebenen 1 bis 4 resp. den Betreibern der Energieerzeugungsanlagen. In einem zweiten Schritt soll auf Basis der gemachten Erfahrungen im Rahmen einer überarbeiteten Version auch ein Mindeststandard festgelegt werden.

Im ersten Abschnitt wird eine detaillierte Einführung in die Defense-in-Depth Strategie gegeben, wobei speziell auf IKT und OT Problemstellungen aus der Strom- und Energiebranche eingegangen wird. Wer sich noch nicht so gut in Cybersecurity auskennt oder wer eine Auffrischung oder Erneuerung auf den letzten Stand braucht, findet in diesem Abschnitt wertvolle Informationen. Der Abschnitt kann auch zum Nachschlagen herbeigezogen werden.

Im zweiten Abschnitt werden konkrete Massnahmen und Hilfsmittel eingeführt, deren Umsetzung empfohlen wird. Basierend auf dem US amerikanischen Framework for Improving Critical Infrastructure Cybersecurity, welches im Minimalstandard zur Stärkung der ICT-Resilienz durch das Eidgenössische Bundesamt für Wirtschaftliche Landesversorgung auch in Deutsch vorliegt, wird ein konkretes Hilfsmittel zur Anwendung durch Strom- und Energieversorgungsunternehmen empfohlen, welches einem kleinsten gemeinsamen Nenner in der aktiven Cyber-Verteidigung entsprechen dürfte.

Die gesetzlichen Grundlagen in Bezug auf Data Privacy werden in dieser Empfehlung explizit nicht behandelt.

Hintergrund und Überblick

(1) In den letzten 15 Jahren hat es in der Energietechnik eine starke Verlagerung zu IT- bzw. ICT-Systemen gegeben. Dieser technologische Wandel ermöglicht das zentrale Steuern und Regeln von Echtzeitinformationen. Dadurch wird man in der Netzbetriebsführung viel agiler und kann auf zeitnahe, kritische Ereignisse viel schneller und automatisiert reagieren. Doch dieser Wandel hin zur Informationstechnologie bringt auch neue Risiken mit sich, welche die Energieunternehmen anerkennen, bewerten und behandeln müssen, um den gesetzlichen Auftrag gemäss Stromversorgungsgesetz, Stromversorgungsverordnung oder dem Energiegesetz erfüllen zu können.

(2) Das Bundesamt für wirtschaftliche Landesversorgung BWL hat eine Risiko- und Verwundbarkeitsanalyse des Teilsektors Stromversorgung durchgeführt und folgende Erkenntnisse zusammengetragen:

- Entlang der gesamten Versorgungskette ist die Produktion von Strom in den Kraft- und Unterwerken heute weniger stark verwundbar hinsichtlich ICT-Gefährdungen als der Betrieb der Verteil- und Übertragungsnetze.
- Kraft- und Unterwerke können theoretisch auch immer noch vor Ort bedient werden. Bei einem grossflächigen Ausfall wären die Energieversorgungsunternehmen aber kaum noch in der Lage, alle kritischen Anlagen schnell genug mit ausreichend Personal besetzen zu können.
- Betrifft die Gefährdung die ICT-Dienstleister der Energieversorgungsunternehmen, so wäre die Kommunikation zwischen den Anlagen und den Leitstellen unter Umständen nur noch über Notkommunikationssysteme aufrechtzuerhalten.
- Der Betrieb der Leitungsnetze erfolgt heute dezentral und wird weitgehend durch digitale Systeme überwacht und teilweise gesteuert. Der Betrieb der Netze ist deswegen stärker verwundbar gegenüber ICT-Gefährdungen als die eigentliche Stromproduktion. In diesem Bereich sind die SCADA-Systeme von besonderer Bedeutung.
- Die Gefährdung durch Mitarbeitende, welche absichtliche oder unabsichtliche Fehlmanipulationen an den SCADA-Systemen vornehmen, ist somit ebenfalls signifikant und nimmt durch den Zentralisierungsprozess bei den Leitstellen weiter zu.
- Mit dem Einbau von „Smart Metern“ und „Smart Grid“-Geräten wird das Schweizer Leitungsnetz zu einem Verbund aus einer Vielzahl kleiner Computer. Dies bietet Vorteile in der Effizienz für den Betrieb der Leitungsnetze, schafft aber neue ICT-Verwundbarkeiten.
- Insgesamt wird die ICT-Verwundbarkeit der Stromversorgung in Zukunft weiter zunehmen.

(3) Mit Ausnahme der Kernenergieanlagen, welche bereits heute weitreichenden regulatorischen Vorschriften des Eidgenössischen Nuklearinspektorats ENSI unterliegen, bestehen zum heutigen Zeitpunkt keine (rechtlich) verbindlichen Minimalvorgaben zur ICT-Sicherheit im Bereich der Stromversorgung.

(4) Das neue Landesversorgungsgesetz, welches per 01.06.2017 in Kraft getreten ist, gibt dem Bundesamt für wirtschaftliche Landesversorgung neu jedoch auch die Kompetenz, subsidiär präventive Massnahmen zur Sicherstellung der Energieversorgung umzusetzen.

(5) Der hier vorliegende ICT-Minimalstandard ist eine solche präventive Massnahme im Sinne des Landesversorgungsgesetzes. Gemäss dem Subsidiaritätsprinzip wurde der ICT-Minimalstandard als Branchendokument abgefasst.

1. Ausgangslage und Zielsetzung

(1) Dieses Handbuch verfolgt den Ansatz einer Defense-in-Depth Strategie, welche vollumfänglich die Risiken im Bereich ICT-Security adressiert. Ziel ist es, mit diesem Dokument den ICT-Verantwortlichen der Schweizer EVU ein Werkzeug zur Verfügung stellen, um die Informatiksicherheit in ihren Unternehmen zu evaluieren, zu beurteilen und zu verbessern. Damit soll die Resilienz der Schweizer EVU gegenüber ICT-Risiken verbessert und dadurch insgesamt die Versorgungssicherheit erhöht werden.

(2) Im ersten Schritt wird die Defense-in-Depth Strategie ausführlich beschrieben, und es werden konkrete Massnahmen mit Beispielen aus der Praxis gegeben, deren Umsetzung empfohlen wird. Im zweiten Schritt wird das US amerikanische NIST *Framework for Improving Critical Infrastructure Cybersecurity* vorgestellt. Es wird empfohlen, dieses Framework als Hilfsmittel einzusetzen, um in einem Self-Assessment die eigene Maturität bezüglich Resilienz gegenüber Cyber-Bedrohungen zu bestimmen. Es ist zudem empfohlen, darauf aufbauend die eigenen Kapazitäten und Fähigkeiten kontinuierlich weiterzuentwickeln.

(3) „ICT-Risiken“ werden umfassend verstanden. Dieses Dokument adressiert ICT-Risiken aller Art von physischem Zugriffsschutz über Schutz vor Datenverlust- und Manipulation bis hin zum Schutz vor Cyber-Angriffen in zerstörerischer Absicht. Insbesondere werden jedoch die Risiken adressiert, welche durch die Verwundbarkeitsanalyse im Rahmen der nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken identifiziert wurden.

1.1 Ziele und Grundsätze

(1) Dieses Handbuch hat den Anspruch, als Leitfaden zu dienen, um eine Defense-in-Depth-Securitystrategie aufzubauen, umzusetzen und betreiben zu können. Der Defense-in-Depth-Ansatz garantiert einen holistischen Approach, um die Sicherheitsrisiken im Bereich der kritischen Informations- und Kommunikationssysteme ganzheitlich identifizieren und behandeln zu können. Dies umfasst neben technischen Massnahmen auch die dazu benötigten Prozesse, Ausbildung und Schulung der Mitarbeitenden sowie die benötigte Security-Governance, um die Strategie erfolgreich umzusetzen und betreiben zu können.

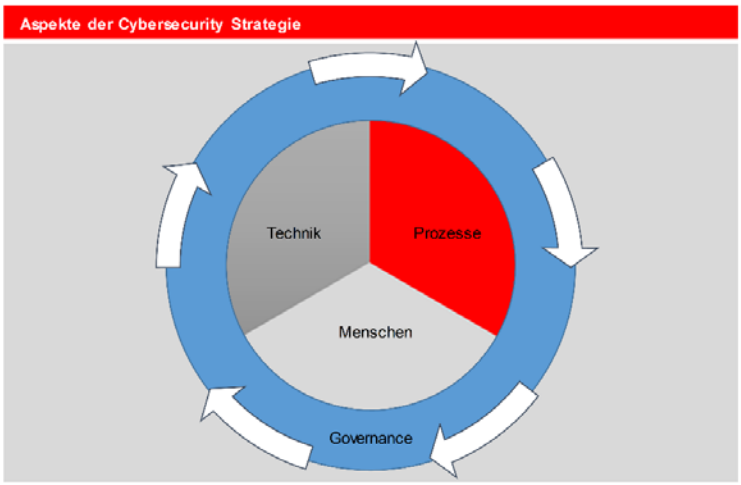

Abbildung 2 Aspekte der Cybersecurity Strategie

(2) Ziel der Defense-in-Depth-Strategie ist es, eine bedarfsgerechte Informationssicherheit für kritische Energiesysteme gewährleisten zu können. Dabei steht die rechtzeitige, korrekte und sichere Zurverfügungstellung aller für die Erfüllung eines sicheren Netzbetriebs notwendigen Informationen an den berechtigten Personenkreis im Fokus. Folgende Kriterien stellen die Grundbausteine der gängigen Sicherheitskonzepte, wie z.B. Defense-in–Depth-Konzepts dar:

- Verfügbarkeit
  Gewährleisten, dass Informationssysteme und die sich darauf befindlichen Informationen sowie die für den Transport benötigten Ressourcen zum Zeitpunkt des Bedarfs verfügbar sind.
- Integrität
  Gewährleisten, dass Informationen jederzeit vollständig, richtig und zuverlässig sind sowie ein unerlaubtes Abändern beziehungsweise Zerstören verhindert wird.
- Vertraulichkeit
  Gewährleisten, dass Informationen ausschliesslich berechtigten Personen beziehungsweise Systemen zugänglich sind.

1.2 Abgrenzungen

(1) Dieses Handbuch fokussiert nur auf jene Business-Prozesse, welche einen direkten Einfluss auf die sichere Regelung und Steuerung der Energienetze haben. Weitere Aspekte der Sicherheit im Bereich Energie, wie zum Beispiel Smart-Meters oder Smart-Grid, sind nicht im Scope dieses Dokuments. Folgende Definitionen und Abgrenzungspunkte definieren den Umfang dieses Handbuchs:

- ICT-Security für kritische Infrastrukturen schliesst alle ICT-Assets ein, welche für einen sicheren und integren Netzbetrieb notwendig sind.
- Die Sicherheit der Office-IT und Wirtschaftsinformatik steht nicht im Fokus des Dokuments. Jedoch werden Anforderungen an die Schnittstellen und den Informationsaustausch zu den Zonen, welche die kritischen ICT-Assets enthalten, gestellt.
- Die elektrische und betriebliche Sicherheit der Betriebsmittel des Hochspannungsnetzes ist nicht Bestandteil dieses Handbuchs.
- Massnahmen zur Arbeitssicherheit sind nicht Bestandteil dieses Handbuchs. Diesbezüglich gelten die Bestimmungen der Starkstromverordnung.
- Die Empfehlung hat Energieversorgungsunternehmen der Netzebenen 1-4 im Hauptfokus.
- Es soll ein branchenweiter Grundschutz implementiert werden, welcher als Basis für ein erhöhtes Sicherheitsniveau dient. Das angestrebte Sicherheitsniveau soll verhindern, dass pro Sicherheitsvorfall nie eine Energiemenge von 50 MWh[1] oder mehr nicht zeitgerecht geliefert werden kann.
- Die Netzebenen 5-7 sind insofern betroffen, als dass dort sichergestellt werden muss, dass diese nicht Ursache für Störungen auf den höheren Netzebenen sind. Dabei müssen insbesondere die vernetzten Leitsysteme berücksichtigt werden.

[1] siehe Branchenempfehlung ICT-Continuity Paragraph 4.2 für die Definition eines relevanten Ereignises (Krise).

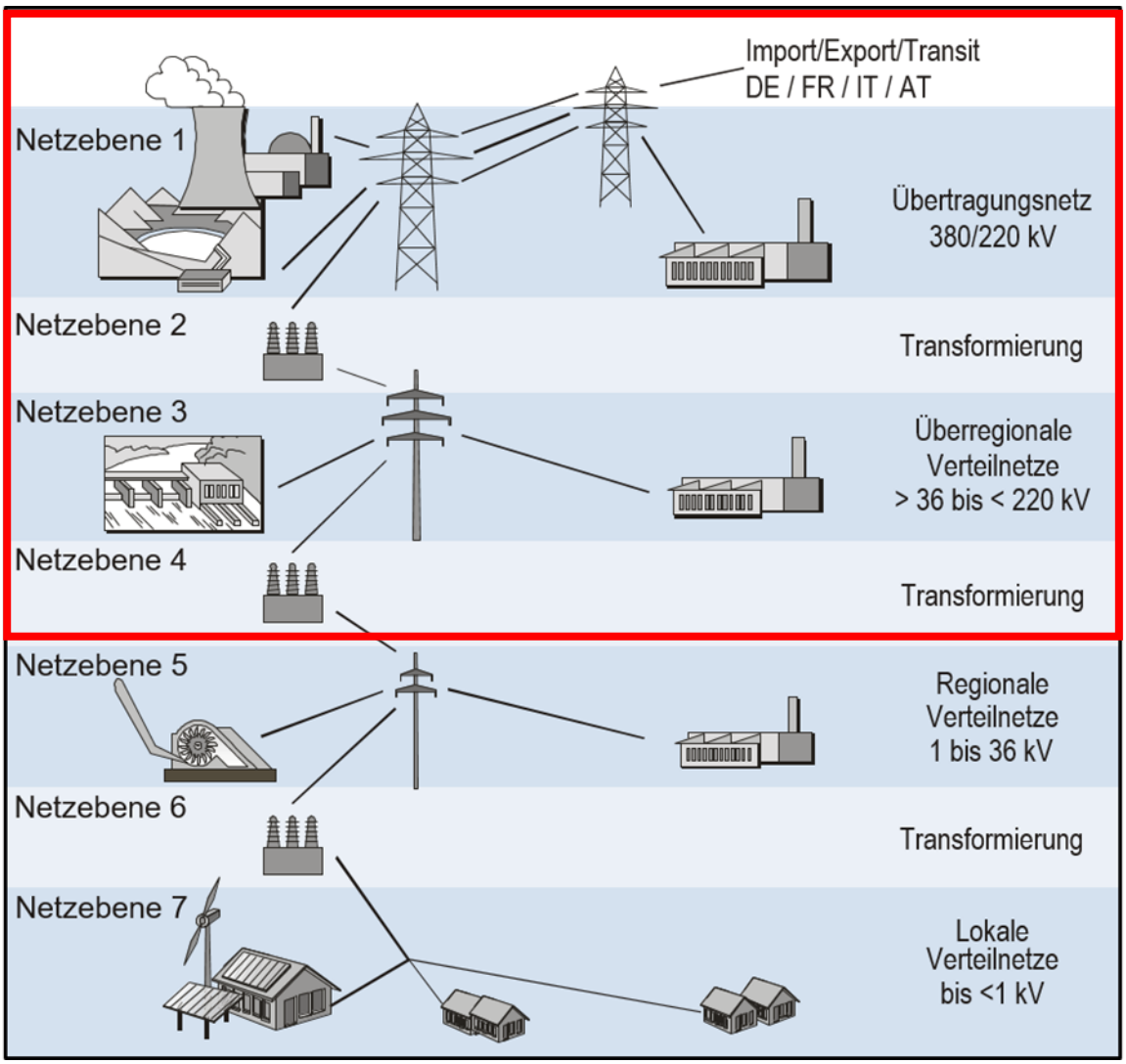

Abbildung 3 Hauptfokus des Handbuchs – Netzebenen 1 bis 4

1.3 Einführung in die Defense-in-Depth-Strategie

(1) Der Begriff "Defense-in-Depth" stammt aus dem Verteidigungsdenken vieler Kulturen und militärischer Strategien: "Hindere einen Angreifer mit möglichst vielen Verteidigungslinien!".

(2) Daten-, Informations- und operationelle Sicherheit werden dabei umfassend und in der Tiefe betrachtet. In der kommerziellen IKT ist dieses Konzept seit Jahren ein Defacto-Standard, und angepasst an die Prozessleittechnik kann es auch im industriellen Umfeld angewendet werden.

(3) ICT-Sicherheit in der industriellen Wirtschaft, d.h. in der "Operational IT (OT)" oder "Prozess IT (PI)", unterscheidet sich jedoch in bestimmter Hinsicht etwas von der kaufmännischen ICT-Sicherheit:

(4) Jede Sicherheitsstrategie einer Organisation muss die Werte schützen, die für die Organisation erfolgskritisch sind. Diese Werte sind von Unternehmen zu Unternehmen und auch von Industriesektor zu Industriesektor verschieden. Im kommerziellen Sektor ist ICT-Sicherheit primär auf Vertraulichkeit

gerichtet, im industriellen Sektor jedoch mehr auf "Leben, Leib und Umwelt" und somit auf die korrekte Verfügbarkeit der ICT.

(5) Defense-in-Depth, d.h. Aneinanderreihung von Verteidigungslinien, beinhaltet auch Überwachung, Erkennung und Reaktion auf bestimmte Ereignisse. Ein Cyber-Angriff kann nicht verhindert werden - deshalb ist das Ziel die rasche Erkennung, Isolierung, Abwehr und Verringerung von Folgen einer Verletzung (Resilienz).

(6) Defense-in-Depth ist ein Konzept; einzelne Technologien und einzelne Software-Applikationen sind wichtig und Mittel zum Zweck. Ein "umfassender Ansatz in der Tiefe" beinhaltet alle Ressourcen und deren Zusammenwirken zur Bereitstellung von effektiven Verteidigungslinien zum Schutz, zur Überwachung und zur Reaktion gegen Cyber-Bedrohungen.

(7) Folgende Hauptdomänen eines Defense-in-Depth-Konzeptes sind anzugehen:

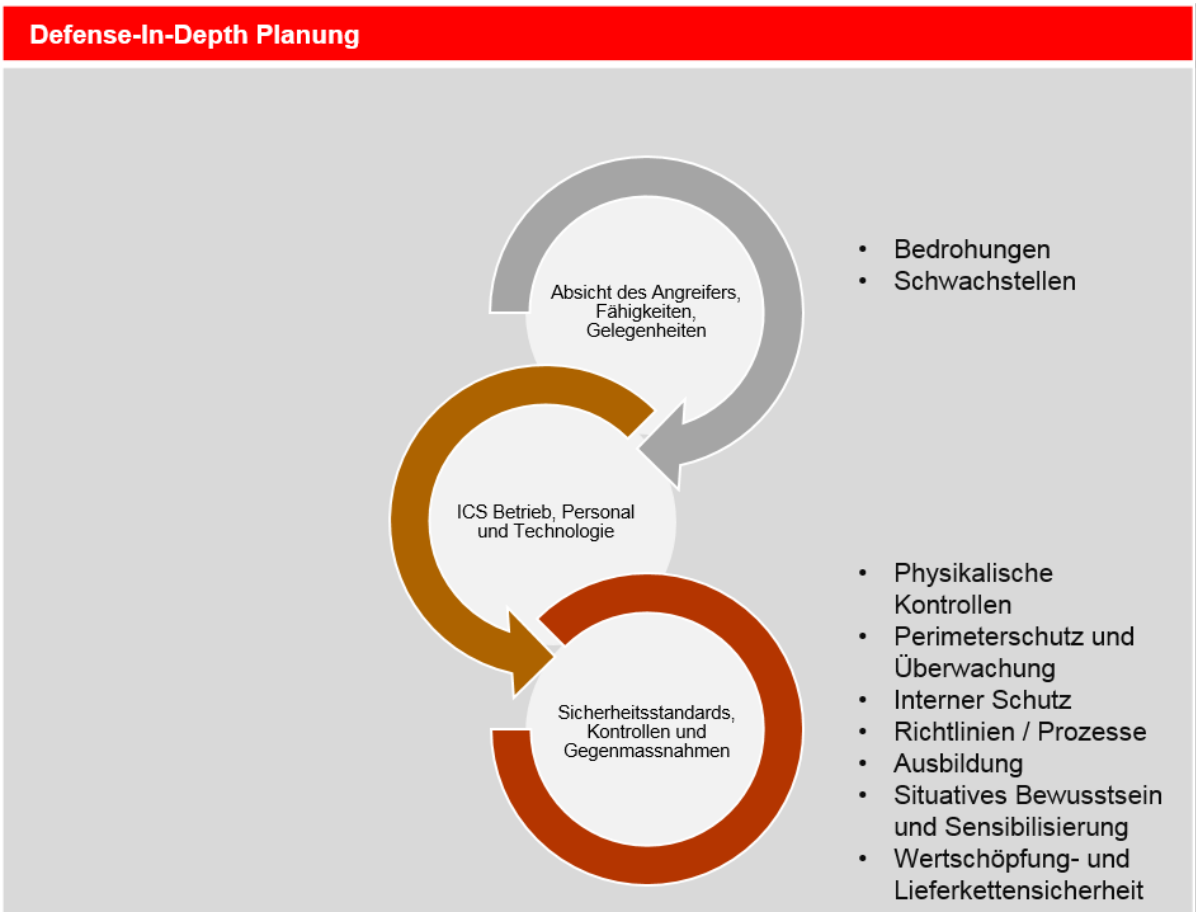

Abbildung 4 Defense-In-Depth-Planung

(8) Bezüglich der Implementierung von Defense-in-Depth-Konzepten bestehen wichtige Unterschiede zwischen dem traditionellen IT-Umfeld und einem ICS. Die untenstehende Tabelle gibt eine Übersicht über die wichtigsten Unterschiede.

Sicherheitsthema	Business-IT (IT)	Operational Technology (OT)
Kritische Daten / Information	Geschäftsdaten (inkl. Finanzdaten) Personendaten	Leitsystemdaten (Steuersignale) Sensordaten („smart meter data“)
Integrität	Kontextuell kritisch.	Kritisch (mögliche Auswirkung auf Leben, Leib und Umwelt)
Verfügbarkeit	i.d.R. während Bürozeiten	Hoch, real-time (365 Tage x 24h)
Vertraulichkeit	Finanz- und Personendaten hoch	Wenig kritisch
Technologie-Lebensdauer	2-3 Jahre; viele Anbieter; allgegenwärtige Erweiterungen	10-20 Jahre; normalerweise der gleiche Verkäufer über Zeit; Produkt-End-of-Life schafft neue Sicherheitsbedenken
Änderungsmanagement	Regelmässig und geplant; mit Mindestnutzungszeiten abgestimmt	Strategische Planung; nicht trivialer Prozess aufgrund von Auswirkungen auf die Produktion
Patch-Verwaltung	Leicht zu definieren; unternehmensweit; remote und automatisiert	Langer Zeitraum bis zur erfolgreichen Patchinstallation; OEM-spezifisch; kann ICS-Funktionalität beeinträchtigen; um ein akzeptables Risiko zu erreichen, müssen Verantwortlichkeiten klar definiert werden
Anti-Virus	Weit verbreitet; leicht implementiert und aktualisiert. Benutzer haben die Kontrolle über Anpassungen und können pro Applikation oder pro Unternehmen definiert werden.	Resourcen-Bedarf kann sich auf ICS auswirken; erfordert in der Regel "Ausschluss"-Ordner, damit Programme ohne Intervention der Viren-Software (in Quarantäne) nicht beeinträchtigen werden.
Test- und Auditverfahren	Verwendung moderner Methoden; Systeme in der Regel elastisch und robust gegenüber Bewertungsmethoden	Tests sind systemspezifisch angepasst; moderne Methoden können unangemessen sein; Gerät kann während Tests anfällig auf Störungen reagieren
Anlagenklassifizierung	Üblich und jährlich durchgeführt; Ergebnisse treiben die Ausgaben	Nur durchgeführt, wenn verpflichtet; kaum Bestände für aussergewöhnliche Anlagen; Entkopplung zwischen Anlagenwert und Gegenmassnahmen
Incident Response und Forensik	Leicht entwickelt und eingesetzt; einige regulatorische Anforderungen; eingebettet in Technologie	Fokussiert auf Aktivitäten zur Systemwiederaufnahme; Forensik-Verfahren neben Ereignisreproduktion unreif; erfordert gute IT- / ICS-Beziehungen
Physische- und Umweltsicherheit	Reicht von schlecht (Büro-Systeme) bis hervorragend (kritische IT-Systeme)	In der Regel hervorragend für kritische Bereiche; variable Reife basierend auf Kritikalität / Kultur
Sichere Systementwicklung	Integraler Bestandteil des Entwicklungsprozesses	Historisch kein integraler Bestandteil des Entwicklungsprozesses; Anbieter entwickeln sich, aber langsamer als IT; Kern-ICS-Lösungen schwierig nachrüstbar mit Sicherheit

Sicherheitsthema	Business-IT (IT)	Operational Technology (OT)
Regulierung	Je nach Sektor und Land unterschiedlich stark ausgeprägt (z.B. Finanz- und Pharmasektor)	Zunehmend, je nach Land (starke Regulierung z.B. US NERC, Deutschland EnWG).

Tabelle 1 Unterschiede zwischen Defense-In-Depth Konzepten für Wirtschaftsinformatik und ICS

(9) Defense-in-Depth-Strategien, die auf Steuersystemen angewendet werden, sind auch abhängig von weiteren Geschäftsrealitäten wie:

- Die Kosten für die Sicherung von Alt-Systemen,
- Der zunehmende Trend, Leitsysteme mit Geschäftsnetzwerken zu verbinden,
- Die Fähigkeit, den Zugriff auf Business- und ICS-Assets für Remotebenutzer zu ermöglichen,
- Supply Chain Vertrauensprobleme,
- Der Stand der Technik hinsichtlich der Fähigkeit, ICS-spezifische Protokolle zu überwachen und zu sichern, und
- Die Fähigkeit, zeitaktuelle Wahrnehmung neuer Bedrohungen für ICS aufrechtzuerhalten.

(10) Defense-in-Depth ist nicht ein fassbarer Gegenstand oder ein Softwarepaket, sondern eine Kombination von Mensch, Technologie, Prozessen und Kenntnissen über mögliche Aggressoren. Denken und handeln löst Probleme, und Technologie ermöglicht die Lösung von Problemen durch die Bereitstellung einer Reihe von Werkzeugen, die das Risiko reduzieren können. Die beste Technologie wird nicht verhindern, dass Menschen Fehler machen - ob vorsätzlich oder unbeabsichtigt. Organisationen müssen Sicherheits-Gegenmassnahmen ständig anpassen und verfeinern, um sich vor bekannten und neuen Bedrohungen zu schützen.

(11) Die Anwendung mehrerer Verteidigungslinien in ICS-Umgebungen verbessert die Sicherheit durch die Erhöhung der "Kosten" eines Angriffs, während die Wahrscheinlichkeit der Erkennung und die Fähigkeit zur Verteidigung gegen einen Angreifer verbessert wird. Sicherheits-Gegenmassnahmen, die auf bewährten Verfahren und Standards basieren, schützen die ICS-kritischen Ressourcen durch mehrere Schichten von Abwehrkräften und verbessern so den Schutz von Betrieb, Personal und Technologie.

(12) Das Endziel ist, einen Angreifer in der lateralen Bewegung durch Netzwerke und Systeme zu behindern und ihn zu höheren Investitionen und Kosten zu zwingen. Die Verwendung mehrerer Ebenen hilft, direkte Angriffe auf kritische Systeme zu mindern, die Aufklärungsaktivitäten auf ICS-Netzwerke und -systeme zu erschweren und gleichzeitig natürliche Bereiche für die Einführung von Intrusion-Detection-Technologien bereitzustellen.

(13) In diesem Abschnitt werden, wie in Tabelle 2 dargelegt, einige der verfügbaren und empfohlenen Lösungen und Strategien für die Defense-in-Depth-Security erörtert. Unternehmen sollten diese Lösungen und Strategien in Kombination verwenden, um Verteidigungslinien zu schaffen, die die ursprüngliche ICS-Funktionalität gewährleisten und einen robustesten Schutz für kritische Vermögenswerte bieten.

Abbildung 5 Koordinierter Einsatz mehrerer Sicherheitsmassnahmen

2. ICS Defense-In-Depth-Strategien

(1) Eine erfolgreiche Strategie zur Cybersecurity schützt die Mittel einer Organisation, die zur Ausführung der kritischen Geschäftsprozesse notwendig sind. Dabei gibt es keine allgemein gültige Definition der Anforderungen oder allgemein gültige Lösungen. Stattdessen ist Cybersecurity als stetiger Prozess zu verstehen, der einen mehrschichtigen Ansatz verlangt. Dieser mehrschichtige Ansatz ist in der Fachliteratur als Defense-in-Depth-Strategie bekannt.

(2) Defense-in-Depth-Strategien sind in jedem Fall individuell und müssen sich an den Bedürfnissen, Möglichkeiten und Risiken der betroffenen Organisation orientieren. Der Ansatz ist dabei immer risikobasiert und berücksichtigt neben den eigenen kritischen Mitteln auch Interdependenzen und Abhängigkeiten von externen Prozessen oder Ressourcen.

(3) Eine Defense-in-Depth-Strategie akzeptiert, dass es keinen vollständigen Schutz gegen jegliche Art von Cyber-Bedrohungen geben kann. Stattdessen ist man sich der eigenen Verwundbarkeit bewusst und entwickelt Strategien und Massnahmen, um die eigene Exposition gegenüber Cyber-Risiken zu identifizieren (IDENTIFY), sich dagegen bestmöglich zu schützen (PROTECT), Verletzungen der Cybersecurity zu detektieren (DETECT), darauf zu reagieren (RESPOND) und schnellstmöglich wieder den Normalzustand zu erreichen (RECOVER).

(4) Um eine Defense-in-Depth-Strategie für industrielle Kontrollsysteme (ICS)[2] zu implementieren, muss eine Organisation die Gesamtheit aus (möglichen) Verwundbarkeiten und Bedrohungen kennen, welche die Daten, Prozesse und Anlagen gefährden, die zusammen das ICS bilden.

2.1 ICT-Security-Governance

(1) Die Security-Governance legt die Grundsteine für eine erfolgreiche und nachhaltige Umsetzung der Defense-in-Depth-Strategie. In diesem Bereich werden die Voraussetzungen geschaffen, dass Bedrohungen für die Prozessleittechnik erkannt, bewertet und behandelt werden. Die Governance liefert dabei eine übergeordnete Struktur, um die Geschäftsziele bezüglich ICT-Security auf strategischer, funktionaler und operativer Ebene zu unterstützen. Das Governance Model beschreibt das,

- "was wird getan"
- "wie wird es getan"
- "wer ist verantwortlich"
- „wie soll gemessen werden"

(2) Die Governance definiert die Regeln, Prozesse, Metriken und organisatorischen Strukturen, die für eine effektive Planung und Steuerung erforderlich sind, um die Geschäftsanforderungen und -ziele des Unternehmens zu erreichen. Diese sollen in einem Strategiedokument festgehalten und durch die Geschäftsleitung freigegeben und im Unternehmen kommuniziert werden. Des Weiteren soll ein Geschäftsleitungsmitglied bestimmt werden, welches zuständig ist für die Informationssicherheit und die nötige Managementunterstützung bei der Erarbeitung und Umsetzung der Defense-in-Depth-

[2] Es existieren in der Fachwelt unterschiedliche Begriffe, die alle plus/minus dasselbe meinen: Industrial Control Systems (ICS), Supervisory Control and Data-Acquisition (SCADA) oder Operational Technology (OT).

Strategie sicherstellt. Die Geschäftsleitung soll durch die Sicherheitsorganisation regelmässig über die Sicherheitsmaturität, Sicherheitsvorfälle und definierte Sicherheit-KPI's informiert werden.

(3) Entscheidend dabei ist, dass hierbei eine uneingeschränkte Unterstützung des höheren Managements vorliegt und somit auch die Aufwände, Prozesse und benötigten Ressourcen für eine erfolgreiche Umsetzung gesprochen werden.

2.2 Organisation und Verantwortlichkeiten

(1) Ein Hauptaspekt der Security-Governance ist eine im Unternehmen etablierte Sicherheitsorganisation, welche klare Aufgaben, Verantwortungen und Kompetenzen hat. Sie ist verantwortlich für die Definition der Defence-in-Depth-Strategie, für deren Umsetzung und Weiterentwicklung. Dabei kommt einem aktiven Risikomanagement eine zentrale Bedeutung zu, um mögliche Bedrohungen für die ICT-Security erkennen und mit Hilfe von Massnahmen behandeln zu können. Die Sicherheitsorganisation muss durch die Geschäftsleitung befähigt und die benötigten Ressourcen zugestellt bekommen um ihre Aufgaben effizient und umfassend wahrnehmen zu können. Wichtig ist dabei, dass die Sicherheitsorganisation fest in dem Unternehmen verankert und akzeptiert ist. Die Rollen und Funktionen innerhalb der Sicherheitsorganisation müssen beschrieben und ausgewiesen, sowie mit klaren Kompetenzen ausgestattet werden. Es müssen Schnittstellen zu anderen (sicherheitsrelevanten) Organisationen innerhalb des Unternehmens definiert und festgehalten, sowie mögliche Kompetenzüberschneidungen geklärt werden.

(2) Ist die Sicherheitsorganisation durch die Geschäftsleitung befähigt worden, kann sie ihre Kernaufgaben uneingeschränkt in enger Zusammenarbeit mit den Unternehmensbereichen umsetzen. Insbesondere gehören dazu folgende Aufgabenschwerpunkte:

- Stellt die Fachführung der Informationssicherheit in Bezug auf OT sicher und legt die Prioritäten der Tätigkeiten der Lage angepasst fest
- Stellt sicher, dass alle notwendigen Sicherheitsdokumente, Weisungen und Richtlinien erarbeitet, wenn nötig aktualisiert und konsequent umgesetzt werden
- Stellt sicher, dass neue, relevante Sicherheits-Themen identifiziert, analysiert und falls notwendig bearbeitet werden
- Stellt sicher, dass entsprechend Know-how und Ressourcen im gesamten Sicherheitsmanagement zur Verfügung stehen
- Stellt sicher, dass periodische Überprüfungen, Audits und Penetration Tests durchgeführt werden
- Stellt sicher, dass die Berichterstattung Richtung Geschäftsleitung inhaltlich korrekt, termin-, stufengerecht und systematisch erfolgt
- Stellt sicher, dass der Sicherheitsprozess mit dem Unternehmens Risiko Management Prozess verzahnt, methodisch integriert ist, sowie die Vorgaben aus dem Risiko Management Prozess berücksichtigt werden

2.2.1 Weisungen und Richtlinien

(1) Im Bereich Informationssicherheit muss das Unternehmen wie in anderen Bereichen auch, eine strategische Richtung einschlagen. Wo will das Unternehmen in 3-5 Jahren bezüglich Informationssicherheit stehen? Was ist der Risikoappetit bezüglich Informationssicherheit? Welche Ressourcen und finanzielle Mittel sollen bezüglich Informationssicherheit investiert werden?

(2) Die Antworten zu diesen strategischen Fragen sollen in einer unternehmensweiten Sicherheitspolitik behandelt und beantwortet werden. Die Sicherheitspolitik ist durch die Geschäftsleitung zu erlassen und in Kraft zu setzen. Folgende strategische Inhalte sollten durch eine Sicherheitspolitik definiert werden und somit Ankerpunkt für jegliche Tätigkeiten und Vorgaben im Bereich Informationssicherheit sein:

- Zweck und Geltungsbereich der Sicherheitspolitik
- Sicherheitsziele
- Sicherheitsgrundsätze
- Risikoappetit
- Zusammenarbeit mit Branche und Behörden
- Anwenden von Sicherheitsstandards
- Berücksichtigung der Wirtschaftlichkeit
- Sicherheitskultur
- Ausnahmen von Sicherheitsvorgaben
- Sicherheit in Projekten
- Sicherheitsorganisation mit Rollen und Funktionen

(3) Nebst der Sicherheitspolitik, welche das Dach der Informationssicherheit bildet, benötigt es je nach Grösse und Struktur des Unternehmens weitere Dokumente mit Weisungscharakter. Folgende Grafik dient als Beispiel wie die Dokumentenhierarchie für die Informationssicherheit in einem Unternehmen aussehen könnte.

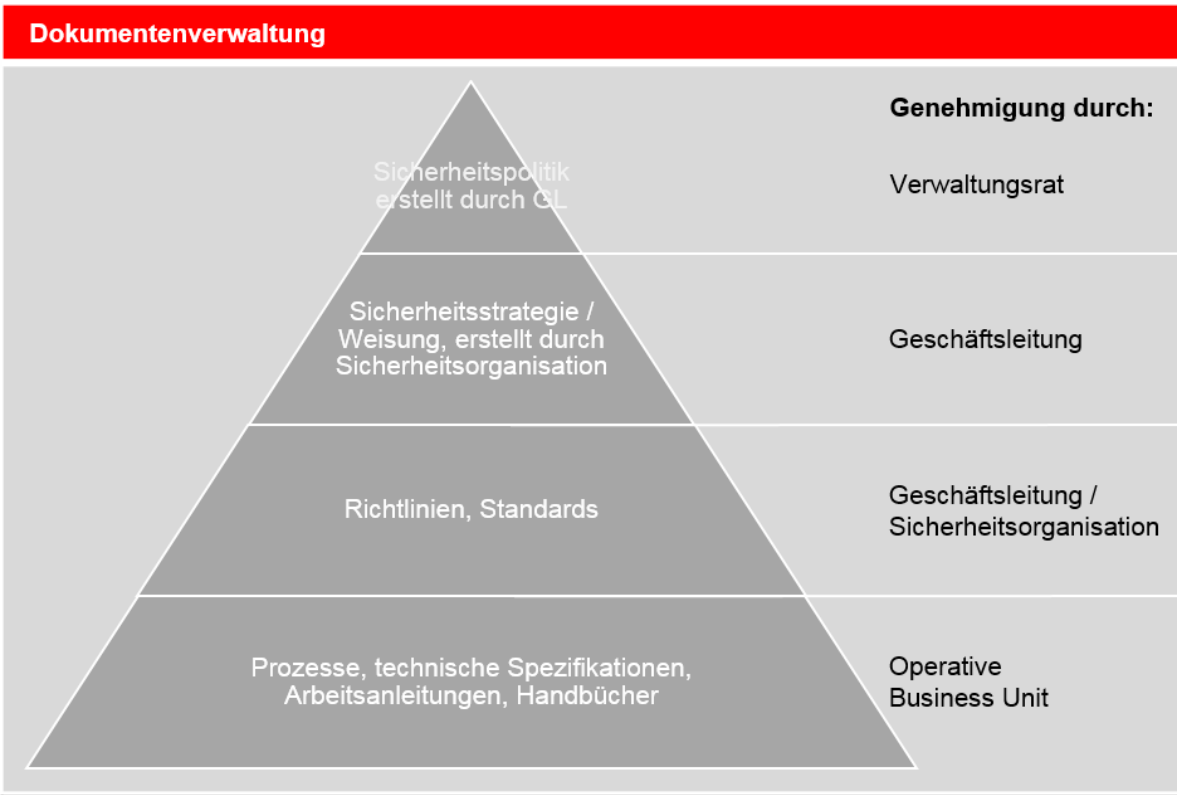

Abbildung 6 Dokumentenhierarchie

(4) Wichtig ist ein firmenweites Regelwerk zu schaffen, welches definiert wie Weisungen und Richtlinien ins Unternehmen eingeführt werden (Owner, Freigabe, Bekanntmachung und Schulung, wiederkehrende Prüfung auf Aktualität) und welche Weisungen oder Richtlinien auch für externe Partner und Dienstleister Gültigkeit haben oder speziell definiert werden müssen.

2.2.2 Prozesse und Prozeduren - Change Management

(1) Eine Organisation besteht aus Personen, Prozessen und Technologien. Die Art und Weise, wie diese entwickelt und organisiert sind, macht den Unterschied von Unternehmen zu Unternehmen aus. Jedes Unternehmen wird durch das Personal, deren Kenntnis, durch Aufgaben, Funktionen und Rollen sowie technische Hilfsmittel definiert. So ist auch jede IT-Organisation in ein Rahmenwerk von IT-Prozessen eingebettet, ob diese nun dokumentiert sind oder bloss praktiziert werden. Die Absicht definierter Abläufe und Prozesse ist Transparenz und Kontrolle und letztlich das Erreichen der Ziele. Im Idealfall sind administrative Richtlinien, Prozesse und Verfahren für die Aufgaben und Tätigkeiten implementiert, die für das Erreichen der Ziele relevant und dienlich sind.

(2) Ein IT-Prozess-Framework dient der Umsetzung des IT-Strategieplanes und muss entsprechend definiert, umgesetzt und von Zeit zu Zeit angepasst werden. Dieses Rahmenwerk umfasst typischerweise eine IT-Prozesslandschaft mit Prozessen, die in Beziehungen miteinander stehen. Einzelne Prozesse verfügen über definierte Abläufe und Verantwortlichkeiten; erstrebte Reifegrade können gemessen werden und dienen der kontinuierlichen Verbesserung. Die IT-Prozesslandschaft sollte sich in die unternehmensweite Prozesslandschaft einfügen und Spezifika für IT definieren, wenn diese von Geschäftsprozessen abweichen. Insgesamt dient ein solches Prozess-Framework der Standardisierung von Abläufen und soll so zu grösserer Effektivität und Effizienz beitragen. ITIL (IT Infrastructure Library) oder COBIT (Control Objectives for IT) sind zwei bekannte Standard IT-Prozess-Rahmenwerke. Change Management ist ein zentraler Prozess in beiden dieser IT-Prozess-Rahmenwerke und dient hier der Veranschaulichung.

Change Management

(3) Change Management ist für die Erhaltung der Integrität von Prozessleitsystemen von grösster Bedeutung. „Ungepatchte“ Software stellt eine der grössten Schwachstellen für ein System dar. Software-Updates auf IT-Systemen, insbesondere Sicherheits-Patches, werden in der Regel rechtzeitig auf Grundlage geeigneter Sicherheitsrichtlinien und -verfahren angewendet. Darüber hinaus werden diese Verfahren oft mit Server-basierten Tools automatisiert. Software-Updates auf ICS können nicht immer rechtzeitig umgesetzt werden. Bevor sie implementiert werden, müssen diese Updates vom Anbieter industrieller Steuerungsanwendungen und dem Endbenutzer der Anwendung gründlich getestet und zur Installation freigegeben werden. Darüber hinaus muss der ICS-Betreiber notwendige Wartungsarbeiten Tage oder gar Wochen im Voraus planen. Ein weiteres Problem ist, dass viele ICS ältere Versionen von Betriebssystemen nutzen, die vom Betriebssystemhersteller nicht mehr unterstützt werden. Folglich können vorhandene Patches nicht nachgeführt werden. Change Management ist auch auf Hardware und Firmware anwendbar. Der Change Management Prozess, angewendet auf ICS, erfordert eine sorgfältige Beurteilung durch die Hersteller und die Betreiber, wobei System-, Netz- und Sicherheitsspezialisten beider Lager eng zusammenarbeiten müssen. Typisch zwingende Charakteristiken in einem Change Management-Prozess beinhalten:

- Definierter Change Prozess, idealerweise schriftlich dokumentiert, damit Änderungen überall wiederholt kontrolliert ablaufen

- Technische und organisatorische Trennung zwischen Entwicklung, Test und Produktion; Schnitt und Verantwortlichkeiten definiert zwischen Herstellung/Entwicklung und Betrieb
- Definition eines Freigabeverfahrens: Aufgabentrennung, 4-Augen-Prinzip, Segregation; Definition von Kriterien und Verantwortungsträgern; Gateway zur Freigabe
- Nachvollziehbarkeit und Reproduzierbarkeit: Dokumentation des Changes und der Konfigurationsdatenbank, Aufzeichnung, Protokollierung, Logging
- Verantwortlichkeiten, Kriterien und Rückführungsmöglichkeit bei Fehlern (Rollback, Fallback)
- Finale Akzeptanz der Endbenutzer (User Acceptance Testing).

2.2.3 Incident Management - CERT (Computer Emergency Response Team)

(1) Der Energiesektor wird immer stärker durch IT Komponenten unterstützt. Dies geschieht innerhalb der Organisation, von administrativen Tätigkeiten über Berechnungsmodelle für den Stromfluss, bis hin zu den Schaltelementen in einem Unterwerk. Obwohl sich die Vernetzung noch nicht komplett durchgesetzt hat, wird diese über kurz oder lang unumgänglich sein. Bereits heute werden in der Regel Schaltungen in den Unterwerken nicht mehr lokal durchgeführt, sondern zentral von einem Kontrollzentrum aus. Nebst den Schaltungen kann die Zentrale ein Unterwerk komplett per Fernzugriff überwachen und in Echtzeit Messwerte der Stromflüsse ablesen.

(2) Ebenso führt die lokale Stromproduktion von Fotovoltaik- und Windanlagen zu einer immer stärkeren Vernetzung. Da hierdurch jeder Betreiber einer entsprechenden Anlage an das Netz eines Stromproduzenten angeschlossen werden kann, entsteht ein landesweites Energie-Netzwerk von erheblicher Komplexität. Ebenfalls sind diese Produzenten durch Business-Prozesse und Schnittstellen miteinander verbunden.

(3) Die rasche Integration der schnelllebigen Computer-Technologien führt zu einer Kollision zweier Welten. Da viele der Komponenten mit dem Fokus auf eine möglichst hohe Langlebigkeit gebaut wurden, sind einige der SCADA Elemente zu einer Zeit gebaut worden als der Fokus der Hersteller noch nicht auf Cybersecurity lag. Ebenso wurden die meisten Fachkräfte nicht mit einem entsprechenden Fokus auf die heutigen Risiken ausgebildet. Dies führt zu der Herausforderung, immer neuere Sicherheitskonzepte und Technologien in ein mehr oder weniger statisches Umfeld zu integrieren.

SOC / CERT

(4) Ein vielversprechendes Konzept für die Erhöhung der operativen Sicherheit ist die Einführung und der Betrieb von einem SOC bzw. CERT. Das Unternehmen muss festlegen ob und welchen Service (SOC/CERT) es aufbauen will. Dabei gilt es auch die Frage zu beantworten, ob das Unternehmen die Funktionen selber betreiben kann oder diese extern als Managed Service beziehen will.

(5) CERT oder CSIRT kümmern sich in der Regel wie der Name sagt „bloss“ um „Computer Emergency“ bzw. „Computer Security Incident Responses“. Ein SOC (Security Operation Center) ist ein Operation Center, welches sich zusätzlich zum Betrieb der Infrastruktur (Server, Datacenter, Netzwerke) auch um die Security und Incident Response Prozesse kümmert. Die Organisation und Aufbau eines SOC richtet sich hierbei stark nach ähnlichen Operation Centers, wie zum Beispiel dem Network Operation Center. Es hat sich über die Zeit ein breites Spektrum entwickelt, wie in der IT entsprechende Operation Center aufgebaut und geführt werden können. Dies kann von einem NASA Mission Control ähnlichem Raum bis zu einer Tisch-Insel innerhalb einer IT-Abteilung hinreichen. Alternativ zum Betrieb innerhalb einer Firma haben sich Managed Security Services Provider, kurz MSSP, etabliert, welche den Betrieb eins SOC als ausgelagerte Dienstleistung erbringen.

(6) Ziel eines SOC ist, die Informationssicherheit einer Organisation zu gewährleisten und sich den wandelnden Anforderungen neuer Bedrohungen anzupassen. Durch den Betrieb können zum Teil gesetzliche sowie Compliance Anforderungen erfüllt werden. Zum Erbringen dieser Leistungen verfügt das SOC über spezialisierte Fachkräfte wie auch entsprechend etablierte Prozesse und Tools.

(7) Die durch ein SOC erbrachten Dienstleistungen können sich von SOC zu SOC unterscheiden. Um die Informationssicherheit der Organisation zu gewährleisten, müssen die benötigten Dienstleistungen auf die spezifische Organisation angepasst werden. Die Dienstleistungen werden dem Kerngeschäft, dessen Infrastruktur und seinen Prozessen entsprechend angepasst.

Security Monitoring

(8) Analysten überwachen kontinuierlich Cybersecurity-Events. Diese Events werden durch Monitoring-**Tools** wie zum Beispiel einem SIEM, IDS oder ähnlichen Tools generiert. Zusätzlich werden via E-Mails oder Ticketing-Systemen gemeldete Incidents überwacht. Aus den Events generierte Alarme werden durch Analysten bearbeiten, hierfür werden Prozesse des Incident-Managements implementiert.

Security Management

(9) Die durch das SOC erbrachten Dienstleistungen, werden auf Effektivität hin überwacht und kontinuierlich weiterentwickelt. Neue SOC-Dienstleistungen in anderen Bereichen des Unternehmens werden durch das Security Services Management implementiert.

Security Services Engineering

(10) Hierdurch wird Consulting und Engineering Support für Informationssicherheit-Tools und -Projekten erbracht. Tools und Plattformen, welche von dem SOC selbst benötigt werden, werden hierdurch ebenfalls eingeführt und weiterentwickelt.

Security Services Operations

(11) Anders als die Engineering Dienstleistung, fokussiert sich die Operation Dienstleistungen auf den stabilen Betrieb der Sicherheits-Plattformen und -Tools. Konfigurationsänderungen an den Systemen werden im Rahmen dieser Dienstleistung erbracht.

Security Incident Investigation and Response

(12) Security Events und Incidents werden den etablierten Prozessen entsprechend behandelt. In der Regel ist diese Dienstleistung eng mit dem Security Monitoring gekoppelt. Events werden analysiert und angemessene Massnahmen werden getroffen. Ebenfalls wird die Eskalation und weitere Unterstützung bei der Behebung des Events durch diese Dienstleistung erbracht. Die hier durchgeführten Tätigkeiten werden oft auch als Incident Management aus dem ITIL Umfeld bezeichnet.

Security Log Management

(13) Ebenfalls eng mit dem Security Monitoring verbunden ist das Security Log Management. Ziel ist es relevante Log Daten zu sammeln, normalisieren, parsen und speichern. Log Daten von Netzwerk-, Sicherheits- und Hostsystemen sowie den einzelnen Applikationen werden gesammelt. Ebenfalls fällt das Evaluieren und Integrieren neuer Log-Quellen in diese Dienstleistung. Diese Dienstleistung wird in der Regel mithilfe von automatischen Scanning-Tools erbracht.

Vulnerability Discovery

(14) Fokus bei dieser Dienstleistung liegt beim Finden von Vulnerabilities (Schwachstellen). Es ist vom Vulnerability Management zu unterscheiden, da dieses in der Regel ein Prozess ausserhalb des SOC

ist, bei welchem ebenfalls die Behebung der gefundenen Vulnerabilities integriert ist. Bei den gefundenen Vulnerabilities kann es sich um schlecht konfigurierte Systeme, Hardware- oder Softwarelücken, oder Prozesslücken handeln.

Threat and Vulnerability Intelligence

(15) Daten von unterschiedlichen Quellen werden gesammelt, um ein Bild der aktuellen Bedrohungslage zu erstellen. Bei den Quellen handelt es sich um interne wie auch externe Quellen zu aktuellen Threats und Vulnerabilities. Es können automatische Feeds dieser Quelle eingerichtet werden, jedoch müssen die gesammelten Daten manuell analysiert und auf deren Relevanz hin bewertet werden.

Security Analytics and Reporting

(16) Gewonnene Informationen von den erbrachten Dienstleistungen werden gesammelt und aufbereitet, zum Beispiel durch die Visualisierung in Reports. Gewonnene Informationen durch diese Reports können wiederum in die erbrachten Dienstleistungen einfliessen um deren Qualität und Effektivität zu verbessern.

Breach Discovery

(17) Hinweise auf aktuelle oder vergangene Sicherheitsverstösse werden analysiert. Dies kann durch digitale Forensik, Erkennung von Anomalien und retrospektive Analysen erbracht werden. Diese Dienstleistung ist eng mit Security Incident Investigation and Response verknüpft. Der Fokus liegt auf der vertieften Analyse der IT-Systeme um eventuelle kompromittierte Systeme zu finden und deren Auswirkungen zu bewerten.

(18) Nebst den oben beschriebenen Dienstleistungen lassen sich innerhalb eines SOC ebenfalls die folgenden klassischen ITIL Prozesse finden:

- Event Management
- Incident Management
- Problem Management

(19) Während ein SOC sich mehrheitlich um den Betrieb und Incident Response im kleineren Rahmen kümmert, ist ein CERT (Computer Emergency Response Team) übergeordnet organisiert. Um die Sicherheit zu erhöhen, werden die Computer- und Netzwerksicherheit analysiert. Zu den erbrachten Dienstleistungen gehört das Publizieren von Warnungen und Alarmmeldungen, Vernetzung von Organisationen, vertiefte Analysen wie auch Incident Response. Oft bieten CERTs ihre Dienstleistungen nicht nur der eigenen Firma an, sondern es gibt einen Kreis von Kunden mit gemeinsamen Interessen und Voraussetzungen (z.B. für den Energiesektor). Der Energiesektor zeigt einen klaren Bedarf nach einer zentralen Organisation, welche vertieftes Fachwissen zu Verfügung stellen und bei der Koordination sowie der Behebung von Vorfällen Unterstützung leisten kann.

(20) Die von einem CERT erbrachten Dienstleistungen können grob in folgende Kategorien eingeteilt werden:

- Proaktive Dienstleistungen
- Reaktive Dienstleistungen
- Security Quality Management Dienstleistungen

(21) Nachfolgend werden die zuvor genannten Kategorien beschrieben:

Proaktive Dienstleistungen

(22) Diese Dienstleistungen haben zum Ziel die Cybersecurity-Incidents zu verringern und verhindern. Dies wird durch die laufende Optimierung der Sicherheitsinfrastruktur sowie durch den Austausch von Informationen erreicht.

Reaktive Dienstleistungen

(23) Diese dienen der Unterstützung nach einem aufgetretenen Cybersecurity-Incident. Diese können je nach Kunde variieren. Diese können im Auftrag eines Kunden durchgeführt werden, oder gehören zu den im Mandat des CERT aufgeführten Verantwortlichkeiten.

Security Quality Management Dienstleistungen

(24) Nebst technischen Dienstleistungen im direkten Bezug zu Vorfällen, können auch Dienstleistungen erbracht werden, welche das Ziel haben die allgemeine Sicherheit einer Organisation zu erhöhen.

Reaktive Dienstleistungen	Proaktive Dienstleistungen	Sicherheitsqualität Management-Dienstleistungen
Alarme und Warnungen Bewältigung von Störfällen - Störfallanalysen - Störfallbewältigung vor Ort - Support bei der Störfallbewältigung - Koordination der Störfallbewältigung Schwachstellenbearbeitung - Schwachstellenanalyse - Schwachstellenbewältigung Koordination der Schwachstellenbewältigung	Ankündigungen Technologieüberwachung Sicherheits-Audits oder Assessments Konfiguration und Unterhalt von Sicherheitstools, Applikationen und Infrastrukturen Entwicklung von Sicherheitstools Intrusion Detektion Service Verbreitung sicherheitsrelevanter Informationen	Risikoanalyse Business Continuity and Disaster Recovery planning Sicherheitsberatung Bewusstseinsbildung Bildung/Schulung Produktbewertung oder Produktzertifizierung

Tabelle 2 Mögliche Dienstleistungen eines CERT

Alarme und Warnungen

(25) Verbreiten von Informationen über Angriffe, Eindringlinge, Sicherheitslücken, Einbruchsalarme, Computer Viren oder auch Falschmeldungen. Ebenso Hinweise bezüglich möglichen kurzfristigen Mitigationsmassnahmen. Die Alarme und Warnungen werden reaktiv auf einen Vorfall kommuniziert.

Störfallanalysen

(26) Für Störfallanalysen gibt es verschiedene Levels und unterschiedliche Teildienstleistungen. Grundsätzlich wird unter Störfallanalyse das Auswerten aller vorhandenen Information eines Vorfalls verstanden. Ziel ist es den Bereich des Vorfalls einzugrenzen, den verursachten Schaden zu beurteilen sowie die möglichen Bewältigungsstrategien aufzuzeigen. Teil der Analyse ist ebenfalls die Korrelation von verschiedenen Informationen wie zum Beispiel Trends, Signaturen und Aktivitäten.

Störfallbewältigung vor Ort

(27) Es wird Unterstützung beim Beheben von Vorfällen vor Ort angeboten. Betroffene Systeme und Infrastruktur werden direkt durch das Team selbst analysiert. Massnahmen zur Behebung und Sicherung werden direkt durch das Team ergriffen.

Support bei der Störfallbewältigung

(28) Anstelle von dem direkten Beheben von Störfälle vor Ort, bietet das Team lediglich Unterstützung beim Beheben von Vorfällen, meist über Fernzugriff. Im Vergleich zur Störfallbewältigung vor Ort besteht keine direkte Interaktion mit den betroffenen Systemen.

Koordination der Störfallbewältigung

(29) Bei Vorfällen, welche mehrere Organisationen betreffen, übernimmt das CERT die Koordination der Massnahmen. Nebst der Zusammenarbeit mit den Opfern einer Attacke, kann dies ebenfalls die Zusammenarbeit mit Strafverfolgungsbehörden oder anderen Behörden beinhalten. Zu den Aufgaben innerhalb dieser Dienstleistung gehören das Sammeln von Statistiken, Informieren von potenziell involvierte Organisationen, austauschen von Informationen und durchführen von Analysen.

Schwachstellenanalyse

(30) Technische Analysen und Untersuchungen zu Schwachstellen in Hardware und Software. Dies beinhaltet ebenfalls das Bestätigen von möglichen Schwachstellen und der Analyse wie diese ausgenutzt werden können.

Schwachstellenbewältigung

(31) Zu bereits bekannten Schwachstellen werden mögliche Mitigationsmassnahmen analysiert. Die gefundenen Massnahmen werden mit den Partnern und Kunden kommuniziert.

Koordination der Schwachstellenbewältigung

(32) Das CERT informiert Partner sowie Kunden über Schwachstellen, deren Risiko sowie Mitigationsmassnahmen. Getroffene Massnahmen können durch das CERT verifiziert werden. Zu den Tätigkeiten dieser Dienstleistung gehört die Kommunikation mit Herstellern, Kunden, Partnern aber auch Spezialisten in den jeweiligen Bereichen. Ebenfalls werden Reports erstellt und das Veröffentlichen von Patches wird koordiniert.

Ankündigungen

(33) Ankündigungen beinhalten Alarme, Warnungen von Schwachstellen, Advisories usw. Ebenso informieren diese Ankündigungen über mittel- bis langfristige Auswirkungen von neuen Schwachstellen oder Bedrohungen.

Technologieüberwachung

(34) Das CERT überwacht neue technologische Entwicklungen, die aktuelle Bedrohungslandschaft sowie Trends. Themen können ebenfalls rechtliche und politische Aspekte sein. Hierfür werden Mailing-Listen, Websites, Artikel und Zeitungen beobachtet. Als Resultat dieser Arbeiten können Announcements, Guidelines oder Empfehlungen entstehen.

Sicherheits-Audits oder Assessments

(35) Durch Audits und Assessments wird die Infrastruktur von Kunden auf die Erfüllung von Vorgaben oder Standards überprüft. Nebst der Analyse von technischen Systemen kann dies ebenfalls die Analyse von Prozessen beinhalten.

Konfiguration und Unterhalt von Sicherheitstools, Applikationen und Infrastrukturen

(36) Durch diese Dienstleistung wird Unterstützung bei der Konfiguration und dem Betrieb von Sicherheitstools, Applikationen und der Infrastruktur angeboten. Nebst der Unterstützung kann es sich hierbei auch um den direkten Betrieb der Infrastruktur handeln.

Entwicklung von Sicherheitstools

(37) Das CERT entwickelt für seine Kunden spezifische Sicherheitstools. Die Tools entsprechen den individuellen Anforderungen und Bedürfnissen des Kunden oder auch einer Gruppe von Kunden. Ebenfalls kann es sich um Erweiterungen von bestehenden Tools handeln.

Intrusion Detektion Service

(38) Das CERT analysiert die IDS Meldungen und ergreift entsprechende Massnahmen. Die Massnahmen werden zusammen mit den Kunden definiert, hierbei kann es sich um das Melden eines Vorfalls an den Kunden handeln, wie auch die direkte Interaktion mit den Systemen.

Verbreitung sicherheitsrelevanter Informationen

(39) Den Kunden wird eine einfach verständliche Sammlung an nützlichen Informationen zur Verfügung gestellt.

- «Berichterstattungsrichtlinien» und Kontaktinformationen für die CSIRT
- Archive von Alarmen, Warnungen und anderen Bekanntmachungen
- Dokumentation der momentan bewährtesten Verfahren (Best Practices)
- Allgemeine Hinweise zur Computersicherheit
- Richtlinien, Vorgehensweisen (Vorgehen/Verfahren) und Checklisten
- Patch-Entwicklungs- und –Verbreitungsinformation
- Herstellerlinks
- Aktuelle Statistiken und Trends der Ereignismeldungen

Risikoanalyse

(40) CERTs können durch ihr Fachwissen einen Mehrwert für die Risikoanalyse ihrer Kunden bieten. Teil der Dienstleistung kann das Führen oder Unterstützen von Analysen und Assessments der Infrastruktur oder Prozesse beinhalten.

Business Continuity and Disaster Recovery Planning

(41) Sicherheitsvorfälle und -trends haben einen immer grösseren Einfluss auf den Betrieb und die Prozesse von Organisationen. CERTs können wertvolle Unterstützungen für die Wiederaufnahme oder der Weiterführung des Betriebes im Falle eines Vorfalles bieten.

Sicherheitsberatung

(42) Das CERT kann Unterstützung und Beratung bei der Implementation von Sicherheits-Infrastrukturen und Prozessen anbieten. Durch, bei Dienstleistungen für andere Kunden, gemachte Erfahrungen kann dieses erworbene Wissen immer wieder miteinfliessen und so den anderen Kunden zur Verfügung gestellt werden, um deren Sicherheit stetig zu verbessern.

Bewusstseinsbildung

(43) Nebst Unterstützung bei der Technik und Prozessen kann ebenfalls Unterstützung bei der Bewusstseinsbildung angeboten werden. Die Bewusstseinsbildung erhöht die Sicherheit bei täglichen Arbei-

ten sowie das grundlegende Verständnis. Dies kann durch das Verfassen von Artikeln, Newsletter, Postern und Ähnlichem umgesetzt werden.

Bildung/Schulung

(44) Es werden Seminare, Workshops, Kurse und Howtos angeboten. Ziel ist es das Fachwissen der Kunden im Bereich rund um Sicherheit zu erhöhen. Die angebotene Dienstleistung wird entsprechend den Bedürfnissen der Kunden gestaltet.

Produktbewertung oder Produktzertifizierung

(45) Das CERT evaluiert neue Produkte und bietet die Möglichkeit diese zertifizieren zu lassen. Es kann sich hierbei um Closed- wie auch Open-Source Produkte handeln.

2.2.4 Outsourcing: Managed Services und Nutzung von Cloud-Diensten

Outsourcing / Managed Services

(1) Viele Organisationen nutzen Managed Services und / oder Outsourcing für Funktionen, die hochspezialisierte Technologien und / oder Fertigkeiten erfordern. Es ist nicht ungewöhnlich, dass Organisationen viele IT-Sicherheitsfunktionen wie Incident Response, Forensics, Cyber Vulnerability Assessments, Risikomanagement, Supply Chain Management oder andere Funktionen, die sie selten verwenden oder ihr Know-how nur periodisch benötigen, auslagern. Der Hauptvorteil von Outsourcing ist, dass es für die Organisation weniger kapitalintensiv ist und kostengünstiger sein kann. Die Anstellung eines Vollzeit-Forensik-Mitarbeitenden ist zum Beispiel aufgrund des hohen Masses an Know-how sehr teuer, aber bei Vorfalluntersuchungen für ein Unternehmen unumgänglich.

(2) Ein Service Level Agreement (SLA) ist ein gemeinsames Mittel zwischen auslagerndem Unternehmen und Dienstleister zur Vereinbarung der Dienstleistungen. Wenn der Dienstleister die Anforderungen der SLA nicht erfüllt, behält sich der Leistungsempfänger das Recht vor, den Vertrag zu kündigen. Wenn es sich um eine externe Instanz für Sicherheitsdienste handelt, ist es wichtig, dass sich beide Seiten auf Rollen, Verantwortlichkeiten, Incident-Handling und -Reporting sowie die Sicherheit von Schnittstellen wie Remote-Access-Richtlinien und Prozeduren, die ein Benutzer fordern kann, einigen. Zusätzlich zum SLA sollten Unternehmen ein Memorandum of Understanding / Agreement (MOU / MOA) und ein Interconnection Security Agreement (ISA) definieren, um die spezifischen Management- und technischen Anforderungen für die Dienstleistungen zu beschreiben.

(3) Wenn es sich um eine externe Partei handelt, die technische Beurteilungen durchführt oder prüft, sollten alle Parteien Regeln für die Zusammenarbeit festlegen und vereinbaren. Cyber-Vulnerability Assessments zum Beispiel erfordern typischerweise ein gewisses Mass an passivem oder aktivem Scannen oder Testen auf den Zielsystemen, was bedeutet, dass die Assessoren entweder selber Zugriff darauf haben oder Zugriffe anderer auf kritische Cyber-Assets innerhalb der Kontrollsystemumgebung beobachten müssen. Das Assessment-Team arbeitet mit seinem organisatorischen Pendant zusammen, um sicherzustellen, dass die Testaktivitäten nicht den Kundenbetrieb stören und sich auch auf Massnahmen zum Monitoring von Protokollen einigen, falls die Aktivitäten irgendwelche Probleme für das Unternehmen verursachen. Die Rules of Engagement (RoE) beinhalten, welche Aktivitäten in welchen Systemen stattfinden können und wer diese Aktivitäten ausführen kann. Es umfasst Entscheidungen darüber, ob das Testen innerhalb des primären (aktiven Produktions-) Steuersystems oder eines glaubwürdigen Ersatzes wie eines Backup- oder sekundären Kontrollsystems, eines Test-netzwerks oder eines eigenständigen Systems stattfindet. Aktive Scans von Produktionssystemen sind zu vermeiden, da sie Betriebsstörungen verursachen oder eine Denial-of-Service-

Bedingung erzeugen können. Passive Aktivitäten wie Netzwerk-Sniffing können angemessen sein. Wenn ein Ersatzsystem verwendet wird, sollte man es mit dem aktiven System vergleichen, um sicherzustellen, dass sie im Betrieb identisch sind. Das Assessment-Team und die Organisation müssen sich darüber einigen, wer während der Testphase ihre "Hände auf der Tastatur" haben wird - besonders, wenn aktive (Produktions-) Steuerungssysteme das Ziel sind. Lokales Personal sollte alle Tests an einer aktiven Steuerung des Assessment-Teams durchführen.

Nutzung von Cloud Services

(1) Wenn Organisationen Cloud-Services für die Datenspeicherung (Übertragung, Speicherung, Verarbeitung) nutzen, sind die entsprechenden Sicherheits- sowie Risikoaspekte zu berücksichtigen. Aus Sicherheitsgründen muss jeder Teil einer extern gehosteten ICS-Architektur ein Mass an Sicherheitshärtung entsprechend der Kritikalität der Funktion, die sie hostet, bereitstellen. Darüber hinaus muss das Unternehmen vom Cloud-Dienstleister verlangen, dass Integrität, Verfügbarkeit und Vertraulichkeit von ICS-Informationen sowie die funktionalen und operativen Details, die mit der Wiederherstellung, dem Ereignis- / Störungsmanagement, dem Failover, der forensischen Unterstützung, dem Monitoring und anderen operativen Abläufen zusammenhängen, berücksichtigt werden. Andere Bereiche, welche Unternehmen berücksichtigen sollten, wenn es um die Verlagerung von Ressourcen in die Cloud geht, sind die Abhängigkeit von ISP-Verbindungen (Internet Service Provider) und die möglichen Bandbreitenerhöhungen, die stattfinden können. Rechtsinstrumente und die Verwendung von SLAs sind wichtig, da alle Anforderungen an die betriebliche Unterstützung explizit identifiziert werden müssen, um sicherzustellen, dass die Erwartungen der Cloud-Provider, der ISP-Verfügbarkeit und der Bandbreitenkapazität vollständig erfüllt sind, um spätere Überraschungen zu vermeiden, falls ein operatives Problem auftritt. Auch andere Aspekte sind zu berücksichtigen, einschliesslich der Auswirkungen von Lastverteilung und andern mögliche Auswirkungen, wenn der Cloud-Provider einen Anstieg der Nutzung der verfügbaren Ressourcen erfährt.

(2) Folgende Massnahmen sind zu treffen, wenn Systeminfrastrukturen oder Prozesse ausgelagert werden (Outsourcing, Managed Services, Cloud-Dienste wie SaaS, IaaS etc.):

- Unterlagen wie Dienstleistungsvertrag, SLA, Non-disclosure Agreement, MOU/MOA, ISA, RoE etc.
- Erstellen interner Weisungen und Richtlinien für die sichere Nutzung von ausgelagerten Dienstleistungen (z.B. Einhalten lokaler Gesetze bei länderübergreifenden Dienstleistungsvereinbarungen, Speichern von Daten etc.).
- Monitoring der Leistungserbringung und SLA, periodischer Austausch zwischen Dienstleister und Leistungsempfänger Stufe Management und operative Führung zur Kontrolle der Erbringung der Dienstleistungen / Einhalten der SLA
- Überprüfen der Leistungserbringung durch den Leistungsempfänger beim Leistungserbringer – sog. 2nd Party Audit
- Überprüfen der Leistungserbringung durch unabhängige Dritte beim Leistungserbringer – sog. 3rd Party Audit, Service Organization Control (SOC) Report wie ISAE 3402 (International Standard for Assurance Engagements)
- Periodische Preis- und/oder Leistungs-Benchmarkings

2.3 Risikomanagement

(1) Will man den Cyber-Sicherheitsstatus mittels einer ICS Defense-in-Depth-Strategie verbessern, muss ein Verständnis für das mit ICS-Cybersicherheit verbundene Unternehmensrisiko geschaffen werden.

Denn schliesslich muss dieses Unternehmensrisiko im Rahmen der gesamten Risikobereitschaft des Unternehmens bewältigt werden.

(2) Wichtig dabei ist, dass die Funktionen des Unternehmens welche zuständig sind für den Betrieb und Wartung der Prozess- und Steuerungssysteme, die Methoden zur Identifikation, und Bewertung der ICT-Security Risiken kennen und zusammen mit den Sicherheitsverantwortlichen im Bereich ICT-Security auf ihre einzigartige System-Umgebung anwenden können. Folgend sind die Hauptschritte des ICT-Risikoprozesses aufgelistet und beschrieben.

(3) Der ICT-Risikoprozess erlaubt es mögliche Bedrohungen für die zu schützenden ICT-Systeme, Applikationen und Daten zu identifizieren, zu bewerten und mit angemessenen Risikostrategien zu behandeln. Dabei geht es primär darum, die identifizierten Risiken angemessen, und unter Einbezug der Wirtschaftlichkeit, mit passenden Massnahmen zu reduzieren. Eine hundertprozentige Sicherheit wird es nie geben. Deshalb muss der Risikoappetit des Unternehmens durch die Geschäftsleitung festgelegt werden. Alle Risiken, welche über der Risikoakzeptanzlinie liegen, müssen aktiv behandelt werden. Restrisiken müssen ausgewiesen und durch die Unternehmensleitung akzeptiert werden.

(4) Der Risikoprozess gliedert sich dabei in die drei Hauptpunkte Risikoanalyse, Risikobewertung sowie die Risikobewältigung. Um die Wirksamkeit der Massnahmen zu überprüfen wird in einem fortlaufenden prozessschritt Risikoüberwachung eine Überprüfung der Risiken durchgeführt und ausgewiesen.

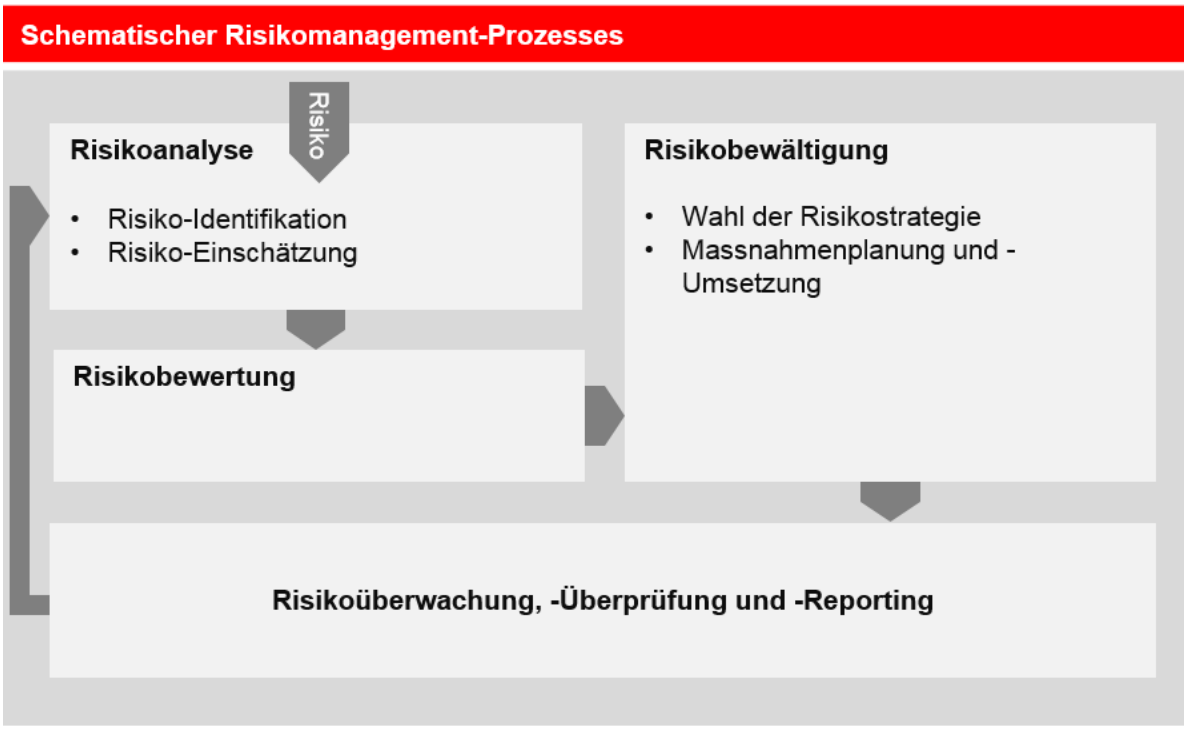

Abbildung 7 Schematische Darstellung des Risikomanagement-Prozesses

2.3.1 Asset-Inventar erstellen, bewerten und bewirtschaften

(1) Um Risiken bewerten zu können, muss man als Erstes die zu schützenden Firmenwerte und Assets bestimmen und inventarisieren. Nur so ist gewährleistet, dass eine umfassende und adäquate Bedrohungsanalyse durchgeführt werden kann.

(2) Dazu soll ein zentrales Asset-Register aufgebaut werden, welches es ermöglicht, den ganzen Life-Cycle eines Assets abzubilden. Neben den Informationen, welche benötigt werden, um die Assets integer zu betreiben, soll das Register auch eine Bewertung der Assets bezüglich der Sicherheitskriterien Vertraulichkeit, Verfügbarkeit und Integrität enthalten. Jedes Asset muss einen Asset-Owner haben, welcher für die Umsetzung des Asset-LifeCycle-Prozesses verantwortlich ist.

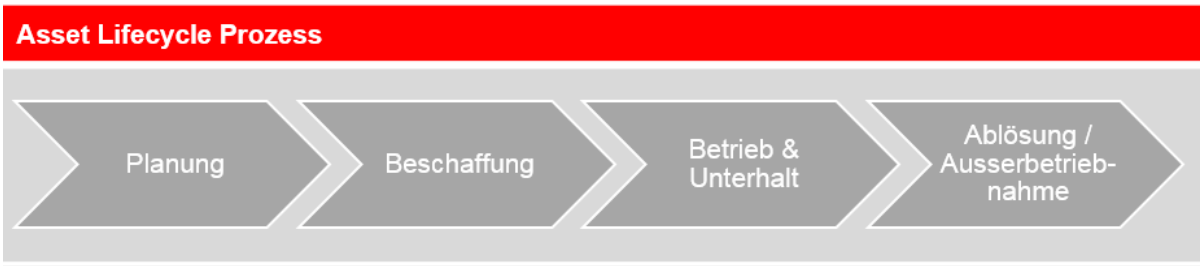

Abbildung 8 Schematischer Asset LifeCycle Prozess

Im Minimum sollen folgende Assets inventarisiert werden:
Folgende Assets müssen inventarisiert werden: a) Alle physischen und virtuellen ICT-Systemkomponenten (wie z.B. Router, WLAN-Access-Points, PCs, mobile Endgeräte, Server, Steuer- und Schutzgeräte etc.) b) Datenbestände c) Anwendungen d) Zonen
Folgende Attribute sind zuzuordnen: a) Verantwortliche/r (je nach Kontext Applikationsverantwortliche/r, Betriebsverantwortliche/r oder Informationsverantwortliche/r) b) Klassifizierung c) Version d) Standort

Tabelle 3 Inventarisierung der Assets

2.3.2 Risikoanalyse

(1) Die Risikoanalyse ist nach der Festlegung des Risikokontexts (Bereich, System, Objekt, über die das Risikomanagement durchgeführt wird) der erste Schritt im Prozess. Die Analyse besteht aus den zwei Hauptschritten Risikoidentifikation und Risikoeinschätzung. Bei der Risikoidentifikation werden möglichst systematisch alle Einflussfaktoren auf den Risikokontext untersucht. Dabei wird eine fortlaufende Bedrohungsanalyse etabliert, welche mit dem aufgebauten Asset-Inventar abgestimmt und verknüpft wird. Hierbei werden mögliche Bedrohungen und deren Akteure identifiziert und mit den vorhandenen Schutzmassnahmen beziehungsweise Schwachstellen der Assets in Zusammenhang gebracht.

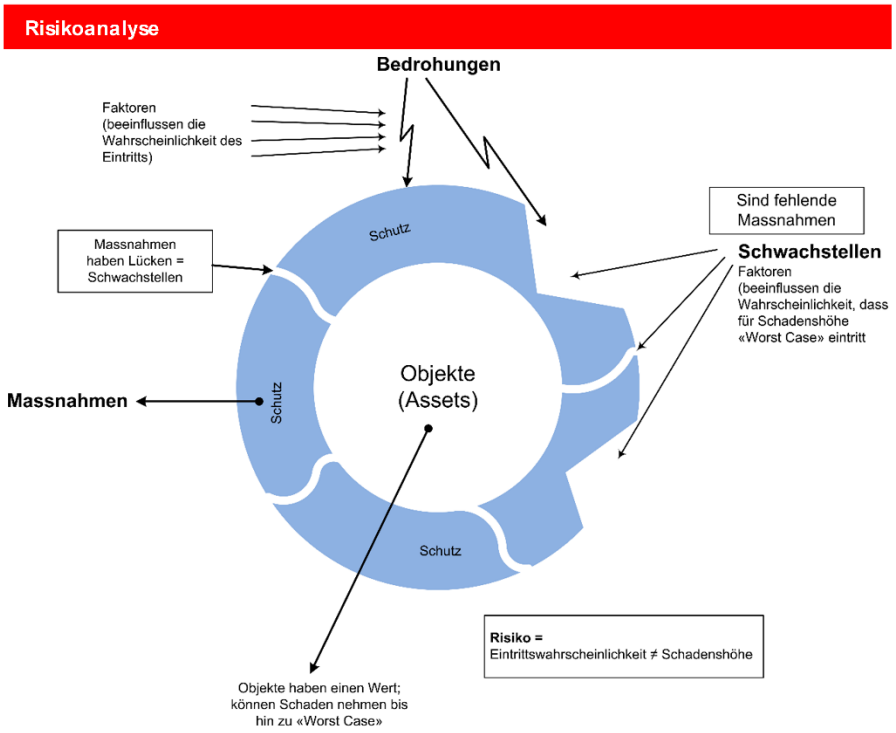

Abbildung 9 Risikoanalyse

(2) Das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Deutschland hat folgende zehn Topbedrohungen für Fertigungs- und Prozessautomatisierungssysteme publiziert: [3]

NR	Bedrohung
1	Social engineering und Phishing
2	Einschleusen von Schadsoftware über Internet und Intranet
3	Infektion mit Schadsoftware über Internet und Intranet
4	Einbruch über Fernwartungszugänge
5	Menschliches Fehlverhalten und Sabotage
6	Mit dem Internet verbundene Steuerungskomponenten
7	Technisches Fehlverhalten und höhere Gewalt
8	Kompromittierung von Extranet und Cloud-Komponenten
9	(D)DoS Angriffe
10	Kompromittierung von Smartphones im Produktionsumfeld

Tabelle 4 Top 10 Bedrohungen gemäss BSI (Momentaufnahme)

[3] Der Bericht ist online verfügbar, unter folgendem Link:
Industrial Control Systems Top 10 Bedrohungen und Gegenmassnahmen

(3) Treffen identifizierte Bedrohungen auf eine Schwachstelle (Lücke), so entsteht ein Risiko für das zu schützende Asset. Diese Lücke kann entweder mit Schutzmassnahmen geschlossen oder aber das Risiko akzeptiert werden (Risikobehandlung). Bedrohungen gehen von verschiedenen Akteuren aus, welche verschiedene Stufen von Know-how, Ressourcen und Motivationen besitzen. Es ist nicht möglich, sich als Unternehmen gegen alle Akteure zu schützen und somit alle Risiken aktiv mitigieren zu können. Gewisse Restrisiken müssen durch das Unternehmen ausgewiesen und akzeptiert werden.

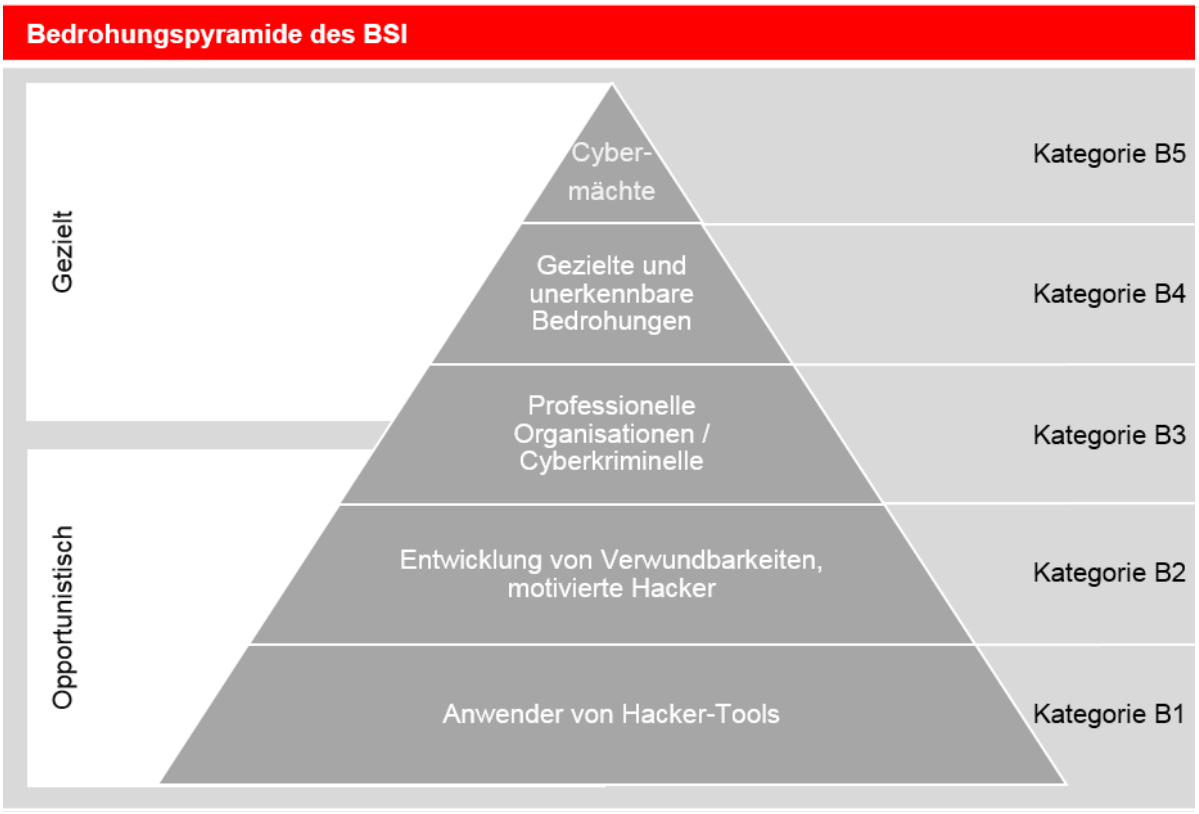

Abbildung 10 Bedrohungspyramide des BSI

NR		Bedrohung	
B 1	Skript-Kiddies	Sie verfügen häufig über kein sehr fundiertes Wissen. Sie verstehen Angriffe auf eine Infrastruktur eher als sportliche Herausforderung und benutzen hierfür üblicherweise Software und Anleitungen, die sie im Internet finden können. Sie nutzen die Schadsoftware, ohne zu verstehen, was im Detail wirklich passiert.	Gering bis mittel
B 2	Motivierte Hacker	Sie sind Personen, die beruflich in die Erforschung und Entwicklung von Angriffsmethoden eingebunden sind. Sie verkaufen ihr Wissen und ihre Dienste in Untergrundmärkten des Cyberspace oder sie setzen ihr Wissen für politische und ideologische Ziele ein (Hacktivists).	Sehr hoch

NR		Bedrohung	
B 3	Professionelle Organisationen und Cyberkriminelle	Kriminelle, die entsprechende Geschäftsmodelle entwickeln, um mittels Cyber-Angriffen und den damit verbundenen Technologien zu spionieren oder Geld zu verdienen. Während sie früher als Einzeltäter auftraten, sind sie heute gut organisiert und beschaffen fehlendes Know-How und Schadsoftware in den Untergrundmärkten. Die Kategorie B3 ist heute die Kategorie mit dem höchsten Schadenpotenzial.	Sehr hoch
B 4	Advanced Persistent Threats (APT's)	Tools welche gezielt und so gut wie unerkannt vorgehen. Sie dringen in geschützte Systeme ein (ev. unter Ausnutzung von Fehlverhalten von Mitarbeitern) und versuchen möglichst lange unerkannt zu bleiben um im System weitere Informationen (z.B. Passwörter) zu stehlen oder „Zeitbomben" / Backdoors zu platzieren.	Sehr hoch
B 5	Cyber-Mächte	USA / China / Russland / UK / Israel: Die gefährlichste Stufe der Bedrohung geht von staatlich unterstützten Akteuren aus den genannten 5 Ländern aus. Diese besitzen regulatorischen und physischen Zugriff auf die massgebenden Hard- und Softwareproduzenten und können so z.B. sicherstellen, dass Produkte bereits mit Back Doors ausgeliefert werden.	Sehr hoch

Tabelle 5 Bedrohungspyramide gemäss BSI

(4) Nach der Identifikation der Risiken erfolgt die Risikoeinschätzung anhand der Eintrittswahrscheinlichkeit und des möglichen Schadensausmasses. Im Bereich ICT-Security ist nebst dem finanziellen Schaden auch die Auswirkung auf die Versorgungssicherheit, Integrität, Vertraulichkeit und Verfügbarkeit der Informationen sowie die Reputation des Unternehmens zu berücksichtigen. Die Risikoeinschätzung kann anhand einer Risikomatrix bewertet werden.

Risikomatrix (Beispiel)

Eintrittswahrscheinlichkeit							
	Wahrscheinlich	Ereignis kann mit hoher Wahrscheinlichkeit eintreten 1-3 Monate (Quartal)	E4	mittel	gross	katastrophal	katastrophal
	Möglich	Ereignis kann eintreten 1 Jahr (Budget)	E3	mittel	mittel	gross	katastrophal
	Selten	Ereignis kann eintreten 1-3 (MFP) Jahre	E2	klein	mittel	mittel	gross
	Unwahrscheinlich	Ereignis kann nur in ganz seltenen Umständen eintreten 3-10 Jahre	E1	klein	klein	mittel	mittel
				S1	S2	S3	S4
				gering	moderat	Bedeutend	Katastrophal
Finanzielle Bewertung EAT = Unternehmensergebnis EK = Eigenkapital				Weniger als CHF 500'000.- < 1% EAT < 0.07% EK	Von CHF 500'000.- bis CHF 5 Mio. > 1% EAT > 0.07% EK	Von CHF 5 Mio. bis CHF 25 Mio. > 10% EAT > 0.7% EK	Grösser CHF 25 Mio. > 30% EAT > 5% EK
Reputation - Medienwahrnehmung - Image - Politische Diskussion - Arbeitgeber-Attraktivität				Selektive, einmalige und kurzfristige Berichterstattung < 1 Woche Regional & Printmedien	Nationale Berichterstattung < 1 Woche Medien-Kampagne und/oder Leitmedien	Nationale Berichterstattung > 1 Woche Medien-Kampagne und/oder Leitmedien; Bewuste Wahrnehmung in der Bevölkerung durch konkrete Beispiele (Funktionale Störungen)	Nationale Berichterstattung > 3 Monate. Nennung min. 1x/Woche Min. 1 Sprachregion Politik und Medien verbünden sich und stellen System in Frage
Versorgungssicherheit				Regionalstörung	Grossstörung	Generalstörung	Flächendeckendes Blackout
Strategie				Umsetzung wesentlicher Elemente verzögert < 1 Monat	Umsetzung wesentlicher Elemente verzögert < 3 Monate	Umsetzung wesentlicher Elemente verzögert < 6 Monate	Umsetzung wesentlicher Elemente gefährdet
				Schadensmass			

Abbildung 11 Risikomatrix (Beispiel)

2.3.3 Risikobewertung

(1) Die in der Risikoanalyse identifizierten Risiken mit ihren Werten für Schadenausmass, Eintrittswahrscheinlichkeit und Risiko, bedürfen einer zusätzlichen Bewertung. Und dies im Kontext des Untersuchungs-Gegenstands. Dabei soll geklärt werden ob die Eintrittswahrscheinlichkeit oder das Schadenausmass oder beides reduziert werden muss. Auch soll die Wechselwirkung zwischen Chance und Risiko analysiert werden. Ein blindes vermeiden von Risiken könnte gleichermassen auch Chancen des Unternehmens verhindern. Auch fliessen in diesem Prozessschritt externe Vorgaben wie gesetzliche Auflagen oder vertraglich verbindliche Abmachungen in die Beurteilung mit rein.

(2) Das Management des Unternehmens muss an dieser Stelle des Risikoprozesses mit Reports zur Risikolandschaft (Auflistung aller identifizierten Risiken mit Bewertung) informiert werden. Das Management hat die Pflicht die Risikolandschaft aus ihrer strategischen Sicht der Unternehmensleitung zu prüfen und zu bestätigen.

(3) Die Ergebnisse dieser Bewertung fliessen dann als „Attribute“ in den nächsten Prozessschritt Risikobewältigung mit ein und müssen da bei der Massnahmenbildung berücksichtigt werden.

2.3.4 Risikobewältigung

(1) In dieser Phase des Risikomanagementprozesses wird die Definition, die Planung und Umsetzung von Massnahmen gemäss der Risikobewertung durchgeführt. Dabei steht im Fokus, das Risikoprofil des Unternehmens auf ein akzeptierbares Niveau (Risiko-Akzeptanz) zu verringern.

(2) Bei der Definition der Sicherheitsmassnahmen ist darauf zu achten, dass die Massnahmen rechtmässig sind, sowie ein optimales Kosten-Nutzen-Verhältnis ausweisen, dem Stand der Technik, dem technologischer Fortschritt und der Bedrohungslage entsprechen. Es ist zu überprüfen, inwieweit das optimale Kosten-Nutzen-Verhältnis dem benötigten Schutzbedarf für national kritische Infrastruktur, angemessen ist. Es kann davon ausgegangen werden, dass einige wirtschaftlich nicht angemessene Sicherheitsmassnahmen im Bereich dieser national kritischen Infrastrukturen umgesetzt werden müssen, um den gewünschten Schutzlevel gewährleisten zu können.

(3) Als vorbereitende Tätigkeiten zur Risikobewältigung gehört die Untersuchung der Machbarkeit der Massnahmen aus Sicht Termin und Aufwand sowie der Sicht der gestellten Anforderungen aus dem vorgelagerten Prozessschritt Risikobewältigung

(4) Zur Minimierung des Risikos stehen folgende Bewältigungs-Strategien zu Verfügung:

- Risiko vermeiden
- Zum Beispiel durch Aufgabe von risikoreichen Prozessen und Aktivitäten oder durch Verlagerungen der Aktivitäten an risikolose Umgebungen.
- Risiko mindern
- Beim Mindern von Risiken werden Massnahmen umgesetzt welche entweder das Schadensausmass oder die Eintrittswahrscheinlichkeit des Risikos minimiert. Dies kann durch technische Massnahmen, Prozesse oder Schulung von Mitarbeitern erreicht werden.
- Risiko transferieren
- Hier steht vor allem die Überwälzung von finanziellen Schäden an Versicherungen im Fokus.
- Risiko akzeptieren

- Risiken oder Restrisiken werden bewusst getragen, um z.B. mögliche Unternehmens-Chancen dadurch nutzen zu können, oder weil die gänzliche Mitigation des Risikos wirtschaftlich nicht tragbar ist.

(5) Die Auswahl einer Bewältigungs-Strategie zu einer Massnahme wird anhand ihrer Wirkung auf das Ursprungsrisiko gemacht. Dabei kann die Risikoeinschätzung und Risikobewertung nochmals durchgeführt werden, um ein optimales Kosten-Nutzen Verhältnis zu erlangen. Eventuell muss dieser Optimierungsprozess mehrmals durchgeführt werden um das Ziel zu erreichen.

(6) Für die so festgelegten Massnahmen muss ein Umsetzungsplan definiert und kommuniziert werden. Dieser berücksichtigt die „Attribute“ der Risikobewertung zum Beispiel bezüglich Dringlichkeit der Massnahme.

(7) Für die definierten Massnahmen muss zwingend ein Massnahmen Eigner bestimmt werden, welcher die Umsetzung der Massnahme verantwortet und Abweichungen vom Umsetzungsplan dem Risiko Eigner meldet. Sicherheit in der Informationstechnologie ist dabei kein abschliessender Zustand, sondern ein kontinuierlicher Prozess. Insbesondere die technische Entwicklung bringt immer wieder neue Gefährdungen und / oder neue Angriffsvektoren mit sich. Auch das Schadensausmass eines einst ermittelten Risikos kann sich über die Zeit ändern. Entsprechend müssen alle Aufgaben im Bereich der Risikobewältigung in regelmässigen Abständen erneut überprüft, allenfalls angepasst und durchgeführt werden.

2.4 Der Faktor Mensch

(1) Menschen sind grundsätzlich fehleranfällige „Systeme“. Unternehmen stehen entsprechend vor vielen Herausforderungen beim Umgang mit dem Faktor Mensch im Zusammenhang mit der ICT-Sicherheit. Grosse und komplexe Systeme sind anfällig für Fehler von unerfahrenem oder ungeübtem Personal sowie Aktivitäten von bösartigen Insider-Bedrohungen. Der typische Fall ist dabei allerdings nicht der böswillig handelnde, sondern vor allem der leichtsinnig oder fahrlässig handelnde Mitarbeitende. Aus Unwissen, Unaufmerksamkeit oder Bequemlichkeit tendieren Mitarbeitende dazu, sich früher oder später fehlerhaft zu verhalten. Ein typisches Szenario ist z.B. der leichtfertige Umgang mit Passwörtern, die z.B. leicht zu erraten sind oder womöglich gar in der Nähe des Gerätes aufbewahrt werden (Post-it am Monitor…). Ein weiteres realistisches Szenario ist das Anklicken eines Links in einer E-Mail, womit z.B. versucht wird, Zugangsdaten zu entwenden oder Malware zu installieren. Aber auch der Einsatz von (möglicherweise nicht autorisierten) privaten Geräten und Datenträgern (USB Sticks, externe Festplatten) sowie der Austausch von Dateien über nicht autorisierte Mail- oder Clouddienste (Geschäftsunterlagen auf Dropbox etc.) kommen regelmässig vor. Solche Fehlverhalten können für das betroffene Unternehmen bereits geschäftskritisch sein, auch wenn bei den geschilderten Beispielen tendenziell keine kriminelle Energie hinter dem Handeln der Mitarbeitenden steckt.

(2) Mit mehr krimineller Energie nimmt die Gefährdung weiter zu. Die kriminelle Motivation kann wiederum unterschiedlich sein. Mitarbeitende können aus finanziellen Gründen versuchen, sich zu bereichern oder können aber auch aus persönlichem Frust handeln und dem Arbeitgeber Schaden zufügen. Das gefährlichste Szenario wäre eine geplante Aktion, bei der Mitarbeitende erpresst oder korrumpiert werden, um beispielsweise Schadsoftware zu installieren oder Zugangsdaten zu verraten.

(3) Unternehmen sind angewiesen, ihre Mitarbeitenden für diese vielfältigen Gefahren zu sensibilisieren und sie im vorschriftsmässigen Umgang mit den ICT-Mitteln regelmässig zu schulen.

2.4.1 Richtlinien

(1) Es sind klare und umsetzbare Massnahmen erforderlich, um den Rahmen für strenge Kontrollen festzulegen, die die ICS-Technologien sichern und auch die für die Bewältigung der menschlichen Faktoren notwendige Governance schaffen. Politiken legen den Rahmen für detaillierte Verfahren und legen die Erwartungen der Organisation hinsichtlich der durchgeführten Tätigkeiten fest. Die Richtlinien erläutern die Regeln für die Sicherung des ICS - unter Angabe der erwarteten Verhaltensregeln und der erforderlichen Kontrollen. Politiken skizzieren, was sein muss, was nicht eintreten darf sowie Sanktionen bei Nichteinhalten.

2.4.2 Verfahren

(1) Historisch gesehen war das Sicherheitsmanagement immer in der Verantwortung der IT-Sicherheitsorganisation, die, in aller Regel durch Richtlinien, Betriebsprozesse und Prozeduren geleitet, unternehmenswichtige Daten und Informationen schützt. Da industrielle Kontrollsysteme ein Teil grösserer zusammenhängender Netze und Architekturen geworden sind, müssen Sicherheitsverfahren und Mechanismen entsprechend angepasst werden, um auch die vernetzte Prozessleittechnik abzudecken.

(2) Verfahren sollten festlegen, wie bestimmte Prozesse durchzuführen oder wie bestimmte Systeme zu konfigurieren sind, damit das Funktionieren von Steuerleitsystemen in einer standardmässigen, sicheren, nachvollziehbaren und wiederholbaren Weise gewährleistet werden kann. Definierte, dokumentierte, standardisierte Verfahren ermöglichen es auch, neue Mitarbeitende schnell und einfach einzuschulen und so sicherzustellen, dass alle Mitarbeitenden die erforderlichen Vorschriften und Standards im gesamten OT-Umfeld einheitlich befolgen. ICS-Sicherheitsverfahren leiten die ICS-Operatoren bei zu ergreifenden Massnahmen in Notfallsituationen, wie z.B. beim Eindringen von Schadsoftware oder auch bei anderen betrieblichen ungeplanten Unterbrüchen. Standardisierte Sicherheitsverfahren sind auf Grund der hohen Anforderungen an Verfügbarkeit und Echtzeitfähigkeit im ICS-Umfeld besonders wichtig, da die Anwendung herstellerspezifischer Protokolle und die Langlebigkeit von Legacy-Systemen die Bemühungen zum Schutz unternehmenskritischer Systeme und insbesondere auch kritischer Infrastrukturen behindern können. In definierten, dokumentierten Standardverfahren können Indikatoren und Messpunkte festgelegt und gemessen werden, können so der Leistungsfähigkeit insgesamt dienen und erlauben Benchmarks über längere Zeit oder den Vergleich mit anderen. Schlussendlich erlauben standardisierte, wiederholbare Verfahren und gemessene Indikatoren auch laufende Überprüfung und kontinuierliche Verbesserung von Effektivität und Effizienz. Es ist schwierig, ein Verfahren zu verbessern, wenn es bei jedem Durchgang verschieden ausgeführt wird, wenn man nicht weiss oder erkennt, was eine Verbesserung bringt und was nicht.

2.4.3 Ausbildung und Bewusstsein

(1) Viele Organisationen übersehen Sicherheitstrainings und Sensibilisierungsaktivitäten öfter als viele andere Bereiche im ICS-Betrieb. OT-Eigentümer und Betreiber verlassen sich auf ihr intimes System- und Prozesswissen, um das ordnungsgemässe Funktionieren des Systems zu gewährleisten, und sie verteilen in der Regel nur Zeit und Ressourcen für systemfunktionalisierte Zwecke. Da sich ICS zunehmend vernetzen und Cyber-Bedrohungen und Schwachstellen zunehmen, ist es für Unternehmen von entscheidender Bedeutung, dass sie ICS-sicherheitsspezifische Schulungen erfordern und unter-

stützen. IT-Implementierer und OT-Betreiber sollten wissen, wie die Indikatoren für potenzielle Kompromisse aussehen und welche Schritte sie ergreifen sollten, um sicherzustellen, dass eine Cyber-Untersuchung gelingt. IT und ICS-Management sollten auch wissen, was sie tun können, um das System sicherer zu machen, damit sie fundierte Entscheidungen hinsichtlich der Kosten / Nutzen der Schutzmassnahmen treffen können, die sie eingeführt haben.

2.5 Lieferanten- und Hersteller-Management

2.5.1 Sicherheitsrichtlinien für Lieferanten und Hersteller-Management

(1) In den letzten Jahren sind sich Anbieter der Bedeutung von Cyber-Sicherheit in industriellen Steuerungslösungen bewusst geworden. Dieses erfolgte primär nach der Bekanntgabe der Cyber-Schwachstellen im Zusammenhang mit Exploits, Stuxnet, SQL Slammer Wurm und anderen.

(2) Um den Anforderungen des neuen Marktes gerecht zu werden, haben viele Hersteller sicherheitsrelevante Komponenten in ihren Produktlebenszyklus integriert. Nicht jeder Hersteller hat diesen Weg gewählt, jedoch die meisten der Marktführer.

(3) Es ist nicht davon auszugehen, dass Anbieter immer strenge Sicherheitsvorkehrungen in ihrem Produktlebenszyklus integriert haben. Deshalb ist es notwendig frühzeitig Anforderungen an die Sicherheit des Steuersystems im Beschaffungsprozess zu adressieren. Dies ist nicht nur vorteilhaft für den Anlagen-Besitzer, sondern bietet auch den Anbietern spezifische Anleitung, welche Funktionalität sie benötigen.

(4) Folgende Punkte sollten berücksichtigt werden:

- Prüfen des Produktlebenszyklus / Entwicklung und welche Sicherheitselemente durch den Lieferanten/Hersteller garantiert werden.
- Mit Lieferanten/Hersteller sicherstellen, dass das eingebettete System keine manipulierten, gefälschten oder getauschten Komponenten enthalten.
- Sicherstellen, dass das eingebettete System der Spezifikation entspricht und keine verdeckten Funktionen bei der Herstellung implementiert wurden
- Prüfen welche Anforderungen der Lieferanten/Hersteller an die Wartung / Service seiner Produkte stellt (Patchhandling / Intervalle / Zugriff), bzw. überprüfen ob die internen Anforderungen / Regeln durch den Hersteller erfüllt sind.
- Erstellen eines Lieferanten/Hersteller Mindestanforderungskatalogs.

2.5.2 Sicherheitsthemen in Ausschreibungen und Verträgen

(1) Bei Ausschreibungen oder Verträgen mit dritten dürfen die Sicherheitsthemen nicht ausseracht gelassen werden. Bei der Ausschreibung muss darauf hingewiesen werden welche Sicherheitsstandards bestehen und mit welchen Sicherheitsauflagen ein System implementiert, bzw. betrieben wird. Ebenso wichtig ist das Festlegen von Geheimhaltungsvereinbarungen und Vereinbarungen mit welchen Prozessveränderungen im Produktivsystem vorgenommen werden. Mit diesen Massnamen soll formell verhindert werden, dass Informationen das Unternehmen verlassen sowie klar festlegt sein, wer welche Veränderungen vornehmen darf.

(2) Im Folgenden ist eine Auflistung möglicher Vertragsinhalte in Bezug auf Sicherheit:

Informationen / Daten

- Welche Informationen sind als vertraulich / geheim eingestuft und wie müssen diese behandelt werden.
- Auf welchem Kommunikationsweg und mit welchem kryptographischen Verfahren müssen die Daten verschlüsselt sein.
- Wo dürfen geheime / vertrauliche Daten gespeichert werden. Bei Ablage auf Fremdsystemen ist zu regeln wie und wann die Daten dauerhaft gelöscht werden. Speziell zu berücksichtigen sind Backup Medien und eventuelle Cloud-Speicherorte.
- Für alle Informationen und Daten, die dem Dienstleister im Rahmen seiner Tätigkeit bekannt werden bzw. anfallen, muss sichergestellt sein, dass diese nur beim Dienstleister verarbeitet oder gespeichert werden. Falls die Speicherung und/oder Verarbeitung von Informationen und Daten von Dritten durchgeführt wird, muss sichergestellt sein, dass der Dritte die entsprechenden Anforderungen dieser Sicherheitsrichtlinie erfüllt.

ICT-Komponenten und Systemen

- Werden Systeme und ICT-Komponenten zur Reparatur oder Entsorgung gegeben, ist die durchgängige Wahrung der Vertraulichkeit sicherzustellen
- Vernichtung von Daten / Konfigurationen auf den ICT-Komponenten und / oder den ICT-Komponenten selbst

Grundschutz / Schnittstellen

- Wie werden Mitarbeiter der Lieferanten, Hersteller auf IT-Grundschutz oder ein vergleichbares Schutzniveau vertraglich verpflichtet
- Sind alle Schnittstellen zwischen den Vertragsparteien identifiziert, so dass dafür entsprechende Sicherheitsanforderungen gestellt werden können
- Ist festgelegt, welche Rechte (Zutrittsrechte, Zugangsrechte, Zugriffsrechte) dem Lieferanten und Hersteller vom Auftraggeber einzuräumen sind
- Wie wird das Personal der Lieferanten und Hersteller identifiziert und wie wird dieses registriert
- Werden gesetzliche Auflagen / Anforderungen und Urheberrechte durch den Lieferanten, Hersteller eingehalten und wie wird dies sichergestellt
- Ist festgelegt in welcher Form der Lieferant, Hersteller Sub-Contracting durchführen darf und wie sind Kontrollmechanismen definiert

2.5.3 Lieferkettenmanagement

(1) Die Lieferkette stellt ein erhebliches Risiko für ICS-Systeme dar. ICS-Hersteller und Software-Entwickler erstellen ihre Produkte an vielen verschiedenen Orten auf der ganzen Welt. Schaltungen und Chips werden häufig von unterschiedlichen Institutionen funktional beschrieben und physisch produziert werden. Sowohl viele bekannte Chiphersteller als auch hochspezialisierte Kleinunternehmen sind sogenannte "fabless companies". Sie entwickeln Schaltungen und Chips, produzieren diese aber nicht selbst. Die Fertigung erfolgt durch darauf spezialisierte Firmen, sogenannte "silicon foundries", in der ganzen Welt, zumeist ausserhalb von Europa. Die gefertigten Chips werden von dort direkt an die Kunden oder den Grosshändler ausgeliefert. Auch die bekannten Distributoren sind weltweit verstreut.

(2) Die Gewährleistung der Sicherheit des Systems oder der Anwendung während des gesamten Entwicklungslebenszyklus ist deshalb für die meisten ICS-Betreiber nicht möglich. Der Kauf von kommerziellen Standardprodukten (COTS[4]-Technologien) erhöht die Wahrscheinlichkeit des Empfangs von nicht-genuinen Geräten. Ausserdem ist ICS-CERT über Berichte im Zusammenhang mit Geräten mit eingebettetem, nicht autorisiertem, Code in seiner Firmware oder dem Betriebssystem bekannt, die eine Hintertür in das Gerät bereitstellen oder es dem Programm ermöglichen, nach dem Installieren "nach Hause zu telefonieren". Um diese Bedrohungen abzuschwächen, müssen die Eigentümer von Vermögenswerten sorgfältig auf die Beschaffungsverträge, die Qualitätskontrolle und die Validierung der Leistungsfähigkeit auf die Spezifikationsprozesse achten. Darüber hinaus ist eine umfassende Prüfung, einschliesslich Scannen von Schwachstellen, eine wichtige Aufgabe, bevor Sie Systeme in Produktionsumgebungen installieren.

(3) Bei erhöhtem Schutzbedarf sind Hersteller und deren Subunternehmer zu qualifizieren, ob sie vertrauenswürdig sind Hard- und Software herzustellen. Der Nachweis ist zu dokumentieren. Eine solche Hersteller-Qualifizierung muss regelmässig erneuert werden.

(4) Beispiele aus der ICS / IT-Umgebung die in den letzten Jahren aufgetreten sind:

- Netzwerk- oder Computerhardware mit installierter Malware,
- Software oder Hardware mit Malware eingefügt durch verschiedene Mittel,
- Schwachstellen in Softwareanwendungen und - netzen innerhalb der Lieferkette
- Infizierung durch Download von Treibern aus dem Internet
- Gefälschte Computerhardware.

2.5.4 Überwachung und Überprüfung von Dienstleistungen

(1) Werden externe Dienstleister für das Projekt eingebunden, zum Beispiel für Hosting, Aufbau, Installation, Software-Entwicklung oder Lieferung von Standard-Software, werden diese auch auf IT-Sicherheit vertraglich verpflichtet. Bei der Überwachung der Dienstleistungen geht es darum die vertraglich festgelten Regeln zu überwachen und zu überprüfen. Es soll verhindert werden, dass während dem Projektablaufs / Serviceerbringung gegen keine der definierten Sicherheitskriterien verstossen wird.

2.5.5 Überwachung und Überprüfung von Fernzugriffen

(1) Werden Services durch Dienstleister bezogen, wird oft ein Fernwartungszugang zu den Systemen benötigt. Diese Art von Zugang stellt eine der grösseren Gefahren in Bezug auf Systemsicherheit dar. Die Herausforderung besteht darin, den Zugang soweit wie nur möglich zu limitieren und Aktionen, die durch den Dienstleiter erfolgen, nachvollziehbar zu loggen. Es muss klar geregelt sein, wer wann mit welchen Regeln auf welche Systeme zugreifen darf.

(2) Im Folgenden eine Auflistung der Anforderungen in Bezug auf Fernwartungszugänge:

- Jeder Fernzugang erfolgt ausschliesslich über personalisierte Accounts, welcher nur auf die benötigten Systeme zugreifen kann

[4] COTS: Commercial off-the-shelf

- Ein Fernzugriff kann nur nach Autorisierung des Betriebspersonals erfolgen. Wird eine Sitzung nicht getrennt, erfolgt dieses automatisch nach einem Zeitintervall. Nach Trennen der Sitzung ist die Verbindung zu den Systemen logisch und, wenn immer möglich, physikalisch getrennt
- Die Vorortwartung durch Dienstleister stellt ein ernst zu nehmendes Sicherheitsrisiko dar. Es ist zu vermeiden, dass der Auftragnehmer eigene Hardware an das Prozessnetz anschliesst (z. B. Wartungs-Notebooks, aber auch Speichergeräte wie USB-Sticks). Falls dies doch nötig sein sollte, muss diese Hardware speziell abgesichert und vom Auftraggeber genehmigt sein sowie zeitnah auf Malware untersucht werden. Der Auftragnehmer ist verpflichtet, die Durchsetzung einer angemessenen internen Sicherheitsrichtlinie für diese Dienstleistung nachzuweisen
- Aufzeichnen der Fernzugriffe (Session Recording)

2.6 Physische Sicherheit

(1) Physische Sicherheitsmassnahmen reduzieren das Risiko versehentlicher oder vorsätzlicher Verluste oder Schäden an organisatorischen Vermögenswerten und der Umwelt. Zum Unternehmensvermögen gehören unter anderem physische Vermögenswerte wie Geräte und Anlagen, die Umwelt und das geistige Eigentum einschliesslich proprietärer Daten wie Prozesseinstellungen und Kundeninformationen.

(2) Physische Sicherheitskontrollen müssen häufig Umwelt-, Sicherheits-, Regulierungs-, Rechts- und sonstige Anforderungen erfüllen, die häufig für eine gegebene Umgebung spezifisch sind. Physische Sicherheitsmassnahmen sollten an die übergeordneten Anforderungen des Gesamtschutzes angepasst werden.

(3) Unternehmen müssen den physischen Schutz der Cyber-Komponenten und Daten, die mit dem ICS verbunden sind, als Teil der Gesamtsicherheit in der ICS-Umgebung ansprechen. Die Sicherheit in vielen ICS-Einrichtungen ist eng mit der Anlagensicherheit verbunden, mit dem vorrangigen Ziel, Menschen aus gefährlichen Situationen herauszuhalten, ohne sie an ihrer Arbeit zu hindern. Physische Sicherheitskontrollen sind physikalische Massnahmen, entweder aktiv oder passiv, die den physischen Zugriff auf alle Informationswerte in der ICS-Umgebung begrenzen. Unternehmen setzen diese Massnahmen ein, um unerwünschte Systemauswirkungen wie die folgenden zu vermeiden:

- Unbefugter physischer Zugang zu sensiblen Orten
- Physikalische Veränderung, Manipulation, Diebstahl oder sonstige Entfernung oder Zerstörung bestehender Systeme, Infrastruktur, Kommunikationsschnittstellen, Personal oder physischer Standorte
- Unerlaubte Beobachtung von sensiblen Informationen und von Vermögenswerten durch visuelle Beobachtung, Notizen, Fotografien oder durch andere Mittel
- Unerlaubte Einführung neuer Systeme, Infrastruktur, Kommunikationsschnittstellen oder anderer Hardware
- Unerlaubte Einführung von Geräten, die absichtlich entworfen wurden, um Hardware-Manipulationen, Abhören oder andere schädliche Tätigkeiten durchzuführen mittels USB-Speichergerät, Wireless Access Points, Bluetooth oder anderen mobilen Technologien.

2.6.1 Grundsätze der physischen Sicherheit

(1) Der physische Zugang zu Steuer- und Kontrollsystemkomponenten impliziert oft den logischen Zugang zum Prozessleitsystem. Ein physischer Zugang ermöglicht einem Delinquenten, durch physi-

sche Massnahmen auch logische Kontrolle zu erlangen. Dies kann z.B. der Fall sein, wenn Computer leicht zugänglich sind und diese mobile Medienlaufwerke haben, wie Disketten-Laufwerke, CDs, DVDs, Blue-ray Laufwerke, externe Festplatten oder USB-Ports. Unternehmen können diese Laufwerke mit Schlössern versehen, sie von den Computern entfernen oder USB-Ports deaktivieren. Abhängig von den Sicherheitsbedürfnissen und -risiken kann man auch Stromschalter deaktivieren oder physisch schützen, um unbefugte Betätigung zu verhindern. Für maximale Sicherheit werden Server in abgeschlossenen Bereichen platziert und mit Authentifizierungsmechanismen (wie 2-Weg-Authentifizierung) geschützt. Netzwerkgeräte im ICS Netzwerk, einschliesslich Switches, Router, Netzwerk-Buchsen, Server, Workstations und Controller, sollen nur einem autorisierten Personenkreis und in einem gesicherten Bereich zugänglich gemacht werden. Zudem sollte der gesicherte Bereich auch mit Umweltschutz-Anforderungen (z.B. Halon-Löschanlagen) vereinbar sein.

(2) Klassische physische Sicherheit bezieht sich in der Regel auf eine konzentrische Ring-Architektur gestaffelter physischer Massnahmen. Mehrere physische Barrieren - sowohl aktive als auch passive - um Gebäude, Einrichtungen, Räume, Geräte oder andere Informationswerte herum repräsentieren diese physischen Sicherheitsperimeter. Zu physischen Sicherheitskontrollen gehören Zäune, Gräben, Erdwälle, Wände, verstärkte Barrikaden, Tore oder andere Massnahmen. Die meisten Unternehmen verwenden als erste Abwehrmassnahme geschützten Zugang zu Anlagen, wie z.B. Zäune, Wachen, Tore und verschlossene Türen.

(3) Physische Zutrittskontrollsysteme sollten sicherstellen, dass nur autorisierte Personen Zugang zu kontrollierten Räumlichkeiten haben. Ein Zutrittskontrollsystem sollte flexibel sein. Die Notwendigkeit des Zugangs kann von der Tages-, Wochen- oder gar Jahreszeit, dem Ausbildungsniveau, Beschäftigungsstatus, der Arbeitsaufgabe, des Anlagenstatus oder unzähligen anderen Faktoren abhängen. Ein System muss sicherstellen, dass Personen, die Zugang erhalten, wirklich jene sind, wer sie behaupten zu sein (in der Regel mit „was die Person besitzt“, wie eine Zugangskarte oder einen Schlüssel; „was sie kennt“, wie eine PIN; oder „wie sie sind“ bezüglich eines biometrischen Merkmals). Zutrittskontrollen sollten sehr zuverlässig sein, aber nicht Routine- oder Notfallaufgaben des Anlagenpersonals beeinträchtigen. Integration von Zutrittskontrollsystemen ins gesamte Prozesssystem bietet einen erweiterten Blick über den reinen Sicherheitszugang hinaus, ermöglicht physisches Tracking und kann Reaktionszeiten, z.B. in Notfallsituationen, beschleunigen und hilft einer verbesserten Gesamtproduktivität. Der Zugang zu Netzwerk- und Computerschränken sollte auf Personen beschränkt sein, die Arbeiten auszuführen haben. Alle Computer und die Netzwerkperipherie sind in sicheren Racks zu installieren. Es sollte ein „remote Terminal“ bzw. ein „remote Human-Machine-Interface“ (HMI) verwendet werden, um an die Rack-Computer anzuschliessen.

(4) Zugangsüberwachungssysteme beinhalten Stand- und Videokameras, Sensoren und verschiedene Arten von Identifikationssystemen. Diese Geräte verhindern nicht ausdrücklich den Zugang zu einem bestimmten Ort, sie zeichnen vielmehr die physische Präsenz oder Abwesenheit auf. Wichtig ist dabei eine ausreichende Beleuchtung für die Art der eingesetzten Überwachungseinrichtung.

(5) Zutrittslimitierende Systeme können eine Kombination von Geräten verwenden, um den physischen Zugriff auf geschützte Ressourcen zu kontrollieren oder zu verhindern. Solche Systeme umfassen sowohl aktive als auch passive Sicherheitsvorkehrungen wie Zäune, Türen, Safes oder Tore. Sie werden oft mit Identifikations- und Überwachungssystemen gekoppelt, um einen rollenbasierten Zugang für bestimmte Personen oder Personengruppen zu ermöglichen.

(6) Die Lokalisierung von Personen und Fahrzeugen in einer grossen Anlage ist nicht nur aus Informationssicherheitsgründen wichtig, sondern auch aus Arbeits- und Betriebssicherheitsgründen (engl. Safety, d.h. Leib und Leben). Lokalisierungstechnologien können die Bewegungen von Personen und Fahrzeugen innerhalb der Anlage verfolgen, um sicherzustellen, dass sie in autorisierten Bereichen bleiben oder sie können dem Personal die nötige Hilfe und Unterstützung in einem Notfall zukommen lassen.

(7) Bei der Adressierung von Sicherheitsbedürfnissen eines Systems und der Daten sind immer auch Umweltfaktoren zu berücksichtigen, zum Beispiel Luftfilter in einer staubigen Umgebung. Dies ist besonders wichtig, wenn der Staub leitend oder magnetisch ist oder in Umgebungen, die Systeme und Medien enthalten, die eine stabile Temperatur oder Feuchtigkeit verlangen. Das Prozessleitsystem sollte einen Alarm auslösen, wenn Umweltvorgaben wie Temperatur oder Feuchtigkeit, Grenzwerte überschreiten.

(8) Heizungs-, Lüftungs- und Klima-Anlagen (engl. Heating, Ventilation, Airconditioning - HVAC) müssen im Normalbetrieb und in Notsituationen das Betriebspersonal schützen, was zur Freisetzung von toxischen Stoffen führen kann. Unternehmen sollten Feuerlöschsysteme sorgfältig einsetzen, um zu vermeiden, dass noch mehr Schaden entsteht. HVAC- und Brandschutzsysteme müssen auch gegen potenzielle Cyber-Vorfälle geschützt werden (z.B. ist es in einem berühmten Fall 2014 Hackern gelungen, beim US Amerikanischen Handelsunternehmen TARGET via HVAC ins Finanzsystem einzudringen).

(9) Eine zuverlässige Stromversorgung ist enorm wichtig, was eine unterbrechungsfreie Stromversorgung (USV) für Steuerleitsysteme unerlässlich macht. Wenn ein Notstromgenerator vorhanden ist, muss die USV-Batterie nur für einige Sekunden Strom liefern; wer jedoch auf externe Stromversorgung angewiesen ist, muss die Lebensdauer der USV-Batterie für mehrere Stunden auslegen. Es sollte mindestens so bemessen sein, dass das System sicher heruntergefahren werden kann.

(10) Die physische Sicherheit des Kontrollzentrums bzw. Kontrollraumes reduziert die Wirkung vieler Bedrohungen. Kontrollzentren und Kontrollräume haben häufig permanent angemeldete Konsolen mit kontinuierlichem Zugriff auf primäre Steuerungsserver, wobei die Reaktionsgeschwindigkeit und die ständige Sicht auf die Anlage von grösster Bedeutung sind. In diesen Bereichen werden oft die Server selbst und andere kritische Computerknoten und Steuersysteme gehostet. Asset-Verantwortliche müssen den Zutritt zu diesen Bereichen nur auf autorisierte Benutzer beschränken, indem sie Authentifizierungsmethoden, wie intelligente oder magnetische Identitätskarten oder biometrische Geräte, verwenden. In vielen Fällen ist es erforderlich, eine Offsite-Notzentrale / Leitstelle zur Verfügung zu halten, damit die Steuerung sichergestellt werden kann, wenn die primäre Leitstelle unbrauchbar wird.

(11) Computer und computergesteuerte Geräte, die für ICS-Funktionen verwendet werden (wie z. B. speicherprogrammierte Steuersysteme - SPS), sollten den ICS-Bereich nicht verlassen. Laptops, tragbare Parametrier- oder Fernwirk-PCs und Handhelds sollten streng gesichert und nicht ausserhalb des ICS-Netzwerks eingesetzt werden.

(12) Unternehmen sollten auch das Verkabelungsdesign und die Implementierung für das Steuerungsnetzwerk sichern. Nicht abgeschirmte Twisted-Pair-Kommunikationskabel, die in einer Büroumgebung akzeptabel sind, sind in der Regel wegen der Anfälligkeit gegenüber Störungen durch Magnetfelder, Funkwellen, Temperatur-Extreme, Feuchtigkeit, Staub und Vibrationen nicht für Anla-

genumgebungen geeignet. Lichtwellen- und Koaxialkabel sind oft bessere Netzwerkverkabelungsoptionen für das Steuerungsnetzwerk, weil sie gegen viele der typischen Umgebungsbedingungen immun sind, einschliesslich elektrischer und Hochfrequenzstörungen, die in industriellen Steuerungsumgebungen oft vorhanden sind. Farbcodes, Etikettenkabel und Steckverbinder reduzieren das Potenzial für einen unbeabsichtigten Cross-Connect. Kabelinstallationen in schliessbaren Schränken beschränken den Zugang zu autorisiertem Personal.

(13) Zusammengefasst können minimale physische Sicherheitsmassnahmen wie folgt definiert werden:

- Definition verschiedener Sicherheitszonen mit verschiedenen Sicherheitsanforderungen an die physische Sicherheit. Gerade in Energieübertragungs-, Verteilungssystemen und im Bereich der dezentralen Erzeugung werden Komponenten über dezentrale Standorte verteilt. Die Ausstattung befindet sich in den Kontroll- und Technikräumen, im Gebäude oder in dezentralen Standorten. Manchmal befindet sich das Gerät bei Dienstleistern oder in öffentlichen Umgebungen. Es ist normalerweise nicht möglich, ein umfassendes Mass an physischem Schutz für periphere, potenziell unbesetzte Standorte zu erreichen; Daher sollte das Restrisiko gegebenenfalls durch ergänzende Massnahmen und kompensierende Kontrollen ergänzt werden.
- Definieren von minimalen physischen präventiven und detektiven Sicherheitskontrollen für die verschiedenen Sicherheitszonen.
- Physische Perimeter-Kontrolle: Umsetzung von Sicherheitsmassnahmen, um Sicherheitszonen zu schützen, die sensible oder kritische Informationen oder Verarbeitungsanlagen enthalten.
- Zutrittskontrollen: Sichere Bereiche sind durch entsprechende Zutrittskontrollen geschützt und nur für autorisiertes Personal zugänglich.
- Büro und Betriebsräume: Physische Sicherheit von Büros u.a. wichtigen Räumlichkeiten wie Leitstellen ist definiert und umgesetzt.
- Schutz gegen externe und Umweltbedrohungen: Physischer Schutz gegen natürliche und bösartige Angriffe ist definiert und umgesetzt.
- Sichere Zonen werden definiert, ausgeschieden und physisch gesichert.
- Zutrittspunkte (Access Points) wie Liefer-, Lade- u.a. Zonen werden definiert, isoliert und entsprechend physisch geschützt.
- Kontrollzentren: Massnahmen zur Gewährleistung der physischen Sicherheit von Kontrollzentren, in denen zentrale Steuerungssysteme wie Steuerungsserver, HMI und unterstützende Systeme untergebracht sind, sollen entworfen, entwickelt und angewendet werden.
- Technik, Geräteräume und periphere Räume: Physische Sicherheitsmassnahmen sind entsprechend der Kritikalität und Gefährdung definiert und umgesetzt.

(14) Es sei hier auch darauf hingewiesen, dass es eine gesonderte VSE Branchenempfehlung[5] zur physischen Sicherheit gibt.

2.7 ICS-Netzwerkarchitekturen

(1) Eine sichere und robuste ICS-Netzwerkarchitektur stellt einen der wichtigsten Grundsätze für einen erfolgreichen Schutz gegen Angriffe dar. Jede Schnittstelle, jeder Übergang und jede Verbindung ist eine potentielle Gefahr. Aus diesen Gründen ist es zwingend erforderlich, dass die gesamten Vorgänge in den verschiedenen Netzen und Anlagen bekannt sind und entsprechend behandelt werden. Dabei bildet die richtige Gruppierung und Segmentierung der Netzwerkarchitektur die Basis.

[5] Das Branchendokument wird voraussichtlich im Frühjahr 2019 veröffentlicht

2.7.1 Grundsätze und Grundlagen

(1) In der Vergangenheit wurden die ICS-Systeme streng isoliert von der Aussenwelt betrieben und abgeschottet. Die heutigen Anforderungen an Informationsaustausch und Automatisation zwischen den ICS-Systemen und den Businessanwendungen führt dazu, dass die verschiedenen Systeme verbunden bzw. vernetzt werden müssen. Ein weiteres Problem stellen die verschiedenen funktionsbezogenen Systeme dar, wie z.B. für Gebäudeüberwachung, Netzsteuerungen, Produktionssteuerungen, welche oft in einem Netzwerk zusammengefasst werden. Somit ist jede Verbindung bzw. Vernetzung zwischen diesen Teilsystemen ein Übergang, welcher ein potentielles Sicherheitsrisiko darstellt. Weiter hat auch der Einsatz von Standard IT-Komponenten (Hard- und Software), welche stetig gepatcht und upgedatet werden müssen, die Anforderung für zusätzliche Zugänge zu den nötigen Mittel herbeigeführt. Darum entstehen in den modernen Systemlandschaften folgende Probleme:

- Jede Schnittstelle, Verbindung und jeder Übergang stellt ein potentielles Risiko dar
- Die Distanz zu den öffentlichen „unsicheren“ Netzen wie das Internet wird stetig kleiner, weil die Systeme immer häufiger und stärker vernetzt werden
- Viele System sind heute auf das Internet „angewiesen“ und erhöhen somit das Cyberrisiko beträchtlich
- Technologien mit bekannten Schwachstellen, welche das unerwünschtes Cyberrisiko mitbringen, werden in der ICT-Umgebung eingesetzt
- Mangel an qualifiziertem Geschäftsmodellen oder dem Verständnis von Anforderungen, Abläufen und Prozessen in der ICS-Umgebung

(2) Die frühere Isolierung der ICS-Umfelder von externen (und historisch nicht vertrauenswürdigen) Netzen ermöglichte es, den Schutzgrad der ICS-Sicherheit für eine Bedrohung zu reduzieren, welche sich praktisch auf den physischen Zugriff auf eine Einrichtung oder eine Anlage beschränkt hat. Die meisten Datenübertragungen im ICS-Umfeld erforderten eine begrenzte Berechtigungs- oder Sicherheitsüberwachung, da Betriebsbefehle, Anweisungen und die Datenerfassung in einer geschlossenen Umgebung mit vertrauenswürdiger Datenkommunikation implementiert waren. Wenn jemand einen Befehl oder eine Anweisung über das Netzwerk sendet, geht man im Allgemeinen davon aus, dass dieser/diese ankommt und eine autorisierte Funktion ausführt, da nur autorisierte Benutzer Zugriff auf das System haben.

(3) Das Zusammenführen einer modernen IT-Architektur mit einem isolierten ICS-Umfeld, in dem möglicherweise keine Schutzmassnahmen gegen Cyberbedrohungen vorhanden sind, ist eine grosse Herausforderung. Eine einfache Vernetzung (d.h. Router und Switches) bietet die naheliegende Möglichkeit, Elemente bzw. Komponenten in Netzwerken miteinander zu verbinden. Ein unbefugter Zugriff durch einen Einzelnen könnte jedoch zu einem unbegrenzten Zugriff auf die gesamte ICS-Umgebung führen.

(4) Eine weitere grosse Herausforderung stellt der Einsatz von Standard IT-Mittel in der ICS-Umgebung dar. Bislang war das Patch-Management ausschliesslich auf den Lieferanten abgestimmt und ein Patchen der Systeme wurde nur wenn absolut nötig durchgeführt. Standard IT-Mittel benötigen permanente „Pflege“ von Anbietern, welche ihre Patch-Services im Web oder in einer Cloud zur Verfügung stellen. Somit nimmt die Distanz zu den öffentlichen Netzen bzw. zum Internet weiter ab und es tritt eine grössere Wahrscheinlichkeit auf, dass Schadsoftware in ICS-Umgebungen eingespielt wird.

a) Die verschiedene Sicherheitsbereiche (Areas, Zonen und Sektoren) in der ICS-Umgebung

(1) Die ICS-Umgebung und die damit involvierten anderen Umsysteme und Business-Umfelder müssen zum besseren Verständnis für die einzelnen Abläufe, Prozesse, Funktionen und Zuständigkeiten in verschiedene Bereiche (Areas, Zonen und Sektoren) aufgeteilt werden. Je nach Bereich liegen andere Verantwortlichkeiten, Zuständigkeiten und Anforderungen vor. Um eine sichere Umgebung schaffen zu können, müssen diese verschiedenen Bereiche betreffend Sicherheit zwingend aufeinander abgestimmt bzw. es muss ein gegenseitiges Verständnis betreffend Funktionen, Prozesse, Anforderungen und Schnittstellen geschaffen werden.

(2) Durch die geforderte und nötige Vernetzung bzw. den nötigen Datenaustausch zwischen den einzelnen Elementen ist es zwingend notwendig, dass die Grundsätze und Vorgaben aller Elemente klar definiert und bekannt sind. Somit ist es zwingend erforderlich, dass in der gesamten ICS-Umgebung wie auch in benachbarten Umgebungen eine ganzheitliche Betrachtung angewendet wird. Somit können die einzelnen Grenzen bzw. nötigen Übergänge identifiziert und genau beschrieben werden. Nur so kann ein bedarfsgerechter und ganzheitlicher Schutz der ICS-Umgebung gewährleistet werden.

b) Gemeinsame architektonische Bereiche

(1) Damit eine mehrschichtige Verteidigungsstrategie aufgebaut werden kann, muss man ein klares Verständnis dafür haben, wie die Umgebungen und Umfelder zusammenpassen und wie diese miteinander vernetzt sind. Das Aufteilen gemeinsamer Kontrollsystemarchitekturen in einzelne Bereiche kann dem Unternehmen bei der Schaffung klarer Grenzen helfen, um eine effektiv mehrschichtige Art der Verteidigung anzuwenden. Es muss klar werden, wie eine Netzwerk-Segmentierung vollzogen werden kann und somit zu definierende Schnittstellen entstehen. Dazu ist es unerlässlich, dass architektonische Area‘s, Zonen und Sektoren bestimmt werden.

(2) Die gesamte Umgebung kann grundsätzliche in drei administrative Sicherheitsbereiche bzw. Sicherheitsareas eingeteilt werden:

Sicherheitsbereiche / Areas	Erläuterung / Beschreibung
I. External Security Area	Sicherheitsarea von externen Partnern und externen Arbeitsumgebungen. Hier gelten die Sicherheitsanforderungen und -richtlinien der einzelnen involvierten Parteien.
II. Enterprise Business Security Area	Die Enterprise Security Area enthält Verbindungen mit dem Internet, den Unternehmens-Standorten und Backup- oder Remote-Einrichtungen (Internet DMZ Sector E5) sowie den Business-Netzwerken, der Unternehmenskommunikation, E-Mail-Servers, Domain Name System (DNS) Servers und IT-Business-Systemen (Sector E4). Aufgrund der Menge der Systeme und der Verbindungen gibt es in dieser Zone eine Vielzahl von Risiken. Aus Sicherheitssicht der ICS-Umgebung sollte man diese Area als nicht vertrauenswürdig betrachten.
III. Process Manufacturing Security Area	Sicherheitsarea des Produktions- und Steuerungsbereichs. Dieser Bereich wird von der OT (Operational Technologie) gebildet. Bereich mit der ICS-Umgebung und den versorgungskritischen Anlagen wie Verteileranlagen (Umspannwerke, Schaltanlagen, Unterwerke, Unterstationen) und Produktionsanlagen (Kraftwerke).

Tabelle 6 Übersicht über die drei administrativen Sicherheitsbereiche bzw. Sicherheitsarea‘s

(3) Dabei wird die Area für Produktion und Steuerung „Process Manufacturing Area“ in eine zentrale und dezentrale Zone aufgeteilt.

Unterbereiche / Zone	Erläuterung / Beschreibung
SCADA / Control Center Security Zone	Diese Sicherheitszone deckt die Sicherheitsanforderungen für zentrale SCADA Kontrollsysteme ab. Diese Sektoren (Sektor P2, 1 und E2) enthalten den Bereich der Verbindungen, in welchen eine überwiegende Mehrheit der Überwachung und Kontrolle über die gesamte Produktions- und Netzsteuerung stattfindet. Es ist ein kritischer Bereich für die Kontinuität und das Management eines Kontrollnetzes. Operative Unterstützungs- und Engineering-Management-Geräte befinden sich zusammen mit Datenerfassungsservern und Datenarchiven auch in diesen Sektoren. Die Kritikalität dieser Zonen ist sehr hoch. Risiken und Gefahren sind mit der direkten Anbindung an externe Systeme oder Netzwerke verbunden.
Supply Critical Plant Security Zone	Dieser Sicherheitsbereich bezieht sich auf die versorgungskritischen Anlagen wie Kraftwerke und Umspannwerke. Sie enthält Systeme, die für die lokale oder entfernte Bereichs- und Anlagensteuerung wie Feldleitgeräte, lokale Bedienelemente HMI‘s, lokale Controller und deren Steuerelemente und grundlegende Ein- / Ausgabegeräte wie Stellglieder und Sensoren verwendet werden. Die Kritikalität dieses Bereiches ist hoch, da diese Bereiche die physikalischen Endgeräte steuern. In einem modernen Steuerungssystem-Netzwerk werden diese Komponenten mit Unterstützung des TCP / IP-Protokolls (Transmission Control Protocol / Internet Protocol) und anderen üblichen Protokollen vernetzt. In diesem Bereich sind auch Schutzsysteme (SIS) enthalten, welche mit anderen Schutzsystemen von anderen Anlagen verbunden sein müssen. Idealerweise isoliert man die Schutzgeräte auf einem separaten Netz, damit sicher-gestellt werden kann, dass ein Eingriff auf das primäre ICS-Netzwerk keinen Einfluss auf die Schutzfunktionen hat. Oft ist es jedoch so, dass hier Kompromisse eingegangen werden müssen.

Tabelle 7 Zentraler und dezentraler Unterbereich der "Process Manufacturing Area"

(4) Jede dieser Zonen erfordert einen einzigartigen Sicherheitsfokus. Eine "Peel-the-Onion" -Analyse wird zeigen, dass ein Eindringling primär versuchen wird, in die zentralen Elemente der Sektoren 1, P2, P3, P4 und P5 (siehe Tabelle 12) einzudringen, weil er dort den grössten Schaden verursachen könnte. Somit muss diesen Bereichen die höchste Kritikalität zugewiesen werden bzw. diese Sektoren erfordern den grössten Schutz. Im Allgemeinen wird versucht, die vollständige Kontrolle über die Kerndienste und die Steuerung der entsprechenden Anlagen zu erlangen. Eine Manipulation der ICS-Informationsressourcen könnte ein Unternehmen in seiner Existenz bedrohen, wenn diese kritische Zone kompromittiert wird.

(5) In einem Angriffsszenario beginnt das Eindringen irgendwann ausserhalb der Kern- bzw. Kontrollsektoren. Der Angreifer versucht mit verschieden Mitteln immer tiefer und tiefer in die Architektur einzudringen. Gestufte und mehrschichtige Architekturen mit kontrollierten Übergängen und Schnittstellen

können das Eindringen in die Kernsektoren erheblich erschweren und sogar verhindern. Überwachte und kontrollierte Übergänge bieten den Systemadministratoren mehr Möglichkeiten, Informations- und Ressourcen-Kontrollen durchzuführen. Weiter können automatisierter Gegenmassnahmen implementiert werden, welche nicht zwingend die Geschäftstätigkeit beeinträchtigen.

(6) Die ortsabhängige Betrachtung ist direkt mit dem physischen Schutz der Elemente in Zusammenhang zu bringen. Die Ausprägung des physischen Schutzes inkl. des Zutrittsschutzes der einzelnen Elemente hat einen direkten Einfluss auf die zu treffenden Massnahmen. Durch eine perfekte Abgrenzung bzw. einen möglichst grossen Schutz können in diesem Bereich weitere Schutz- und Härtungsmassnahmen erheblich reduziert werden. Der Ansatz von einem möglichst grossen Grundschutz verfolgt dabei NERC. Somit muss in der Bewertung der Kritikalität diesem Schutz grosse Beachtung geschenkt werden.

c) Horizontale Segmentierung in funktionale Sektoren

(1) Die einzelnen Sektoren in der gesamten Systemlandschaft bilden die Abgrenzung betreffend der Funktion bzw. Funktionalität und den Aufgaben. Somit kann die gesamte Landschaft in folgende Sektoren aufgeteilt werden:

Sektoren	Beschreibung
External	Externe Arbeitsplätze und Systeme von Lieferanten, Herstellern und Supportern. Beinhaltet auch Home-Office und Remote-Zugänge mittels Web. In diesem Sektor befinden sich auch Cloud-Services.
Internet	Internet, öffentliche Netze und die dazugehörenden Provider bzw. Dienstanbieter und ihre Komponenten. Dabei ist die reine Datenübertragung über das Internet im Fokus.
Internet DMZ	Demilitarisierte Zone zur sicheren Trennung der verschiedenen Netze.
Enterprise Business	Sektor, in welchem sämtliche Business-Applikationen und -Services gehostet werden, wie zum Beispiel Office-Applikationen, GIS-, ERP- oder Energie-Management-Systeme.
DMZ SCADA OT/IT	Der demilitarisierte Sektor ist eine Pufferzone zwischen der IT- und OT-Welt, welche nach klar definierten Regeln einen sicheren Informationsaustausch ermöglicht.
SCADA / Control Center	Beinhaltet sämtliche zentralen Systeme, welche für die zentrale Steuerung und Überwachung des Stromnetzes und der Produktion notwendig sind.
SCADA Frontend DMZ	Demilitarisierte Zone zur sicheren Trennung der verschiedenen Netze. Terminierung der Anlagen-Gateway-Anbindungen. Typischerweise Frontendsysteme oder Prozesskopplungssysteme.
WAN	Wide Area Network. Switches, Router und Datenmultiplexer zur Übertragung der Datensignale zwischen den einzelnen Standorten. Beinhaltet auch das physische Medium wie LWL, Kupfer oder Funk.
Local HMI	Human-Machine Interface zur geschützten Bedienung der gesamten lokalen versorgungskritischen Anlage. Anbindung an das Gateway bzw. Verbindung zur Anlage erfolgt typischerweise über IEC 60870-5-104 und/oder IEC 61850.

Sektoren	Beschreibung
Controller	Feldkontroller für Prozess- und Schutztechnik, welche über eine TCP-/IP-Schnittstelle untereinander verbunden sind. Aktoren und Sensoren, welche direkt über eine TCP-/IP-Schnittstelle an einen Feldkontroller (Gateway der Stationsleittechnik) angebunden sind, typischerweise über IEC 60870-5-104 und/oder IEC 61850.
Field Devices	Aktoren und Sensoren, welche mittels lokalem Feldbus, herstellerspezifischem Bus oder analog an den Feldkontroller angeschlossen sind. Die Anbindung ist IP-less.
Outside Plant Business	Businessnahe Anwendungen in den versorgungskritischen Anlagen.

Tabelle 8 Horizontale Segmentierung nach funktionalen Sektoren

d) Einzelelemente bewerten / Bestimmung der Distanz zum Internet

(1) Durch die vermehrten Anforderungen an die Vernetzung und der Erhöhung der Komplexität ist es zwingend notwendig, dass die einzelnen Elemente in der Systemlandschaft bestimmt, bewertet, zusammengefasst bzw. gruppiert werden. Somit kann die gesamte Komplexität schematisch und logisch dargestellt werden. Um die einzelnen Elemente bewerten zu können, muss eine weitere Aufteilung derselben erfolgen.

(2) Wichtig ist, dass die Systemlandschaft vollumfänglich betrachtet wird. Alle Elemente, welche irgendwie mit einem Element der ICS-Umgebung kommuniziert oder in Verbindung gebracht werden kann, müssen in die Betrachtung einfliessen. Dies beinhaltet auch „Patch- und Update-Server“ von Lieferanten, Remotezugänge von Mitarbeitenden und Lieferanten usw. Die untenstehende Grafik zeigt eine idealtypische Konfiguration.

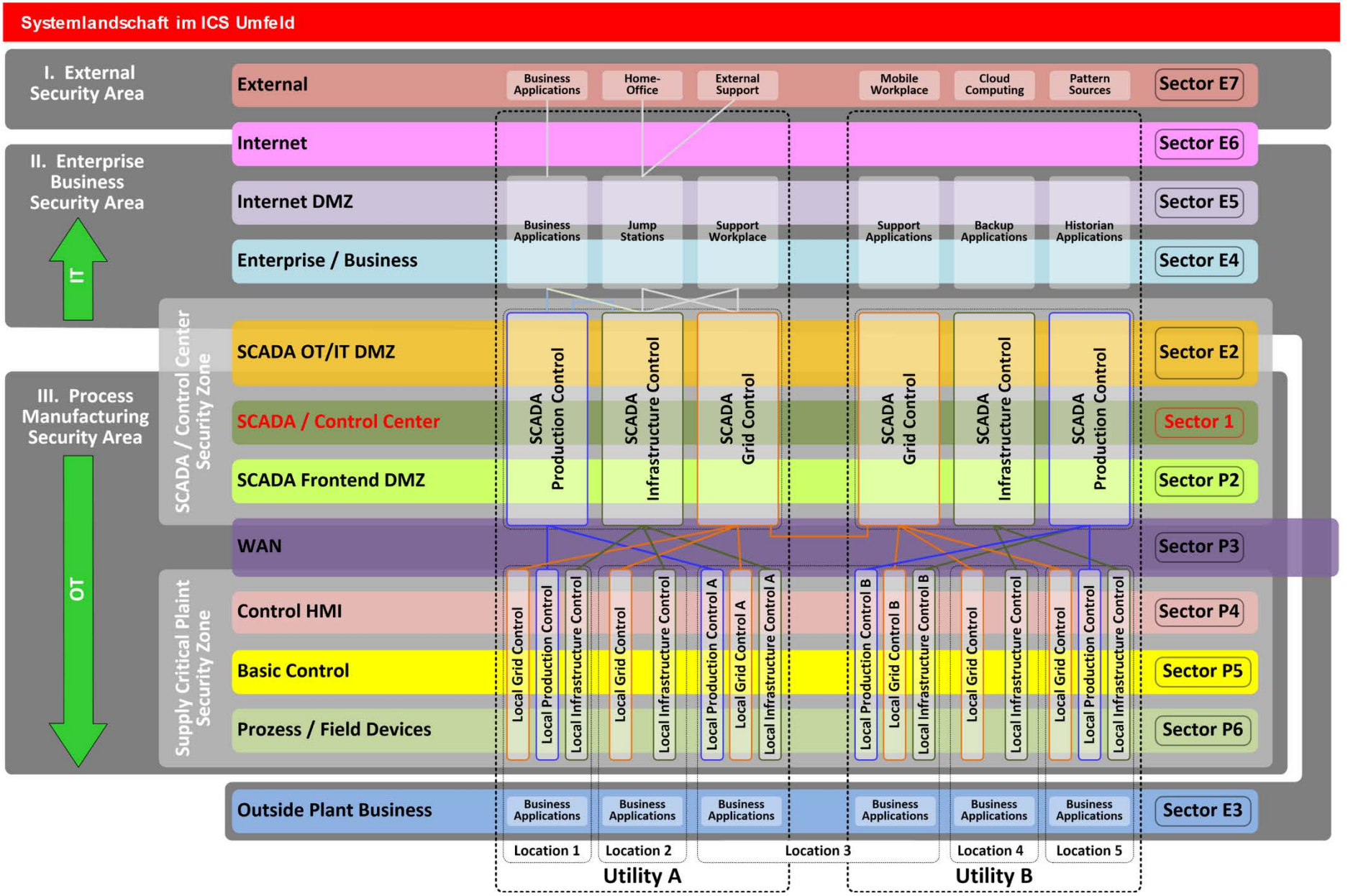

Abbildung 12 Systemlandschaft im ICS Umfeld

e) Beschreibung der einzelnen Sicherheitssektoren und Zuweisung der Kritikalität bzw. nötigen Distanz zum Internet

Sector	Bezeichnung	Kritikalität	Nötige Distanz zum Intern
E7	External	Out of scope	Die Distanz zum Internet bzw. Isolation gegenüber dem Internet wird durch die externe Organisation festgelegt. Gegenüber der ICS-Umgebung ist dieser Sektor als unsicher zu betrachten, auch wenn zwischen diesem Sektor und der ICS-Umgebung verschlüsselte und gehärtete Verbindungen aufgebaut werden.
E6	Internet	Out of scope	Das Internet gilt als die grösste Gefahrenquelle für potentielle Angriffe auf die ICS-Umgebung. Somit dürfen keine direkten Verbindungen in diesen Sektor möglich sein. In diesem Sektor dürfen sich keine Elemente befinden, welche direkten Zugang zur ICS-Umgebung hat. Verbindungen, welche über diesen Sektor geführt werden, müssen zwingend geschützt werden (Verfügbarkeit, Vertraulichkeit und Integrität der Informationen).
E5	Internet DMZ	Out of scope	In der Internet DMZ der Enterprise / Business IT werden alle Verbindungen vom und zum Internet terminiert. Hier kommen Proxy-und ALG-Systeme zum Einsatz. Weiter sollen Datenübertragungen in einer Daten-DMZ terminiert werden. In diesem Sektor muss die erste Prüfung auf Malware bzw. Schadsoftware stattfinden. Die Definition und tiefe der Prüfungen obliegt hier den Vorgaben der Business IT und ihren Systemen.
E4	Enterprise Business	Out of scope	Dieser Sektor obliegt den Vorgaben und Anforderungen betreffend Sicherheit und Schutz der Enterprise / Business IT. Gegenüber der ICS-Umgebung ist aber auch dieser Sektor als unsicher zu betrachten, da sich dieser immer näher zum Internet bewegt. Die Integration von Cloud-Services, ständiges Patchen und auch direkte Verbindung ins Internet über einen Webbrowser machen diesen Sektor aus Sicht ICS sehr unsicher. Auch erfolgen viele Angriffe auf die ICS-Umgebung über diesen Sektor, welcher als Zwischenstufe für einen Angriff genutzt wird.
E2	DMZ SCADA OT/IT	3	Dieser Sektor bildet einen sicheren Übergang zwischen den unsicheren Umgebungen der Enterprise / Business IT-Anwendungen und weiterführend auch die nötigen Verbindungen via Internet zu Drittparteien oder direkt ins Internet. Somit müssen in diesem Sektor alle möglichen Verbindungen terminiert werden. Nötige Fileübertragungen sind zu terminieren und die nötigen Prüfungen gegen potentielle Gefahren haben zu erfolgen. Somit befindet sich in diesem Sektor die letzte Möglichkeit, einen potentiellen Angriff oder das potentielle Einspielen einer Schadsoftware zu unterbinden.

Sector	Bezeichnung	Kritikalität	Nötige Distanz zum Intern
1	SCADA Control Center	5	Sektor mit den am meisten zu schützenden Elementen. In diesem Sektor dürfen nur Verbindungen aufgebaut werden, welche in der entsprechenden DMZ terminiert bzw. aufgebrochen wurden. Das Einspielen von Files bzw. der automatische Datenaustausch hat in jedem Fall nur über die vorgegebenen Wege mit den definierten Prüfungen und Terminierungen zu erfolgen. Dieser Sektor muss eine möglichst grosse Distanz zum Internet aufweisen.
P2	SCADA	4	In diesem Sektor erfolgt die Anbindung der versorgungkritischen Anlagen an das SCADA. Dabei wirken die Frontend- oder Prozesskopplungssysteme als Trennung zwischen den beiden Sicherheitsbereichen. Die grosse Herausforderung in diesem Sektor liegt im geschützten Übergang zwischen den versorgungskritischen Anlagen und dem SCADA. Dieser Übergang muss zwingend restriktiv und gut gehärtet werden. Es muss unterbunden werden, dass ein allfälliger Angreifer über diese Verbindung in das zentrale SCADA eindringen kann. Weiter ist eine Isolation zwischen den Verbindungen für die Anbindung der einzelnen versorgungskritischen Anlagen zu realisieren. Es muss sichergestellt sein, dass über diesen Sektor keine Verbindung zwischen den einzelnen versorgungskritischen Anlagen hergestellt werden kann.
P3	WAN	4	In diesem Sektor ist eine grosse Isolation der Verbindungen gefordert. In klassischen WAN-Netzen kann diese Isolation ohne grössere Probleme hergestellt werden. Die zu übertragenden Verbindungen haben verschlüsselt zu erfolgen. Dabei empfiehlt sich, dass die gesamte Datenübertragung ganzheitlich verschlüsselt wird, womit auch das Management der Elemente verschlüsselt übertragen wird. Es muss verhindert werden, dass zwischen den einzelnen Datenverbindungen Übergänge entstehen. Die Isolation ist dabei über das gesamte WAN zu betrachten.
P4	Local HMI	3	Dieser Sektor stellt in einer versorgungkritischen Anlage besondere Anforderungen an den Schutz der Elemente, da hier das menschliche Element grossen Einfluss auf das Gesamtsystem hat. Mit der Schaffung eines eigenen Sektors und der Bildung der nötigen Übergänge können Vorgänge überwacht, kontrolliert und nötigenfalls verhindert werden.
P5	Controller	3	In diesem Sektor befindet sich das lokale Prozess-LAN mit den dazugehörenden Controllern. Eine funktionsspezifische Segmentierung ist anzustreben. Die Verbindungen in andere Netze sind einzuschränken und so auszulegen, dass diese überwacht, kontrolliert und nötigenfalls verhindert werden können.

Sector	Bezeichnung	Kritikalität	Nötige Distanz zum Intern
P6	Field Devices	2	In diesem Sektor können sich Elemente befinden, welche über einen schlechten oder nicht genügenden physischen Schutz verfügen (Freiluftanlage, Aussenkasten usw.). Somit haben die Anbindungen an die Controller oder die lokale Prozesstechnik über Verbindungen zu erfolgen, welche nicht direkt mit dem lokalen Prozess-LAN verbunden sind. Hier sollen IP-lose Verbindungen oder Verbindungen über isolierte und abgeschottete Netze erfolgen. Es darf kein IP-Übergang zum Prozessnetzwerk vorhanden sein.
E3	Outside Plant Business	Out of Scope	Dieser Sektor bildet den Bereich für businessnahe Anwendungen in den versorgungkritischen Anlagen. Er ist isoliert zu den anderen Sektoren zu betreiben. Die Schnittstelle bzw. der Übergang hat über den Sektor P3 WAN an den Enterprise Business Sektor E4 zu erfolgen. Nötige Verbindungen müssen immer über den Sektor E4 geführt werden. Die Anforderungen an die Sicherheit obliegt hier im Bereich Enterprise IT.

Tabelle 9 Kritikalität der einzelnen Sicherheitssektoren

(1) Wie bei der Kritikalität, wird dabei nach IEC 62443-3-2 wie folgt unterschieden:

Beurteilung der Kritikalität nach IEC 62443-3-2				
Trivial	Minor	Moderate	Major	Critical
1 ●	2 ●	3 ●	4 ●	5 ●

Tabelle 10 Beurteilung der Kritikalität nach IEC 62443-3-2

(2) Somit stellt in dieser Betrachtung der Sektor 1 den Bereich dar, welche den höchsten Schutzbedarf darstellt (siehe Spalte Kritikalität, Tabelle 9).

f) Vertikale Gruppierung nach Standorten, Zuständigkeiten, Funktionen und Prozessen

(1) Da versorgungskritische Anlagen mit verschiedenen funktions- und prozessspezifischen Systemen gesteuert und überwacht werden, für welche auch noch verschiedene Bereiche im Unternehmen oder verschiedene Unternehmen verantwortlich sind, ist eine vertikale Gruppierung der Systemlandschaft erforderlich.

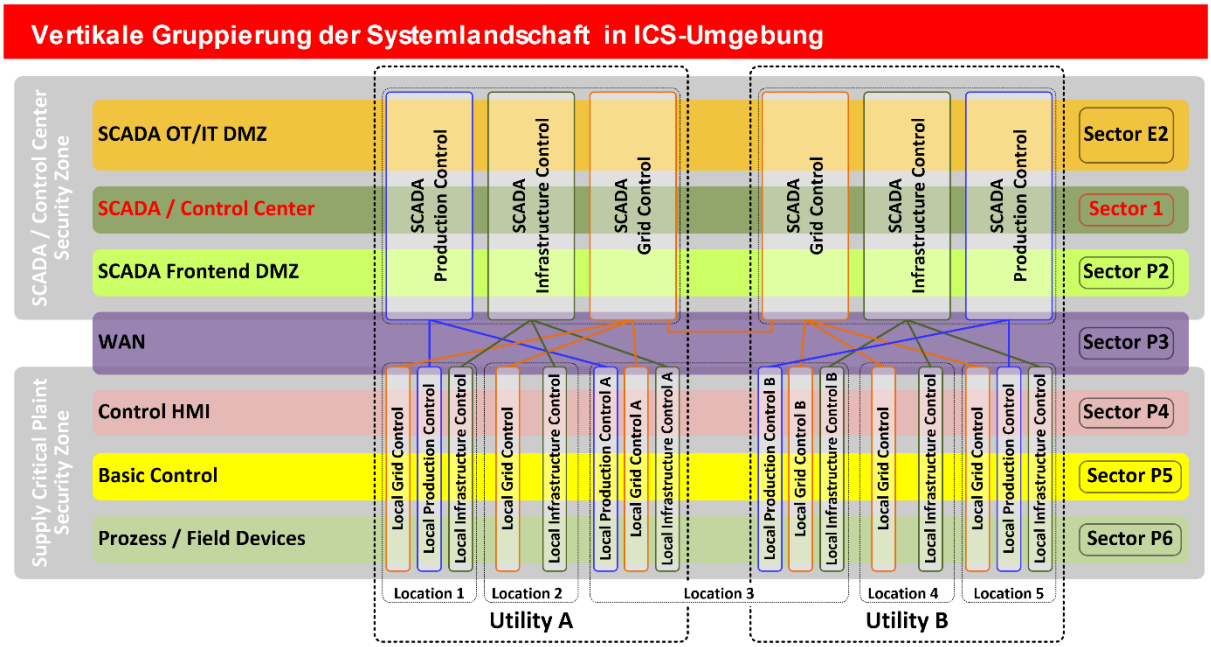

Abbildung 13 Vertikale Gruppierung der Systemlandschaft in ICS-Umgebung

(2) Gemäss Bild oben ist eine klare Gruppierung und Abgrenzung zwischen den verschiedenen funktionalen und organisatorischen Elementen erforderlich. Eine Vernetzung der einzelnen Elemente kann zu einem erhöhten Risiko und zu einer grossen Verwundbarkeit führen. Übergänge zwischen den verschiedenen Elementen sind zu definieren und mit dem nötigen Schutz zu versehen. Durch einen einzigen ungeschützten Übergang werden zwei funktionale Netze zusammengeschlossen und somit geschwächt.

2.7.2 Elemente in Netzwerkzonen gruppieren

(1) Grundsätzlich ist jedes Element in der ICS-Umgebung zu untersuchen und genauer zu betrachten. Dabei ist zu identifizieren, welche Elemente mit welchen anderen Elementen seine Daten austauschen muss. Dazu sind die Elemente ganzheitlich zu untersuchen, d.h. es müssen alle möglichen Verbindungen von und zum Element bekannt sein. Dabei ist für alle Elemente eine Inventarisierung auszuführen. Anhand einer Matrix kann schlussendlich festgestellt werden, wie die einzelnen Elemente gruppiert, segmentiert oder isoliert werden müssen. Dabei muss beachtet werden, welchen physischen Schutz das jeweilige Element aufweist, welche Arten von Kommunikationsschnittstellen vorhanden sind (z.B. Ethernet, Seriell, Wireless etc.) und wie diese Systeme gemanagt werden (einspielen von Updates, auslesen von Logfiles, ändern von Konfigurationen). In erste Linie sind al-

le Elemente in der ICS-Umgebung nach dem Prinzip „nur was bekannt und nötig“ zu härten (weiterführende Informationen sind unter dem Punkt Systeme- und Komponenten-Sicherheit aufgeführt).

(2) Die Gruppierung und Segmentierung hat nach folgenden Faktoren und Eigenschaften zu erfolgen:

- Welche Elemente verfügen über welchen physischen Schutz; wo ist ein guter physischer Schutz vorhanden, damit ein unberechtigter physischer Zugriff auf das System unterbunden werden kann?
- Welche Elemente haben eine zentrale Funktion; wo kann der grösste potentielle Schaden durch einen Angreifer oder eine Schadsoftware entstehen?
- Welche Elemente sind gehärtet; welcher Schutz ist für potentielle Fehlmanipulationen und gegen das Eindringen von Schadsoftware vorhanden?
- Welche Elemente müssen mit welchen anderen Elementen für ihre Funktion Verbindungen aufbauen können?
- Wo ist es sinnvoll, dass Übergänge zwischen Elementen geschaffen werden, so dass Sicherheitsprüfungen, Isolationen und Einschränkungen vollzogen werden können?
- Welche Elemente können mit Prüf-, Isolations- und Einschränkungstools versehen werden?
- Welche Elemente bilden zentrale und somit kritische Punkte, wo potentielle Gefahr besteht, dass das Gesamtsystem verwundbar ist?
- Welche Elemente haben welchen Patch- und Updatezyklus?

a) Gruppierungen in der Sicherheitszone SCADA / Control Center und Erstellen der internen Verbindungsmatrix

(1) Die Sicherheitszone SCADA / Control Center stellt die grössten Anforderungen an die Sicherheit. Hier kann ein potentieller Angreifer oder eine potentielle Schadsoftware die grössten Wirkungen erzielen. Bei der Bildung von Gruppierungen und Segmentierungen müssen verschiedene Faktoren berücksichtigt werden. Wichtig ist, dass die Umgebung in dieser Zone vollumfänglich betrachtet wird.

(2) Die Gruppierung und Segmentierung kann gemäss Abbildung 12 erfolgen, wobei es sich um ein Beispiel handelt. Die Anordnungen können dabei natürlich variieren und sind nach den jeweiligen Vorgaben und Analysen durchzuführen.

(3) Nach der Gruppierung und Segmentierung ist es sinnvoll, dass für jeden Sektor eine lokale Verbindungsmatrix erstellt wird. Hier müssen alle Verbindungen, welche in den einzelnen Gruppen und Segmenten auftreten, aufgeführt werden.

Beispiel für interne Verbindungsmatrix im Sector E2 SCADA DMZ OT/IT

von \ nach	File Server 1	File Server 2	Jump Server 1	Jump Server 2	Historian Server	AV- und Patch-Server	Secure File Server
File Server 1	x	tcp/22 tcp/443	tcp/22 tcp/443	tcp/22 tcp/443	Nein	Nein	Nein
File Server 2	tcp/22 tcp/443	x	tcp/22 tcp/443	tcp/22 tcp/443	Nein	Nein	Nein
Jump Server 1	tcp/22 tcp/443	tcp/22 tcp/443	x	tcp/22 tcp/443	tcp/22 tcp/443	tcp/22 tcp/443	tcp/22 tcp/443
Jump Server 2	tcp/22 tcp/443	tcp/22 tcp/443	tcp/22 tcp/443	x	tcp/22 tcp/443	tcp/22 tcp/443	tcp/22 tcp/443
Historian Server	tcp/22 tcp/443	tcp/22 tcp/443	Nein	Nein	x	tcp/22 tcp/443	Nein
AV- und Patch-Server	Nein	Nein	Nein	Nein	Nein	x	Nein
Secure File Server	Nein	Nein	Nein	Nein	Nein	Nein	x

Abbildung 14 Beispiel für interne Verbindungsmatrix im Sector E2 SCADA DMZ OT/IT

(4) Gemäss Beispiel oben muss eine Inventarisierung der nötigen Verbindungen zwischen den einzelnen Elementen innerhalb des jeweiligen Sektors erfolgen. Jede nötige Verbindung muss beschrieben werden, ihre Funktion muss bekannt sein. Dabei ist zwingend darauf zu achten, dass immer sichere Protokolle verwendet werden. Weiter sind Protokolle und Datenstrukturen zu verwenden, welche durch nötige Kontroll- bzw. Überwachungskomponenten wie ALF oder ALG (Application Layer Firewall oder Application Layer Gateway) aufgebrochen bzw. terminiert und die zu übertragenden Daten auf ihren Inhalte geprüft werden können. Diese Verbindungsmatrix muss natürlich gemäss horizontaler Betrachtung für jede ICS-Umgebung wie Grid Control, Production Control und Infrastructure Control erstellt werden. Sektor übergreifende Verbindungen werden unter diesem Punkt bewusst noch nicht beschrieben.

b) Gruppierungen im Bereich versorgungskritische Anlagen

(1) Wie im vorhergehenden Punkt beschrieben, muss auch für den Bereich der versorgungskritischen Anlagen pro Sektor eine Verbindungsmatrix erstellt werden. Auch werden die nötigen Verbindungen aufgezeigt. Die Betrachtung beschränkt sich auf jeden Sektor. In der Verbindungsmatrix sollen nicht nur TCP/IP- oder UDP/IP-Verbindungen aufgeführt werden, sondern es müssen auch IP-less-Verbindungen oder standartspezifische Verbindungen (z.B. Goose bei IEC61850) beschrieben und eingepflegt werden. Nur so erhält man eine abschliessende und vollumfängliche Betrachtung innerhalb des Sektors.

Interne Verbindungsmatrix für die den Sektor P5 Basic Control in einer versorgungskritischen Anlage

von \ nach		Gateway Direction Field	Gateway Direction Protection	Gateway Direction HMI	Field Device 1 Direction Field	Field Device 2 Direction Field	Field Controller 1 Direction Field	Field Controller 2 Direction Field	Field Sensor 1 Direction Field	Protection Sensor 1 Direction Protection	Protection Sensor 2 Direction Protection	Protection Field Controller 1 Direction Protection	Protection Field Controller 2 Direction Protection	Local HMI Direction HMI
Gateway	Direction Field	x	Nein	Nein	tcp/102 udp/123	tcp/102 udp/123	tcp/102 udp/123	tcp/102 udp/123	tcp/102 udp/123	Nein	Nein	Nein	Nein	Nein
Gateway	Direction Protection	Nein	x	Nein	Nein	Nein	Nein	Nein	Nein	tcp/102 udp/123	tcp/102 udp/123	tcp/102 udp/123	tcp/102 udp/123	Nein
Gateway	Direction HMI	Nein	Nein	x	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	tcp/102 udp/123
Field Device 1	Direction Field	tcp/102 udp/123	Nein	Nein	x	tcp/102 udp/123	tcp/102 udp/123	tcp/102 udp/123	tcp/102 udp/123	Nein	Nein	Nein	Nein	Nein
Field Device 2	Direction Field	tcp/102 udp/123	Nein	Nein	tcp/102 udp/123	x	tcp/102 udp/123	tcp/102 udp/123	tcp/102 udp/123	Nein	Nein	Nein	Nein	Nein
Field Controller 1	Direction Field	tcp/102 udp/123	Nein	Nein	tcp/102 udp/123	tcp/102 udp/123	x	tcp/102 udp/123	tcp/102 udp/123	Nein	Nein	Nein	Nein	Nein
Field Controller 2	Direction Field	tcp/102 udp/123	Nein	Nein	tcp/102 udp/123	tcp/102 udp/123	tcp/102 udp/123	x	tcp/102 udp/123	Nein	Nein	Nein	Nein	Nein
Field Sensor 1	Direction Field	tcp/102 udp/123	Nein	Nein	tcp/102 udp/123	tcp/102 udp/123	tcp/102 udp/123	tcp/102 udp/123	x	Nein	Nein	Nein	Nein	Nein
Protection Sensor 1	Direction Protection	Nein	tcp/102 udp/123	Nein	Nein	Nein	Nein	Nein	Nein	x	tcp/102 Goose	tcp/102 Goose	tcp/102 Goose	Nein
Protection Sensor 2	Direction Protection	Nein	tcp/102 udp/123	Nein	Nein	Nein	Nein	Nein	Nein	tcp/102 Goose	x	tcp/102 Goose	tcp/102 Goose	Nein
Protection Field Controller 1	Direction Protection	Nein	tcp/102 udp/123	Nein	Nein	Nein	Nein	Nein	Nein	tcp/102 Goose	tcp/102 Goose	x	tcp/102 Goose	Nein
Protection Field Controller 2	Direction Protection	Nein	tcp/102 udp/123	Nein	Nein	Nein	Nein	Nein	Nein	tcp/102 Goose	tcp/102 Goose	tcp/102 Goose	x	Nein
Local HMI	Direction HMI	Nein	Nein	tcp/102 udp/123	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	x

Abbildung 15 Verbindungsmatrix für die den Sektor P5 in einer versorgungskritischen Anlage

2.7.3 Netzwerkmanagement, Inventarisierung und Performance

(1) Das Netzwerkmanagement bildet die Voraussetzung für den sicheren und zuverlässigen Betrieb eines Netzes. Bedingt durch die Komplexität grösserer Netze müssen diverse Kontroll-, Überwachungs-, und Wegekonfigurations-Funktionen mittels eines Netzwerkmanagementsystems ausgeführt werden. Zu den Aufgaben des Netzwerkmanagements gehören daher u.a. das Sammeln von Informationen über die Nutzung des Netzes durch die angeschlossenen Elemente, die Erstellung von Berichten und Statistiken für die Planung, den Betrieb, den Ausfall und die Wartung, die Konfiguration des Netzes und damit verbundene Konfigurationsänderungen, die Leistungs-, Ereignis- und Fehlerüberwachung. In Verbindung mit der offenen Kommunikation legte die internationale Standardisierungs-Organisation (ISO) fünf Funktionsbereiche für das Netzwerkmanagement fest: Fehlermanagement, Leistungsmanagement, Konfigurationsmanagement, Abrechnungsmanagement und Sicherheitsmanagement.

- Das Fehlermanagement fasst alle Funktionen zusammen, die zur Fehlerprophylaxe, Fehlererkennung und Fehlerbehebung im Netzwerk benutzt werden können.
- Das Konfigurationsmanagement enthält Hilfsmittel und Funktionen zur Planung, Erweiterung und Änderung der Konfiguration sowie zur Pflege der Konfigurationsinformationen.
- Das Leistungsmanagement stellt Hilfsmittel und Werkzeuge zur Messung und Verbesserung des Leistungsverhaltens des Netzwerks, zum so genannten Netztuning bereit.
- Das Abrechnungsmanagement enthält Mittel zur ordnungsgemässen Abwicklung der Benutzung des Netzwerks, wie Zugangsverwaltung, Verbraucherkontrolle, Abrechnungshilfen sowie Informationsdienste.
- Das Sicherheitsmanagement ist verantwortlich für die Überwachung der Zugriffsberechtigungen auf Netze, LAN-Segmente, Elemente, Dienste und weitere Ressourcen.

Inventarisierung des Netzwerks

(1) Vor dem „managen“ des Netzwerkes steht zunächst die Erfassung sämtlicher Elemente und Komponenten im Netzwerk. Diese Aufgabe kann von einer sogenannten Inventarisierungssoftware automatisiert übernommen werden. Sie zeichnet anhand aktiver IP-Adressen über den PING-Befehl nicht nur die Existenz diverser Geräte auf, sondern hinterlegen zu jedem Bestandteil zusätzlich verschiedene Informationen in einer Datenbank. In Bezug auf einen Client-Rechner sind dies etwa Daten zur verbauten Hardware, zum Betriebssystem aber auch zur auf dem PC installierten Software. Ein umfassender Überblick zu den installierten Programmen ist nicht zuletzt für ein reibungsloses Lizenzmanagement sehr wichtig.

(2) Nicht nur die Inventarisierung der Netzwerkelemente und angeschlossen Endgeräte ist wichtig, auch die Inventarisierung von möglichen und nötigen Verbindungen (z.B. TCP-IP-Verbindungen) im gesamten Netzwerk zwischen den einzelnen Elementen muss erfasst und inventarisiert werden. Nur so kann sichergestellt werden, dass das Wirken in einem Netzwerk auch verstanden wird. Diese Inventarisierungen bilden dabei auch die Grundlagen für nötige Sicherheitselemente. Einmalige Netzwerkerfassungen sind im Sinne einer Bestandsaufnahme sinnvoll, aber immer nur eine Momentaufnahme. Daher empfiehlt es sich, die Netzwerkaufnahme kontinuierlich durchzuführen bzw. bestehende Netzwerkinventarisierungen müssen stetig auf den neusten Stand gehalten werden.

Performance sicherstellen

(1) In modernen Netzwerken, über die ausser dem reinen Datenverkehr zusätzlich oft die Sprachkommunikation (VoIP) sowie Videokonferenzen laufen, ist es nicht immer leicht, die erforderliche Leistung zu jedem Zeitpunkt zur Verfügung zu stellen. Gerade VoIP reagiert im Vergleich zu anderen Anwendungen im Netzwerk extrem empfindlich auf Verzögerungen und Paketverluste. Aus diesem Grund ist es notwendig, sich bereits vor der Installation mit den spezifischen VoIP-Parametern auseinanderzusetzen, um in der Praxis die richtigen Messdaten erheben zu können. Doch um die VoIP-Performance eines Unternehmensnetzwerks feststellen zu können, müssen vor der geplanten Beschaffung und Installation von VoIP/UC-Komponenten wie Telefone, Server und Gateways die Tauglichkeit des Netzwerkes geprüft werden. Die kann mittels VoIP-Simulatoren und -Analysatoren erfolgen. Diese können tausende von Anwendern und deren Telefonverhalten nachbilden und Schritt für Schritt in das Netzwerk einzuspielen werden.

(2) Oft sind Anwendungen im Bereich SCADA und kritischer Infrastruktur auf „Echtzeitdaten“ angewiesen. Die Performance des Netzwerkes muss deshalb für diese Anwendungen gebaut oder getunt werden. Dabei spielen auch Faktoren wie Jitter und Laufzeiten eine grosse Rolle. Es ist dabei zwingend darauf zu achten, dass auch bei grosser Auslastung des Netzwerkes durch andere Anwendungen wie Video und VoIP die geforderten Parameter betreffen Echtzeit, Jitter und Laufzeiten jederzeit eingehalten werden müssen. Falls das vorhanden Netzwerk Engpässe aufweisen kann, ist die Einführung von Priorisierungen ein guter Weg sein.

(3) Skalierbarkeit ist heute eine der wichtigsten Eigenschaften einer IT-Infrastruktur. Sie verspricht etwa, die Verfügbarkeit von Applikationen und Diensten auch bei einem deutlichen Zuwachs an Netzwerkverkehr sicherzustellen. Doch herauszufinden, wie skalierbar das eigene Netz ist oder einfach nur zu erfahren, wo im Falle einer hohen Belastung der Flaschenhals sitzt, ist äusserst komplex. In der Praxis nutzen IT-Verantwortliche dazu Stresstests, die durch Werkzeuge unterstützt werden, die eine künstliche Last im LAN erzeugen. Doch allein damit, unglaublich grosse Mengen an Bits und Bytes in die Leitungen zu pumpen, ist es nicht getan, die Ergebnisse solcher Tests sind nur in Verbindung mit den richtigen organisatorischen Massnahmen im Umfeld wirklich aussagekräftig.

Netzwerk Monitoring

(1) Die Überwachung des Netzwerks und einzelner Komponenten, das zur Erkennung und Behebung von Fehlern überaus wichtige Netzwerk Monitoring, erfolgt meist über die Protokolle SNMP (Simple Network Management Protocol) oder WMI (Windows Management Instrumentation). Ausserdem ist die Überwachung durch Software-Agenten eine weit verbreitete Methode, um sich ein Bild vom Zustand einer Netzwerkkomponente zu machen. Neben dem Verwalten und Überwachen der Komponenten beinhaltet Netzwerkmanagement auch die Kontrolle von Servern und bereitgestellten Diensten (Webserver, Mailserver etc.).

(2) Für das Netzwerk Monitoring greifen Administratoren oft auf spezielle Software zurück. Als bekanntester Vertretern im Open Source-Seite gilt Nagios. Da das immer noch weit verbreitete Unix-Programm aber kaum mehr weiterentwickelt wird und zudem viele Funktionen nur über Plug-Ins verfügbar sind, kommen immer häufiger die relativ jungen Werkzeuge OpenNMS und Shinken zum Einsatz. Während letzteres auf Nagios aufbaut und seine Überwachungsfunktionen ebenso wie das Vorbild mittels diverser Konfigurationsdateien definiert, verfolgt OpenNMS einen ganzheitlicheren Ansatz und beherrscht viele Aufgaben bereits in den Grundeinstellungen. Cacti, MRTG oder Zabbix sind weitere Exemplare von freien Lösungen zum Netzwerkmanagement.

(3) Ebenso sind auf dem Markt diverse kommerzielle Produkte zum Netzwerk Monitoring erhältlich. Hier sind zum Beispiel mit HP Open View, IBM Tivoli oder dem Microsoft Operations Manager die Produkte der grossen IT-Anbieter zu nennen. Doch auch kleinere Unternehmen wie etwa Ipswitch oder Paessler bietet mit WhatsUp Gold oder PRTG Network Monitor eigene Produkte ab.

(4) Wichtig ist es, dass auch beim Netzwerkmonitoring die nötigen Funktionen und Anforderungen betreffend Sicherheit angewendet werden. Ein Netzwerkmanagement zusammen mit dem Netzwerk bietet für einen potentiellen Angreifer eine ideale Möglichkeit, Manipulationen und Aktionen in versorgungkritischen Anlagen vorzunehmen. Die Verwendung von SNMPv3 (Simple Network Management Protocol Version 3) und SSH-Verbindungen muss zwingend implementiert werden. Bei Verwendung von anderen und proprietären Protokollen ist zwingend darauf zu achten, dass die Integrität und Schutz der Daten gewährleistet ist. Verschlüsselungs- und andere Schutz-Techniken sind zwingend anzuwenden.

VLAN und VPN

(1) Das Management eines Netzwerks muss in eigenen abgeschotteten Netzen erfolgen und wird durch das Bilden eines VLANs erleichtert. Dieses Virtual Local Area Network teilt Geräte in einem lokalen Netzwerk in Gruppen ein, zwischen denen Verbindungen grundsätzlich unterbunden sind, aber über eine Firewall oder ALG gezielt ermöglicht werden können. Ein Virtual Private Network (VPN) spielt immer dann eine Rolle, wenn es gilt, ein nach aussen abgeschirmtes Netzwerk sicher über fremde oder nicht vertrauenswürdige Netze bereitzustellen.

2.8 Netzwerkperimeter Sicherheit

(1) Sobald ein Unternehmen eine robuste Netzwerkarchitektur entwickelt und implementiert hat, sollte auch die Sicherheitsarchitektur für das Netzwerk und die Systeme implementiert werden. Die Sicherheitsarchitektur umfasst die spezifischen Kontrollen und ihre strategische Platzierung von Detektoren und Proben innerhalb des Netzwerks oder Systeme, um die verschiedenen Schichten der Sicherheit-Defense-in-Depth zu etablieren. Netzwerkdiagramme, Verbindungsmatrizen und Informationsflussdiagramme, die alle Systeme und ihre Verschaltungen mit dem physischen Inventar koppeln, sind zwingend notwendig, um ein betriebliches Verständnis der Informationsflüsse und nötigen Verbindungen innerhalb des Netzwerkes zu erhalten. Durch die Bildung Arealen, Zonen und Sektoren und dem Überlagern der Schutzstufen für jedes System oder Subsystem, das während der Inventuraktivitäten zugewiesen wurde, kann bestimmt werden, welche Steuer- und Überwachungselemente eingerichtet wurden, um das System zu schützen, ohne die Leistung zu beeinträchtigen.

(2) Systemverantwortliche müssen die Anwendung von Sicherheitskontrollen im Netzwerk, System, Anwendung und physischen Schichten berücksichtigen, um die Informationssicherheit zu gewährleisten. Dazu gehören Richtlinien- und Sicherheitsmanagement, Anwendungssicherheit, Datensicherheit, Plattformsicherheit, Netzwerk- und Perimeter-Sicherheit, physische Sicherheit und Benutzersicherheit. Die Sicherheitsarchitektur besteht darin, dass alle Verteidigungsmechanismen und -kontrollen zusammenkommen und die Netzwerkarchitektur überlagern. Die Sicherheitsarchitektur definiert, wo Defense-in-Depth-Massnahmen im gesamten Unternehmen angewendet werden. NIST 800-82, "Leitfaden für industrielle Steuerungssysteme (ICS) Security", bietet dazu eine unternehmensweite übergelagerte ICS-Sicherheitskontrolle auf der Grundlage der NIST 800-53, "Security and Privacy Controls für Federal Information Systems und Unternehmen“.

2.8.1 Grundsätze für sichere Netzwerkzugänge und Zonenübergänge

(1) In der ICS-Umgebung entstehen durch die integrierten Architekturen und die Vernetzung mit anderen Umgebungen und Umfeldern Zugangsmöglichkeiten zu kritischen Systemen. Die Eigenschaften solcher Architekturen erfordern den Austausch von Daten aus unterschiedlichen Informationsquellen, was von einem potentiellen Eindringling ausgenutzt werden könnte. IEC 62443-3-2; Sicherheit für Industrielle Automatisierungs- und Steuerungssysteme - Security Risk Assessment and System Design umschreibt diese Problematik.

(2) Folgende Grundsätze sind umzusetzen:

- Die Gruppierung und Segmentierung hat immer dann zu erfolgen, wenn Verbindungen zwischen den OT-Elementen einen erhöhten Schutzbedarf oder Kritikalität bzw. eine nötige Kontrolle aufweisen müssen. Es müssen somit prüf- und kontrollierbare Übergänge bzw. Schnittstellen geschaffen werden.
- Es muss sichergestellt sein, dass jeder Verbindungsaufbau in die OT-Umgebung aus dem Sector und Element erfolgen muss, welcher einen höheren Schutzbedarf bzw. Kritikalität aufweist.
- Auch innerhalb der Sektoren müssen nach Möglichkeit sichere Protokolle verwendet werden.
- Die Implementation von MAC-Authentisierung ist auf den OT-Netzwerkkomponenten anzuwenden (Switche und Router)
- Die Implementation von Flusskontrollen bzw. Verbindungsfreigaben auf Layer 3 und 4 mittels Zugriffskontrolllisten in den Netzwerkkomponenten ist anzuwenden.
- Unautorisierte Zugriffe und Zugriffsversuche sollen erkannt, aufgezeichnet, alarmiert und eskaliert werden
- Nicht benutze Ports (Access und Trunk) müssen auf allen OT-Elementen (Netzwerk und Host) deaktiviert werden
- Radius- und Kontrollserver für Systeme in der OT-Umgebung für kritische Infrastrukturen in der Stromversorgung können ein zentrales Risiko darstellen. Somit ist die Einführung und Verwendung genau zu überprüfen und sehr restriktive zu halten. Vernetzung mit System aus der IT-Umgebung ist zu unterbinden.
- Kontrollen der physischen Zugriffe, indem Konsolenanschlusskabel entfernt werden, oder nur kennwortgeschützte Konsole eingeführt werden oder einen virtuellen Terminalzugriff mit bestimmten Zeitlimits und eingeschränkten Zugriffsrichtlinien realisieren.
- Verwenden einer Eins-zu-Eins-Beziehung zwischen Subnetzen und VLANs. Dies erfordert die Verwendung einer Firewall, eines Routers oder mehrschichtigen Switches, um mehrere VLANs zu verbinden. Viele Router und Firewalls unterstützen getaggte Frames, so dass eine einzelne physikalische Schnittstelle zwischen mehreren logischen Netzwerken führen kann.
- Es wird empfohlen, die Zugriffe auf die VLANS mittels Firewall zu steuern. Erstellen rollenbasierten Benutzerkonten für alle VLANs. Erstellen einer Zugriffsliste, um den Zugriff auf telnet / secure shell (SSH) von bestimmten Netzwerken und Hosts zu beschränken
- Erstellen und Anwenden von Layer 2 (L2) Zugriffssteuerungslisten (ACLs) und virtuellen ACLs, die die direkte Kommunikation bei L2 zwischen einem potentiellen Angreifer und dem angegriffenen Gerät blockieren. Implementation von mehr Intelligenz in das OT-Netzwerk, so dass weitergeleitet Address Resolution Protocol (ARP) -Pakete ihre Identität und Korrektheit überprüft werden können
- Verwendung von privaten VLANs, um Netzwerke vor unerwünschten Zugriffen von nicht vertrauenswürdigen Geräten zu schützen.

- Aktivierung von Port-Sicherheit in den Elementen des OT-Netzwerkes
- Implementation von Broadcast- und Multicast-Flusskontrollen und Begrenzungen auf den jeweiligen Ports der Elemente im OT-Netzwerk
- Isolation des Managements der OT-Netzwerkkomponenten in ein isoliertes VLAN oder Implementation von Out-of-Band-Management anstelle des In-Band-Management.
- Beschränkung der Anzahl Media Access Control (MAC) Adressen, die von einem einzelnen Port verwendet werden, sodass die Gerätekennung für ein Gerät direkt mit dem Ursprungsport verbunden ist. Deaktivierung unbenutzter Ports und Zuordnen der deaktivierten Ports einem nicht verwendeten VLAN.
- Erstellen und Anwenden von L3-ACLs nach IP-Adresse (empfohlen für die meisten statischen drahtgebundenen Netzwerke), MAC-Adressenfilterung, Portzuweisung, dynamische Zuweisung (empfohlen für die meisten drahtlosen Netzwerke und gemeinsame Switch-Port-Netzwerke), Protokolle und Anwendungen. Standardmässiges Behandeln von nur bekannten und vertrauenswürdigen Ports als solche und konfigurieren aller anderen Ports als nicht vertrauenswürdig. Dies verhindert, dass angeschlossene Geräte die QoS-Werte unangemessen manipulieren.
- Deaktivierung von VTP (VLAN Trunking Protokoll) / MVRP (Multiple VLAN Registration Protokoll) und DTP (Dynamic Trunking Protokoll) auf allen nicht vertrauenswürdigen Ports. Dies ist eine bewährte Methode zur Verwendung von VLANs innerhalb von OT-Netzwerken, da sie mögliche unerwünschte Protokollinteraktionen in den Netzwerk-VLAN-Konfigurationen begrenzen (oder sogar verhindern) kann. Diese Vorsichtsmassnahme kann auch das Risiko einschränken oder verhindern, dass ein Administratorfehler das gesamte Netzwerk weiterleitet.

Empfohlene sichere Netzwerkarchitektur

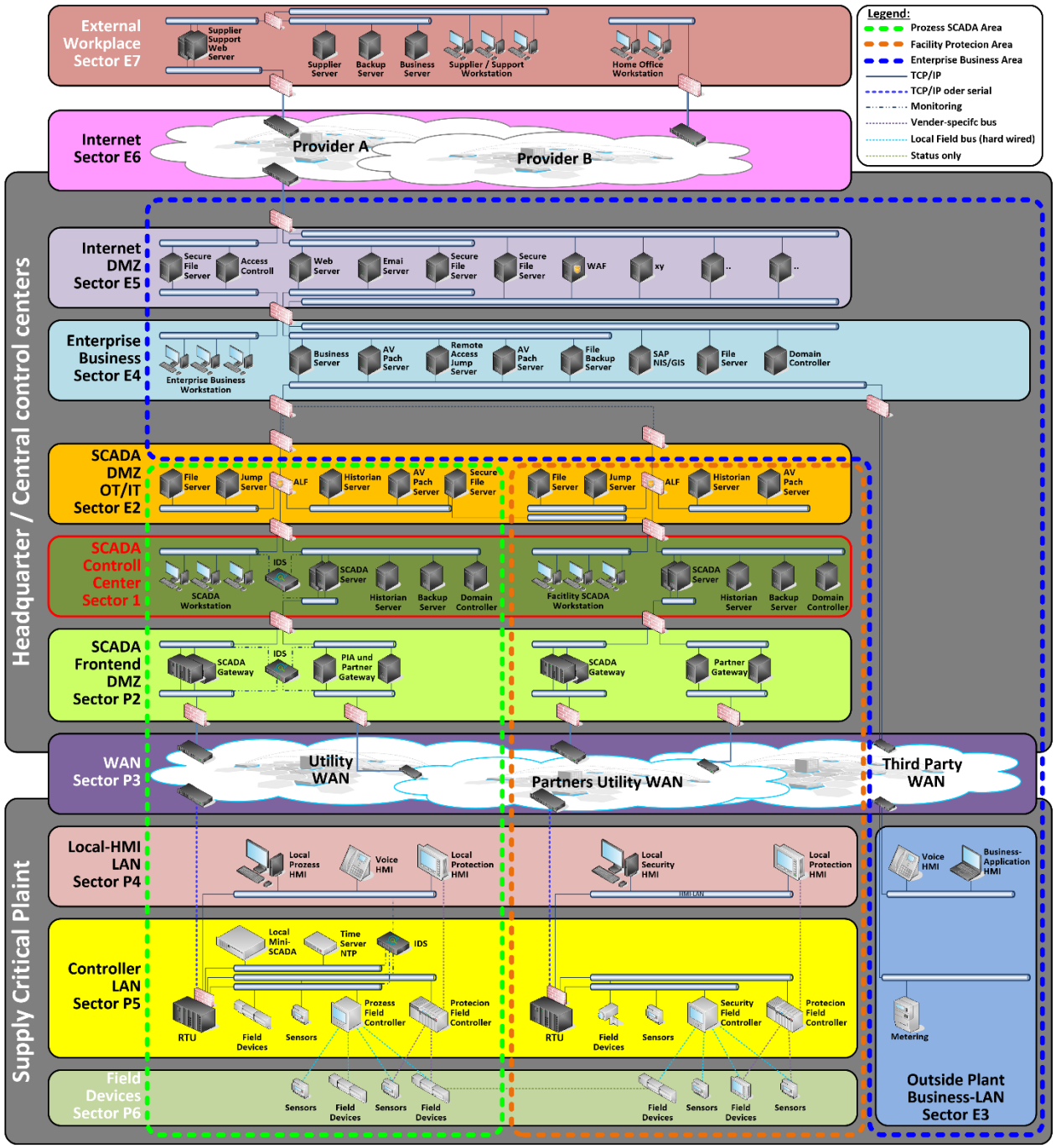

Abbildung 16 Empfohlene sichere Netzwerkarchitektur

(3) Die ICS-Perimeter-Sicherheit schliesst Kontrollen für physische und logische Sicherheit ein, um die Infrastrukturen innerhalb dieser Perimeter zu schützen. Als erster Schritt müssen dazu die Kommunikationsgrenzen definiert werden. Dies erfordert eine Evaluierung, um festzustellen, wo die Bedrohungsakteure potentielle Eindringungsvektoren zur Infiltration des ICS nutzen könnten. Die logische

Sicherheit umfasst Kontrollen wie Authentifizierungsmechanismen, ACLs innerhalb von Netzwerkkomponenten, IDS / IPS-Signaturen (siehe Tabelle 11), Überwachungswerkzeuge und andere Mittel, um die Systeme aus einer logischen Perspektive zu schützen. Physische Perimeter-Sicherheit umfasst alle Mittel die physischen Infrastrukturen schützen, wie z.B. Schlüsselkarten zum Öffnen von Türen, Bewegungsmelder und Kameras oder Sicherheitskräfte.
Um sichere Netzwerke aufbauen zu können, ist es wichtig, dass die nötigen Vorgänge, nötigen Verbindungen, Schutzklassen und Übergänge und mögliche nutzbare Technologien bekannt sind. Folgende technischen Möglichkeiten helfen sichere Netzwerke aufzubauen:

Möglichkeit	Beschreibung
Network Access Control	Network Access Control (NAC; deutsch Netzwerkzugangskontrolle) ist eine Technologie um unautorisierte Zugriffe aus dem Netzwerk zu unterbinden. Mit NAC werden Endgeräte während der Authentifizierung auf Richtlinienkonformität geprüft. Viele Netzwerkgeräte verfügen über NAC-Funktionalitäten. Heute werden meistens die MAC-Adressen und IP-Adressen-Kontrolle eingesetzt. Moderne Systeme setzten auf die Zugangskontrolle, welche auf Zertifikaten basiert.
Netzsegmentierung Bildung von Subnetzen	Das Gruppieren und Segmentieren von Netzen beginnt mit der Bildung von möglichst kleinen Netzen bzw. Subnetzen. Ein Netzsegment soll so klein gehalten werden, dass nur die nötigen funktionalen Anforderungen erfüllt werden können. Grosse Netze, welche viele Elemente enthalten, vergrössern das Risiko für potentielle Ausbreitung von Malware und bieten einem potentiellen Angreifer mehr Handlungsspielraum. Es müssen kleine Netze und Subnetze gebildet werden, damit kontrollierbare Übergänge geschaffen werden können.
Virtuelle LANs Vlan's	Ein Virtual Local Area Network (VLAN) ist ein logisches Teilnetz innerhalb eines Switches oder eines gesamten physischen Netzwerks. Es kann sich über einen oder mehrere Switches hinweg ausdehnen. Ein VLAN trennt physische Netze in Teilnetze auf, indem es dafür sorgt, dass VLAN-fähige Switches die Frames (Datenpakete) eines VLANs nicht in ein anderes VLAN weiterleiten (obwohl die Teilnetze an gemeinsamen Switches angeschlossen sein können). Somit kann eine Segmentierung und Gruppierung auf einem gemeinsamen Netzwerk realisiert werden. VLANs enden auf Firewall oder Router, wo kontrollierte Übergänge zu anderen VLANs realisiert werden.
Routing	Das Routing bestimmt den gesamten Weg eines Nachrichtenstroms durch das Netzwerk; das Forwarding beschreibt hingegen den Entscheidungsprozess eines einzelnen Netzknotens, über welchen seiner Nachbarn er eine vorliegende Nachricht weiterleiten soll. Häufig werden jedoch Routing und Forwarding unter dem Begriff „Routing“ miteinander vermengt; in diesem Fall bezeichnet Routing ganz allgemein die Übermittlung von Nachrichten über Nachrichtennetze. Im Unterschied zu Verteilern (Hubs und Switches) arbeitet das Routing ohne Einschränkungen auch in vermaschten Netzen. Die Vermittlungstechnik bezeichnet mit dem Begriff Verkehrslenkung die Auswahl der Wegeabschnitte beim Aufbau von Nachrichtenverbindungen, die unter Berücksichtigung von Kriterien, wie bspw. der kürzesten Entfernung, erfolgen kann. Handelt es sich um eine leitungsvermittelte Verbindung, wird ein Übertragungskanal für die gesamte Zeit der Verbindung ausgewählt, und alle Nachrichten werden über denselben Weg geleitet. Handelt es sich dagegen um eine paketvermittelte Datenübertragung, wird der Weg für jedes Paket von jedem Netzknoten neu bestimmt.

Möglichkeit	Beschreibung
Firewall	Eine Firewall wird grundsätzliche zwischen zwei Netzwerksegmenten eingesetzt. Sie überprüft lediglich ein- und ausgehenden Netzwerk-Verbindungen nach bestimmten Regeln und unterbindet als gefährlich eingestufte Kommunikationsversuche. Mitunter ist auch von einem „Paketfilter“ die Rede, da Daten im Netzwerk als sogenannte „Datenpakete“ übertragen werden. Firewalls unterscheiden dabei einerseits nach bestimmten „Zonen“. So kann beispielsweise das heimische oder das Firmennetzwerk als sichere beziehungsweise vertrauenswürdige „Zone“ definiert werden, in der Kommunikation ungehindert passieren kann, während das Internet als unsicherer eingestuft wird. Daneben können Firewalls bestimmte Programme oder Dienste unterschiedlich behandeln. Legitime, als sicher eingestufte Programme dürfen dann ungehindert mit dem anderen Element im Netzwerk kommunizieren, unbekannte Programme, bei denen es sich um Schadsoftware handeln könnte, nicht. Und auch bestimmte Server – erkennbar an ihrer IP-Adresse – können in der Firewall als sicher oder unsicher definiert werden.
Demilitarisierte Zonen DMZ	Eine demilitarisierte Zone (manchmal auch als Perimeternetzwerk bezeichnet) ist ein physisches und logisches Subnetzwerk, das als Vermittler für angeschlossene Sicherheitsgeräte fungiert, so dass diese mit einem grösseren und nicht vertrauenswürdigen Netzwerk, meist dem Firmennetzwerk oder Internet verbunden werden können. Die DMZ fügt dem LAN eines Unternehmens eine zusätzliche Sicherheitsschicht hinzu. Somit hat ein externer Eindringling nur einen direkten Zugang zu Geräten innerhalb der DMZ und nicht zu irgendeinem anderen Teil des Netzwerks.
Verschlüsselung, Signaturen und Zertifikate	Um eine Verbindung zwischen zwei Elementen sichern zu können, werden Verschlüsselung Techniken wie SSH eingesetzt. Secure Shell oder SSH bezeichnet sowohl ein Netzwerkprotokoll als auch entsprechende Programme, mit deren Hilfe man auf eine sichere Art und Weise eine verschlüsselte Netzwerkverbindung mit einem entfernten Gerät herstellen kann. Eine weitere Verschlüsselung Methode ist SSL/TLS, dabei werden die zu übertragenden Daten verschlüsselt.
Datendioden	Datendioden sind Elemente, welche zwischen zwei Netzen oder Subnetzen geschaltet werden können. Dabei ist die Datenübertragung auf eine Richtung beschränkt. So können Daten sicher und zuverlässig von sicheren Netzen in unsichere Netze übertragen werden, ohne dass ein Rückkanal vorhanden sein muss, welcher eine potentielle Schwachstelle im Netzwerk bilden kann.
Protokoll-Umsetzer	Eine gute Methode zur sicheren Datenübertragung ist der Einsatz von Protokollumsetzern. Dabei wird ein portbasierender Datenstrom so umgesetzt, dass nur die eigentlichen Nutzdaten übertragen werden. Der gesamte TCP-IP Bestandteils wird dabei entfernt und somit werden diese möglichen Schwachstellen eliminiert.

a) Netzwerkzugangs- und Zugriffskontrollen

(1) Der Zugang zu einem ICS-Netzwerk kann mit einfachen Mitteln eingeschränkt werden. Schon auf den L2-Geräten kann eine MAC-Adressen Authentisierung vollzogen werden. Dabei wird im ICS-Netzwerk nur registrierten und erfassten Komponenten der Zugriff gewährt. Weiter können in den Netzwerkkomponenten die Zugriffs- und Datenflusskontrollen mit Zugriffkontrolllisten (ACL oder DACL) implementiert werden. Da es sich oft bei den ICS-Netzen um statische Netze handelt sind diese einfach zu implementieren. In klassischen Netzwerken werden Zugriffskontrollen nach IEE-E802.1x ausgeführt. Oft werden in diesen Netzen zentrale System für die Zugriffkontrollen wie Radius- und Control-Server eingesetzt. Da in den ICS-Netzen eine klare Segmentierung und Abgrenzung zwischen den einzelnen Sektoren angestrebt wird und lokale Radius- und Control-Server oft keinen Sinn machen, muss man sich die Frage stellen, in wie weit der Einsatz von IEE-E802.1x mit allen Funktionen Sinn macht. Eine Anmeldung an das Netzwerk erfolgt immer häufiger über Zertifikate, welche durch die Hersteller ausgestellt werden. Somit hat man eine weitere Möglichkeit die Zugänge zu überwachen und zu kontrollieren.

(2) Heutige L2-Netzwerkgeräte verfügen über etliche Funktionen, welche den Netzwerkzugriff steuern und regeln können. Da die ICS-Umgebung eher statisch ist und über eine längere Zeitspanne Bestand hat, können lokale Einträge und Listen in den jeweiligen Netzwerkendgeräten absolut Sinn machen. So kann auch die Verwundbarkeit über zentrale Radius- und Kontroll-Server eliminiert werden.

(3) Zugriffe auf die ICS-Netzwerke sollen geloggt werden. Weiter sollen unautorisierte Zugriffsversuche erkannt und eskaliert werden. Beim Einsatz eines zentralen SIEM (Security Information and Event Management) muss die nötige Schnittstelle und Verbindung vorhanden sein.

b) Netzwerksegmentierung / Bildung von Subnetzen

(1) Wie in den vorderen Kapiteln beschrieben, stellt die richtige Netzwerksegmentierung und die Bildung von Subnetzten eine grundlegende und entscheidende Handlung dar. Mögliche Verbindungen und Kommunikationen zwischen den einzelnen Netzelementen sollen nur wenn nötig zugelassen werden. Weiter müssen die gesamten Netze in Areale, Zonen und Sektoren eingeteilt werden bzw. nötige Netzwerkzonenübergänge geschaffen werden, damit die nötigen Kontrollen und Überprüfungen vorgenommen werden können. Es ist in jedem Fall zwingend erforderlich, dass alle möglichen und nötigen Verbindung und Kommunikation zwischen den einzelnen Elementen im ICS-Netzwerk bekannt und beschrieben sind.

c) Virtuelle LANs

(1) Ein virtuelles LAN (VLAN) teilt physische Netzwerke in kleinere logische Netzwerke auf, die aus einer einzelnen Broadcast-Domäne bestehen, die den Datenverkehr von anderen VLANs isoliert. Die Verwendung von VLANs schränkt den Broadcast-Verkehr ein und ermöglicht es, dass logische Subnetze mehrere physische Standorte umfassen.

(2) Einerseits erscheint es für Sicherheitsprofis ratsam, in Bezug auf die neuesten technischen Fortschritte immer auf dem Laufenden zu bleiben. Ebenso kann man ihnen aber raten, sich noch einmal mit den Grundlagen der Netzwerksicherheit zu beschäftigen. Oder konkreter: Sicherheitsprofis sollten erwägen, ihr Wissen über Konzepte wie virtuelle Local Area Networks (VLANs) zu erweitern. Denn es ist durchaus vorstellbar, dass in bestimmten Situationen ein gut konfiguriertes VLAN das einzige Hindernis zwischen der ICS-Umgebung und einem Eindringling bildet, der es auf die Umgebung abgesehen hat.

(3) VLANs gibt es schon fast so lange wie Ethernet-Switches. In einer typischen VLAN-Konfiguration ist jeder Knoten eines Netzwerks physisch mit einem Ethernet-Switch verbunden. Der Netzwerk-Administrator konfiguriert den Switch dann so, dass bestimmte Ports für bestimmte Gruppen segmentiert sind. Jede dieser Gruppierungen wird als VLAN bezeichnet. Alle Mitglieder desselben VLAN können miteinander kommunizieren, ohne andere Netzwerkgeräte passieren zu müssen, ausser in speziellen Fällen, in denen sich ein VLAN über zwei oder mehr geografische Standorte erstreckt. Die Überlegungen hinter dieser Layer-2-Segmentierung sind unterschiedlich. Hinsichtlich Sicherheit bietet sie dem Administrator eine Möglichkeit, sein Netzwerk gegen die gefürchteten Angriffe von Insidern abzuschotten.

(4) VLANs bieten also einige Sicherheitsvorteile, sind aber selbst nicht ohne Risiken. Ein Punkt, den Sicherheitsprofis im Auge behalten sollten, ist das sogenannte VLAN-Hopping. Wie der Name schon sagt, geht es dabei um Endnutzer, die unerlaubterweise mit einem VLAN kommunizieren, zu dem sie nicht gehören. Dieser Angriff lässt sich am leichtesten dann durchführen, wenn ein VLAN mehr als einen Switch umfasst. In Unternehmen mit Gruppen-basierten VLANs ist das häufig der Fall, weil eine oder mehrere Gruppen für eine Anbindung über einen einzigen Switch zu gross werden. In diesem Fall lässt sich ein Konzept namens VLAN-Trunking nutzen. Dabei werden ein oder mehrere Ports eines Ethernet-Switches so konfiguriert, dass sie nur VLAN-Datenverkehr von einem anderen physischen Switch entgegennehmen und weiterleiten. Bei einem möglichen Angriff fügt ein Angreifer mit bösen Absichten einen zweiten 802.1Q-Header in einen Ethernet-Frame ein, so dass dieser in ein nicht autorisiertes VLAN weitergegeben werden kann. Dies ist möglich, weil der erste Switch das Frame untersucht, den ersten der beiden Header daraus entfernt und den Rest des Frames dann weiterleitet. Der zweite 802.1Q-Header ist dann aber immer noch im Frame, was zu einem logischen Fehler führt, der ein Netzwerk massiv stören kann. Um sich gegen solche Angriffe zu wehren, müssen Administratoren gut auf ihre Netzwerk-Logs achten. Zusätzlich kann ein Warnmechanismus auf Layer 3 implementiert werden.

(5) Man muss VLANs in ICS-Umgebungen explizit sichern, da Standardkonfigurationen und Standardnetzwerkkonfigurationen an sich nicht sicher sind. Bei der Verwendung von VLANs muss auf den Netzwerkelementen DTP (Dynamic Trunking Protocol) deaktiviert werden. Somit sind die Ports als statische Access-Ports zu konfigurieren. Dadurch wird verhindert, dass Switch-Spoofing-Exploits angewendet werden. Darüber hinaus müssen die nicht verwendeten Switch-Ports deaktiviert werden, so wird verhindert, dass ein unerlaubter Zugriff auf das Netzwerk erfolgen kann.

(6) Standartmässig sind die Netzwerkelemente mit dem VLAN 1 ausgelegt. Dieses VLAN soll niemals verwendet werden.

d) Firewalls

(1) Die Netzwerksicherheit hängt von mehreren Komponenten ab, die jeweils mit bestimmten Rollen ausgestattet sind. Firewalls bilden ein wichtiges Element in einer sicheren Netzwerkumgebung, um mögliche Angreifer am Eindringen zu hindern. Um Firewalls in Netzwerkumgebungen einpflegen zu können, müssen im Vorfeld die Netzwerke in der ICS-Umgebung segmentiert und gruppiert werden. Somit werden Übergänge geschaffen, wo Firewalls eingesetzt werden können.

(2) Firewalls fungieren als Wächter oder Gatekeeper zwischen Zonen. Wenn sie richtig konfiguriert sind, werden nur gewünschte und nötige Verbindungen zugelassen und aufgebaut. Firewall-Regeln überwachen den Netzwerkverkehr und aktivieren einen vertrauenswürdigen Pfad zu Benutzern und einen vertrauenswürdigen Kanal zu anderen Geräten. Dies ist nur so effektiv wie die Effizienz der

Regeln, mit denen sie konfiguriert sind. In einer Firewall werden Regeln definiert, welche sequenziell abgearbeitet werden. Somit müssen alle möglichen Verbindungsmöglichkeiten explizit und sequenziell konfiguriert werden. Die goldene Regel der Firewall sagt "Was nicht explizit erlaubt ist, wird nicht zugelassen", was bedeutet, dass die letzte Regel immer die „restlichen Möglichkeiten“ verhindert.

(3) Die Aufgabe der Firewall besteht darin:

- Festlegung der Domänentrennung.
- Systemereignisse überwachen (und protokollieren).
- Benutzer authentifizieren, bevor sie Zugriff haben.
- Überwachen des Eingangs- und Ausgangsverkehrs und verhindern von unbefugter Kommunikation.

(4) Es gibt zwei Arten von Firewalls: die Rechner- oder Host-Firewall und die Netzwerk-Firewall. Die Host-Firewall schützt einen bestimmten Host. Es kann Teil des Betriebssystems sein, oder es kann eine Applikation direkt im Einklang mit dem Host sein. Die verwendete Firewall schützt das Netzwerk mit einer von mehreren Techniken:

Paketfilterung

(5) Paket-Filtering- oder Netzwerk-Layer-Firewalls (Layer 3) treffen Entscheidungen auf der Basis von Quell- und Zieladressen und Ports in IP-Paketen. Diese Grundform von Firewall-Schutz ist tatsächlich nicht mehr als ein einfacher Sortieralgorithmus. Im Allgemeinen ermöglichen Ihnen diese Firewalls etwas Kontrolle durch die Verwendung von Zugriffslisten. Paket-Filtering kann auch oft von anderen Netzwerkgeräten wie Routern ausgeführt werden. Üblicherweise erhalten Sie dies auch beim Herunterladen von kostenloser Firewall-Software.

(6) Paket-Filtering funktioniert gut in kleinen Netzwerken. Bei der Anwendung in grösseren Netzwerken kann es jedoch sehr komplex und schwer zu konfigurieren sein. Diese Art von Firewall hat wenig oder keine Aufzeichnungsmöglichkeit. Damit lässt es sich schwer bestimmen, ob eine Attacke stattgefunden hat. Diese Art von Firewall filtert den Datenverkehr basierend auf Regeln. Sie steuern den Datenverkehr auf Basis der ersten drei Ebenen des OSI-Modells: MAC-Adresse und IP-Adresse mit einer Filterung basierend auf der Transportschicht (Portnummern).

Circuit-Level-Gateways

(7) Circuit-Level-Gateways arbeiten auf der Session-Schicht des OSI-Modells oder als "Shim-Layer" zwischen der Applikationsschicht und der Transportschicht des TCP / IP-Stacks. Sie überwachen TCP-Handshaking zwischen Paketen, um festzustellen, ob eine angeforderte Sitzung legitim ist. Informationen, die über einen Circuit-Level-Gateway an einen entfernten Rechner übergeben wurden, erscheinen aus dem Gateway. Circuit-Level Firewall-Anwendungen stellen die Technologie der nächsten Generation dar. Diese Firewall-Technologie überwacht das TCP Handshaking zwischen den Paketen um zu bestätigen, dass eine Sitzung bzw. Verbindung zugelassen ist. Der Firewall-Verkehr ist auf der Grundlage bestimmter Sitzungsregeln sauber definiert und kann nur auf den involvierten Elementen gesteuert werden. Circuit-Level-Firewalls überwachen und überprüfen den Inhalt der Datenpakete nicht. Auf der anderen Seite filtern sie auch keine einzelnen Pakete.

Proxy-Gateways, Application-Layer-Firewall, Application-Layer-Gateway

(8) Diese Firewall bietet Filterung auf der Anwendungsebene. Mit anderen Worten, es beschränkt die Arten von Anwendungen und Protokolle, die über Sicherheitsgrenzen wie z. B. File Transfer Protocol (FTP), Hyper-text Transfer Protocol (HTTP) und so weiter kommunizieren.

Stateful-Inspection

(9) In einer Stateful-Inspektion-Firewall werden die Datenpakete analysiert und der Verbindungsstatus wird in die Entscheidung einbezogen. Bei dieser Technik, werden die Datenpakete (eigentlich: Segmente) während der Übertragung auf der Vermittlungsschicht (3. Schicht des OSI-Modelles) analysiert und in dynamischen Zustandstabellen gespeichert. Auf Basis des Zustands der Datenverbindungen werden die Entscheidungen für die Weiterleitung der Datenpakete getroffen. Datenpakete, die nicht bestimmten Kriterien zugeordnet werden können oder eventuell zu einer DoS-Attacke gehören, werden verworfen. Firewalls mit SPI-Technik sind daher in sicherheitsrelevanten Anwendungen den reinen Paketfilter-Firewalls überlegen.

Deep-Packet-Inspection

(10) Mittels Deep Packet Inspection können weitergehende, insbesondere protokollspezifische Informationen analysiert werden. Dadurch wird es möglich, Regeln zu verwenden basierend auf URLs, Dateinamen, Datei-inhalten (Virenscan oder Data Loss Prevention) und ähnlichem. Dies ähnelt den Möglichkeiten eines Proxys oder eines Content Filters, deckt in der Regel aber zahlreiche Protokolle ab.

(11) Um auch verschlüsselte Verbindungsdaten und Inhalte analysieren zu können, wird SSL Deep Packet Inspection eingesetzt, die eine bestehende SSL-Verschlüsselung terminiert, die Inhalte untersucht und anschliessend für den Client wieder neu verschlüsselt. Dazu ist es in der Regel notwendig, auf dem Client ein CA-Root-Zertifikat zu installieren, das es der Firewall erlaubt, im laufenden Betrieb passende Zertifikate selbst zu generieren. Technisch entspricht dies einem Man-in-the-Middle-Angriff.

(12) Firewall-Platzierung sollte koordiniert, geplant und sorgfältig durchdacht sein. Der Einsatzort der Firewall muss so geplant werden, dass keine Person oder kein Element im gesamten Netzwerk die Sicherheit der Firewall umgehen kann. Beispielsweise führt ein Element mit zwei Netzwerkkarten (NIC‘s), die oft als "Dual-Homed" -Host bezeichnet werden, ein Cyber-Risiko ein, wenn eine Netzwerkarte mit dem Business- oder Firmennetzwerk und die andere mit der ICS-Umgebung verbunden ist. Obwohl diese Art der Konfiguration das Management vereinfacht und die Komplexität verringert, werden Umgebungsschutzmechanismen effektiv umgangen und können eine beträchtliche Verwundbarkeit erzeugen, die Bedrohungsakteure in virtuellen Umgebungen ebenfalls ausnutzen können.

(13) Systemadministratoren sollten das Firewall-Regelwerk, wie im Bild untern gezeigt, spezifizieren und bedarfsgerecht aufbauen. Grundsätzlich gilt: Es wird sichergestellt, dass bei jedem Übergang nur der Verkehr, der speziell auf jeder Ebene erlaubt werden muss, auch durch die Firewall geht. Es ist auch wichtig, dass das Firewall-Regelwerk immer auf dem neuesten Stand gehalten wird, da selbst eine geringfügige Veränderung die Effektivität gegenüber den aktuellen Intrusions-Vektoren bzw. -Schwachstellen verringern könnte. Änderungen des Firewall-Regelwerkes können Datenflussberechtigungen beeinträchtigen. Testen Sie sie daher immer, um sicherzustellen, dass die Änderung die Sicherheit nicht negiert. Periodische Überprüfungen von Firewall-Platzierungen und dem Firewall-Regelwerk tragen dazu bei, dass der nötige Schutz erhalten bleibt.

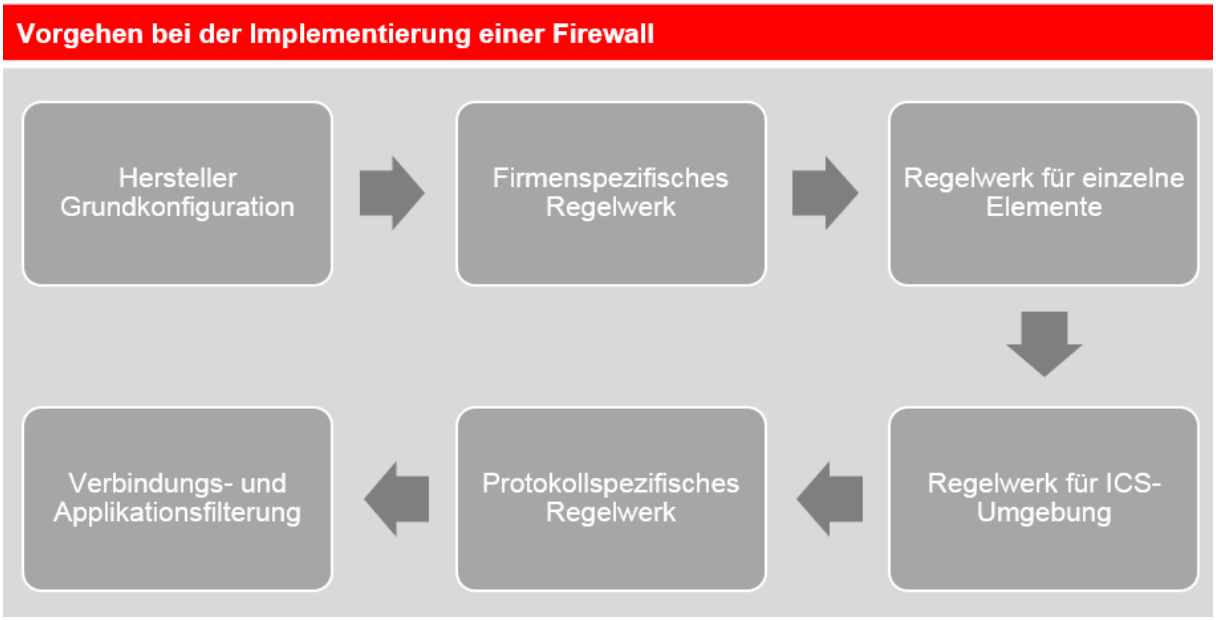

Abbildung 17 Vorgehen bei der Implementierung einer Firewall

(14) Falsches Platzieren einer Firewall kann dazu führen, dass die Firewall weniger effektiv ist. Bypassing der Firewall, ob vorsätzlich oder nicht, ist ein ziemlich häufiges Auftreten. Modems, die direkt Zugang zu ICS-Elementen haben, Hersteller-VPNs, die direkten Zugang in die ICS-Umgebung haben, drahtlose Zugriffspunkte und Einsatz von Dual-NIC-Host, können die Effektivität der Firewall beeinträchtigen und somit den nötigen Schutz der ICS-Umgebung aufheben.

e) Demilitarisierte Zonen

(1) Eine demilitarisierte Zone (manchmal als Perimeternetzwerk bezeichnet) ist ein physisches und logisches Subnetzwerk, das als Vermittler für angeschlossene Sicherheitsgeräte fungiert, so dass sie einem grösseren und nicht vertrauenswürdigen Netzwerk, meist dem Internet, nicht ausgesetzt sind. Die DMZ fügt dem Netzwerk eines Unternehmens eine zusätzliche Sicherheitsschicht hinzu. Somit hat ein externer Eindringling nur einen direkten Zugang zu Geräten innerhalb der DMZ und nicht zu irgendeinem anderen Teil des Netzwerks.

(2) Die Möglichkeit, eine DMZ zwischen den Unternehmens-Netzwerk und der ICS-Umgebung zu etablieren, stellt eine signifikante Verbesserung bei der Verwendung von Firewalls dar. Das Erstellen einer DMZ erfordert, dass die Firewall drei oder mehr Schnittstellen anstelle der typischen öffentlichen und privaten Schnittstellen bietet. Eine der Schnittstellen verbindet sich mit dem Firmennetzwerk, das zweite mit der ICS-Umgebung und die verbleibenden Schnittstellen zu den gemeinsam genutzten oder unsicheren Geräten wie dem Datenarchiv-Server, File-Servern usw. im DMZ-Netz.

(3) Durch die Platzierung von spezifischen Elementen in einer DMZ sind keine direkten Kommunikationspfade vom Firmen-Business-Netzwerk in die ICS-Umgebung erforderlich, es enden somit alle Verbindungen oder Pfade effektiv in der DMZ. Die meisten Firewalls können mehrere DMZs verwalten und können angeben, welche Art von Verkehr zwischen den Zonen weitergeleitet werden kann. Die Firewall kann beliebige Pakete aus dem Firmennetzwerk vom Überleiten in die ICS-Umgebung blockieren und kann auch den Verkehr von den anderen Netzwerkzonen einschliesslich des Kontrollnetzwerks regeln. Bei gut geplanten Regelsätzen kann eine klare Trennung zwischen der ICS-

Umgebung und anderen Netzwerken mit geringem oder keinem Verkehr zwischen den Unternehmensnetzwerk und der ICS-Umgebung gewährleistet werden.

(4) Das primäre Sicherheitsrisiko in dieser Art von Architektur besteht darin, wenn ein Angreifer ein Element in der DMZ kompromittiert und verwendet, um so die die ICS-Umgebung über einen von der DMZ zugelassenen Anwendungsverkehr einzudringen. Dieses Risiko kann reduziert werden, wenn die Systeme in der DMZ gehärtet und aktiv gepflegt werden. Wenn das Firewall-Regelwerk nur Verbindungen zulässt, die von SCADA-Netzwerkgeräten zwischen dem Steuerungsnetz und der DMZ initiiert werden. Andere Probleme mit dieser Architektur bilden die zusätzliche Komplexität und die potenziell erhöhten Kosten für Firewalls mit mehreren Ports. Für kritischere Systeme sollte die verbesserte Sicherheit diese Nachteile jedoch mehr als ausgleichen.

(5) Zwei-Zonen-Lösungen (keine DMZ) sind marginal akzeptabel, sollten aber nur mit äusserster Sorgfalt eingesetzt werden. Die sichersten, verwaltbarsten und skalierbarsten Steuerungsnetzwerk- und Firmennetz Segmentierungs-Architekturen verwenden typischerweise ein System mit mindestens drei Sektoren mit einer oder mehreren DMZs.

(6) Es sollen mehrere DMZs für getrennte Funktionalitäten und Zugriffsberechtigungen wie Peerverbindungen, den Datenarchiv, ICS-Kommunikationsprotokolle, den ICCP-Server in Überwachungs- und Datenerfassungssystemen (SCADA-Systemen), die Sicherheitsserver, Replikations-Server und Entwicklungsserver gebildet werden. Mehrere DMZs haben sich bewährt, um grosse Umgebungen aus Netzwerken mit unterschiedlichen Betreibern und Nutzern zu schützen. Der sichere Datenfluss in und aus den verschiedenen Umgebungen ist für den Betrieb von entscheidender Bedeutung.

(7) Anlagenbetreiber sollten den Zugriff auf eine ICS-DMZ nur auf berechtigte Benutzer, Anwendungen und Dienste beschränken. Soweit möglich sollten der Ein- und Ausstiegsverkehr zu und von der DMZ aufgezeichnet und überwacht werden, so dass sie zur Quell- / Ziel- / Dienstfilterung, einer zusätzliche Sicherheitsüberwachung und Anomalie-Erkennung auf der Nutzdatenebene genutzt werden kann (IDS- und IPS-Funktionen).

(8) Der Zugriff aus der höheren Sicherheitszone d.h. innerhalb der Kontroll- oder Betriebsebenen erfolgt im Allgemeinen, um Daten an die DMZ-Anwendung zu "schieben" und diese Daten den autorisierten Unternehmensbenutzern zur Verfügung zu stellen. Der Zugriff für den Unternehmensbenutzer wird nur vom DMZ-Anwendungsserver gezogen, wodurch eine weitere Trennung erreicht wird. Es ist wichtig, diese logische Trennung zu erstellen, so dass ein Bedrohungsakteur das Vertrauen zwischen den Unternehmens-Enklaven in der DMZ nicht nutzen kann, um von der DMZ in die Steuerung zu "schwenken".

(9) Dennoch ist beim Einsatz von DMZ-Lösungen Vorsicht geboten. Es besteht auch hier die Gefahr, dass ansonsten logisch getrennte Domänen verbunden werden. Gehen Sie nicht davon aus, dass die Implementierung einer DMZ ein Allheilmittel ist, um die Bedrohungsakteure daran zu hindern, tiefer in kritische Umgebungen einzudringen. Die zielführende Ausnutzung von Vertrauensdaten über einen Sicherheitsumkreis ist ein plausibler Intrusionsvektor. Wenn jedoch eine DMZ mit entsprechender Sicherheit entwickelt und eingesetzt wird, erhöht die Gegenmassnahme den Arbeitsaufwand für den Gegner bzw. Angreifer, sorgt für eine stärkere Kontrolle des Anlagenbetreibers und reduziert das Cyberrisiko auf wichtige versorgungskritische Anlagen.

f) Verschlüsselungen

(1) Hinter SSH und SSL/TLS verstecken sich zwei Verfahren zur Verschlüsselung bei Netzwerkverbindungen. Bezüglich Ursprung und Zweck unterscheiden sich die beiden Methoden deutlich. Vereinfacht ausgedrückt wird mit SSL die Verschlüsselung der Daten betrieben, während SSH für eine sichere Kommunikationsverbindung zwischen einem Client und einem Server sorgt. Als Erklärung reicht das aber noch nicht. Im Wesentlichen geht es hier um die zwei Säulen der IT-Sicherheit schlechthin. Auf der einen Seite, bei SSL, sollen der Missbrauch und das Ausspionieren von Daten verhindert werden. Auf der anderen Seite sollen mit SSH sichere Zugänge zu zentralen Rechnern Hacker- oder Sabotageattacken verhindern.

(2) SSL steht für Secure Sockets Layer und ist heute bereits ein veralteter Standard. Der Nachfolger heisst TLS (heute in der Version 1.2), was für Transport Layer Security steht. Die Unterschiede sind relativ gering, aufgrund einiger zusätzlicher Funktionen ist TLS aber noch sicherer als sein Vorgänger SSL. Es handelt sich um ein sogenanntes hybrides Verschlüsselungsprotokoll, das asymmetrische und symmetrische Verfahren kombiniert einsetzt.

Asymmetrisches Public-Key-Verfahren:

(3) Zunächst wird ein Schlüsselpaar erzeugt, das aus einem öffentlichen und einem dazugehörigen privaten Key besteht. Unter Verwendung des Public Key des Empfängers wird der Text chiffriert und versendet. Der Empfänger muss mit seinem passenden Privat Key die Daten wieder entschlüsseln.

- Vorteile: relativ hohe Sicherheit, weniger Schlüssel, kein Schlüsselverteilungsproblem
- Nachteile: erheblich langsamer, sehr lange Schlüssel, explizite Verschlüsselung

Symmetrische Verschlüsselung:

(4) Bei diesem Kryptosystem nutzen Absender und Empfänger denselben Key.

- Vorteile: triviales Schlüsselmanagement, hohe Geschwindigkeit
- Nachteile: ein Key für Ent- und Verschlüsselung, Schlüssel muss transportiert werden, grosse Schlüsselanzahl

(5) Bei TLS/SSL wird zunächst wird ein symmetrischer Sitzungsschlüssel (Session-Key) generiert, der anschliessend die schützenswerten Daten codiert und versendet. Auf dem Endgerät angekommen nimmt dieser die Daten in Empfang und dechiffriert sie asymmetrisch. Durch dieses Verfahren können asymmetrische Einmalschlüssel an die Empfänger verteilt und gleichzeitig die schnellere symmetrische Verschlüsselung für den Datentransport genutzt werden. SSL bzw. dessen Nachfolger TLS kommt insbesondere bei https-Verbindungen zur Anwendung, weshalb die meisten Webserver TLS mit Camellia- oder AES-Algorithmen einsetzen. Im Klartext heisst das: TLS ist das Protokoll und legt die Rahmenbedingungen für die verschlüsselte Übertragung fest. AES und Camellia sind die Methoden, mit denen die Chiffrierung umgesetzt wird.

(6) SSH steht für Secure Shell und ist ein Netzwerkverschlüsselungsprotokoll, das einem ganz anderen Ansatz als TLS bzw. SSL entsprungen war. Secure Shell oder SSH bezeichnet sowohl ein Netzwerkprotokoll als auch entsprechende Programme, mit deren Hilfe man auf eine sichere Art und Weise eine verschlüsselte Netzwerkverbindung mit einem entfernten Gerät herstellen kann. Häufig wird diese Methode verwendet, um lokal eine entfernte Kommandozeile verfügbar zu machen, das heisst, auf einer lokalen Konsole werden die Ausgaben der entfernten Konsole ausgege-

ben und die lokalen Tastatureingaben werden an den entfernten Rechner gesendet. Genutzt werden kann dies beispielsweise zur Fernwartung eines in einem entfernten Rechenzentrum stehenden Servers. Die neuere Protokoll-Version SSH-2 bietet weitere Funktionen wie Datenübertragung per SFTP.

(7) Ganz anders als SSL bzw. TLS setzt SSH nur das asymmetrische Public-Key-Prinzip ein. Dafür sendet der Server als Erstes seinen Public Key, den der Client verschlüsselt zurückschickt. Mit seinem passenden Privat Key ausgestattet kann der Server nun verschlüsselte Verbindungen mit dem Client zulassen. Ein Problem stellt sich ein, wenn sich ein Proxy-Server oder eine Firewall auf dem Weg befindet. Dafür werden entweder andere, weiterentwickelte Protokolle (HTTPS) und Zertifikate genutzt, oder es wird ein SSH-Tunnel angelegt. Auf diese Weise lassen sich unsichere Netzwerkprotokolle eingebettet in einem gesicherten und verschlüsselten Netzwerkprotokoll abhör- und manipulationssicher transportieren.

Das Problem der verschlüsselten Verbindungen

(8) Verschlüsselte Verbindung bringen aber auch grosse Gefahren mit sich. Der Inhalt dieser Verbindungen können nicht so einfach auf Schadsoftware oder auf Fehlfunktion geprüft werden. Weiter können über SSH-Verbindungen ganze Netzwerke zusammengeschaltet werden, ohne dass jegliche Sicherheitshürde, wie Firewall, etwas davon mitbekommt. Somit muss sehr genau definiert werden, welche Elemente über verschlüsselte Verbindung kommunizieren müssen. Jede verschlüsselte Verbindung sollte auf der Firewall, oder spätestens auf dem IDS/IPS terminiert sein.

g) Digitale Signaturen, digitale Zertifikate und Public-Key-Infrastrukturen

(1) Digitale Signaturen und Zertifikate stellen heute die Grundlage für das Vertrauen im Internet dar. Mehr und mehr Geräte werden mit dem Internet verbunden, die sogenannten Internet of Things (IoT) Geräte und Machine-to-Machine (M2M) ermöglichen konstante Kommunikation und Datenaustausch. Schnell entstehen wahre Big-Data-Ströme und das alles relativ ungesichert, denn die Kommunikation wird in der Regel nicht durch digitale Zertifikate ermöglicht.

Digitale Signaturen

(2) Bei einer digitalen Signatur (nicht zu verwechseln mit einem digitalen Zertifikat) handelt es sich um eine elektronische Signatur, mit deren Hilfe der Absender einer Nachricht oder der Unterzeichner eines Dokuments seine Identität nachweisen kann. Unter Umständen lässt sich damit auch sicherstellen, dass der ursprüngliche Inhalt eines versendeten Dokuments oder einer Nachricht nicht verändert wurde. Digitale Signaturen sind einfach zu übertragen, lassen sich nicht durch Dritte imitieren und werden mit einem automatischen Zeitstempel versehen. Da der Empfang der originalen signierten Nachricht nachgewiesen werden kann, ist es dem Absender später zudem nicht möglich, den Versand der Nachricht abzustreiten.

Digitale Zertifikate

(3) Ein digitales Zertifikat ist ein elektronischer Personalausweis, der es einer Person, einem Computer oder einer Organisation ermöglicht, mit Hilfe der Public Key Infrastruktur (PKI) Informationen sicher über das Internet auszutauschen. Ein digitales Zertifikat wird oftmals auch als Public Key Zertifikat bezeichnet.

(4) Genau wie ein Personalausweis stellt ein digitales Zertifikat Informationen über die Identität zur Verfügung, kann nicht gefälscht, dafür aber verifiziert werden, da es von einer offiziellen, vertrauenswürdigen Institution ausgestellt wurde. Das Zertifikat beinhaltet den Namen des Zertifikatseigen-

tümers, eine Seriennummer, Verfallsdatum, eine Kopie des öffentlichen Schlüssels des Zertifikatseigentümers (diese wird genutzt, um Nachrichten zu verschlüsseln und digital zu signieren) und die digitale Signatur der ausstellenden Institution, sodass der Empfänger verifizieren kann, dass das Zertifikat echt ist.

(5) Weit verbreitet sind Public-Key-Zertifikate nach dem Standard X.509, welche die Identität des Inhabers und weitere Eigenschaften eines öffentlichen kryptographischen Schlüssels bestätigen. Attributzertifikate enthalten dagegen keinen öffentlichen Schlüssel, sondern verweisen auf ein Public-Key-Zertifikat und legen dessen Geltungsbereich genauer fest. Im Kontext elektronischer Signaturen wird der Begriff Zertifikat technikneutraler aufgefasst (siehe Abschnitt Rechtliche Aspekte im Artikel Public-Key-Zertifikate), so dass ein Zertifikat sich nicht notwendigerweise auf einen kryptographischen Schlüssel beziehen muss, sondern allgemein Daten zur Prüfung einer elektronischen Signatur enthält. In der Praxis handelt es sich jedoch immer um Public-Key-Zertifikate.

(6) Diese signierten Zertifikate können eindeutig zugewiesen werden. Nur wenn es eindeutig zugewiesen werden kann, kann es nicht verändert – also verfälscht – werden. Alle Zertifikate werden von einer Zertifizierungsstelle (Certification Authority, CA) verwaltet, die sich um die Sicherheit und den vertrauenswürdigen Status dessen kümmert.

(7) Um die Authentizität des genannten Public-Key-Zertifikats zu verifizieren – mit anderen Worten, um nachzuweisen, dass der genannte Ursprung mit dem tatsächlichen Ursprung übereinstimmt – kommen noch mehr Zertifikate ins Spiel. Sie bilden Zertifikatsketten, die als Validierungspfad bekannt sind und Path Tracking erlauben. Insgesamt bilden die einzelnen Zertifizierungspfade eine robuste Public Key Infrastructure (PKI).

(8) Angreifer setzen zumeist Man-in-the-Middle-Angriffe ein. Sie klinken sich also mit einem kompromittierten Zertifikat in die Kommunikation ein. Cyberkriminelle haben ein paar tausend Trojaner entwickelt, die es ihnen ermöglichen, alle möglichen Zertifikate zu stehlen, zu verändern und wieder einzuschleusen.

(9) Zahlreiche Experten nehmen an, dass es in Zukunft noch wesentlich mehr Angriffe über missbrauchte Zertifikate geben wird. Dies besonders im Hinblick auf das Internet der Dinge. Viele dieser neuen Geräte sollen das Leben jedes einzelnen vereinfachen und gleichzeitig Effizienzsprünge in der industriellen Fertigung ermöglichen. Hier muss ein umfassender Sicherheitsansatz angewendet werden, der Zertifikate auf ihre Echtheit prüft und die gefälschten in eine Quarantäne verschiebt.

(10) Ein digitales Zertifikat ist in der Regel zwei Jahre gültig, dagegen ist die Lebensdauer von Komponenten in versorgungskritischen Anlagen oft > 10 Jahre. Dies stellt die Einführung von Zertifikaten vor eine neue Herausforderung.

h) PKI (Public-Key-Infrastruktur)

(1) Eine PKI (Public-Key-Infrastruktur) bietet Anwendern in einem an sich unsicheren öffentlichen Netzwerk, wie dem Internet, einige Vorteile: sicheren und vertraulichen Austausch von Daten mit Hilfe eines Paares aus einem öffentlichen und einem privaten Kryptographie-Schlüssel. Dieser wird von einer vertrauenswürdigen Stelle bezogen und über diese weitergegeben. Die Public-Key-Infrastruktur stellt ein digitales Zertifikat zur Verfügung, das der Identifizierung einer Person oder eines Unternehmens dient. Zudem bietet sie Verzeichnis-Dienste zum Speichern und gegebenenfalls auch zum Widerrufen von Zertifikaten. Die nötigen Komponenten einer PKI sind weitgehend verstanden, doch verfolgt eine Reihe von Anbietern neue Ansätze und Services dafür.

(2) Voraussetzung für eine Public-Key-Infrastruktur ist ein Public-Key-Verschlüsselungsverfahren. Dieses stellt die gebräuchlichste Form für die Authentifizierung des Absenders von Nachrichten bzw. der Verschlüsselung von Nachrichten dar. Bei der herkömmlichen Verschlüsselung wurde in der Regel ein geheimer Schlüssel für die Verschlüsselung und spätere Entschlüsselung von Nachrichten erstellt und weitergegeben. Dieses System mit geheimen oder privaten Schlüssel hat allerdings einen gravierenden Nachteil: Wird der Schlüssel von einem Dritten abgefangen oder geknackt, lassen sich die Nachrichten problemlos entschlüsseln. Aus diesem Grund wird im Internet der Ansatz mit Public-Key-Verschlüsselungsverfahren und einer Public-Key-Infrastruktur bevorzugt. Private-Key-Verschlüsselung wird gelegentlich auch als symmetrische Verschlüsselung bezeichnet, während man bei der Public-Key-Verschlüsselung von einer asymmetrischen Verschlüsselung spricht.

Eine Public-Key-Infrastruktur umfasst folgende Komponenten:

- eine Zertifizierungsstelle für die Ausgabe und Verifizierung digitaler Zertifikate
- ein Zertifikat mit dem öffentlichen Schlüssel oder Informationen zum öffentlichen Schlüssel
- eine Registrierungsstelle zur Verifizierung der Zertifizierungsstelle vor Ausgabe eines digitalen Zertifikats an den Antragsteller
- eines oder mehrere Verzeichnisse zur Aufbewahrung der Zertifikate (und ihrer öffentlichen Schlüssel)
- ein System zur Zertifikat-Verwaltung

Funktionsweise von Public- und Private-Key-Verschlüsselung

(3) Für die Public-Key-Verschlüsselung werden gleichzeitig ein öffentlicher sowie ein privater Schlüssel erstellt. Die Zertifizierungsstelle verwendet hierfür den gleichen Algorithmus (beliebt ist der bekannte RSA). Der private Schlüssel wird nur dem Anforderer ausgehändigt, während der öffentliche Schlüssel in einem allen Parteien zugänglichen Verzeichnis zur Verfügung steht (als Komponente eines digitalen Zertifikats). Demgegenüber wird der private Schlüssel nie an andere weitergegeben oder über das Internet versandt. Er dient zur Entschlüsselung von Nachrichten, die mit dem Public Key verschlüsselt wurden; diesen hat der Absender aus dem öffentlich zugänglichen Verzeichnis bezogen.

(4) Wenn für versorgungskritische Anlagen die digitale Zertifikate mit einem PKI verwendet werden, muss die PKI-Infrastruktur lokal im Unternehmen und isoliert vom Internet aufgebaut werden. Bei der Nutzung von öffentlichen oder externen PKI im Internet, wären sonst Verbindungen zu diesen Stellen notwendig. Somit baut man sich eine zusätzliche Sicherheitslücke in das vermeintlich sichere Netzwerk ein. Die Einführung von digitalen Zertifikaten in Zusammenhang mit einem PKI muss deshalb gut überlegt und geplant werden. Zumal die heutigen Komponentenlieferanten von versorgungskritischen Anlagen diese Funktion noch nicht implementiert haben oder anwenden.

i) Datendioden

(1) Ein unidirektionales Netzwerkgerät (auch als unidirektionales Sicherheitsgateway oder Datendiode bezeichnet) ist ein Netzwerkgerät oder eine Vorrichtung, die es ermöglicht, dass Daten nur in einer Richtung übertragen werden. Benutzer finden sie am häufigsten in Hochsicherheitsumgebungen, wo sie als Verbindungen zwischen zwei oder mehreren Netzwerken unterschiedlicher Sicherheitsklassifikationen dienen. Diese Technologie findet sich heute auf der industriellen Steuerungsebene für Anlagen wie Kernkraftwerke und Stromerzeugung.

(2) Die physikalische Natur von unidirektionalen Netzwerken erlaubt nur, dass Daten von einer Seite einer Netzwerkverbindung zu einer anderen und nicht umgekehrt übertragen werden. Die Vorteile für die Nutzer des Netzwerks mit höherer kritischer Priorität (z. B. eines ICS-Segments) liegen darin, das Daten in einem niedrigeren Kritikalitätsnetzwerk (niedrige Seite), wie z. B. von einem Server in einer DMZ, übertragen werden können und gleichzeitig den Kommunikationszugriff vom Netzwerk mit niedriger kritischer Priorität zum ICS-Netzwerk verhindert werden kann. Die gesteuerte Schnittstelle, die die Sende- und Empfangselemente eines unidirektionalen Netzwerks umfasst, fungiert als ein unidirektionaler Kommunikationsprotokollbruch zwischen den beiden miteinander verbundenen Netzwerkdomänen. Dies schliesst die Verwendung des unidirektionalen Netzwerks bei der Übertragung von Protokollen wie TCP, die eine Kommunikation (einschliesslich Bestätigungen) zwischen Sender und Empfänger erfordern, nicht aus.

(3) Betreiber von versorgungskritischen Anlagen verwenden immer mehr Datendioden.

j) Protokollumsetzer

(1) In der ICS-Umgebung werden oft Datenverbindungen eingesetzt, wo kleine Datenmengen übertragen werden müssen. Somit können zum effektiven Schutz auf klassischen Datenübertragung mittels seriellem Ports zurückgegriffen werden. Diese Verbindungen funktionieren in der Regel ohne IP-Funktionalität und sind als klassische Punkt zu Punkt Verbindungen anzusehen. Somit erreicht man eine „IP lose“ Verbindungen. Durch diese Massnahme kann ein grosser Teil von Schwachstellen in der ICS-Umgebung eliminiert werden bzw. es sind gar keine Schwachstellen vorhanden.

(2) Zur Erfüllung dieser Funktionalität werden gemäss Bild unten jeweils zwei Elemente benötigt:

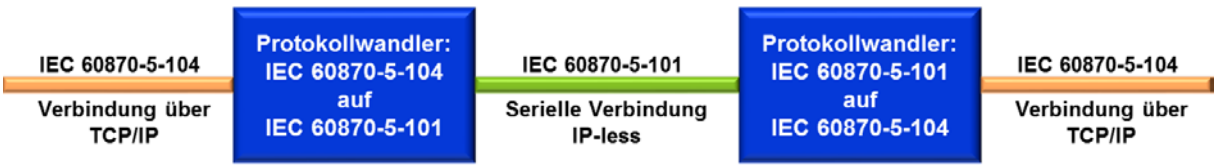

Abbildung 18 Einsatz von Protokollumsetzern

(3) Der Einsatz dieser Methode kann eine Segmentierung zwischen zwei Sektoren oder Segmenten erfolgen. Durch die „IP lose“ Übertragung können viele Schwachstellen, welche klassische IP-Netzwerke aufweisen, eliminiert werden.

2.8.2 Zonenübergänge definieren und beschreiben

(1) Grundsätzlich gibt es in der ICS-Umgebung horizontale und vertikale Zonenübergänge. Alle Arten von Zonenübergängen müssen definiert und beschrieben werden.

a) Horizontale Übergänge von Sektoren und Zonen

(1) Soweit nötig, anwendbar, sinnvoll und technisch möglich, wird die dem System zugrundeliegende Netzwerkstruktur horizontal in unabhängige Sektoren und Zonen (z. B. nach Standorten und Funktionen) aufgeteilt, wobei die Trennung der Sektoren/Zonen durch Firewalls, filternde Router, Gateways oder über DMZ erfolgen muss. Auch innerhalb der einzelnen Sektoren und Zonen hat eine Segmentierung zu erfolgen. Es müssen Bereiche geschaffen werden, bei welchen kontrollier- und steuerbare Übergange vorhanden sind. So kann verhindert werden, dass sich ein Angreifer oder Schadsoftware sich frei fortbewegen oder verbreiten kann. An den Übergangen können Überwachungs- und Steuerungselemente eingebaut werden, welche es ermöglich den Verkehr zu überwachen, kontrollieren und einzuschränken.

b) Vertikale Übergänge von Sektoren und Zonen

(1) Soweit nötig, anwendbar, sinnvoll und technisch möglich, wird die dem System zugrundeliegende Netzwerkstruktur vertikal in Sektoren und Zonen mit verschiedenen Funktionen (Grid-Control, Produktion-Control und Infrastruktur-Control) und unterschiedlichem Schutzbedarf aufgeteilt. Wo technisch möglich, werden diese Netzwerk-Zonen durch Firewalls, filternden Router, Gateways und mit DMZ getrennt. Die Kommunikation mit weiteren Netzwerken hat ausschliesslich über vom Auftraggeber zugelassene Kommunikationsprotokolle unter Einhaltung der geltenden Sicherheitsregeln zu erfolgen. Die vertikalen Zonenübergänge müssen genau geplant und definiert werden. Wenn möglich sollen vertikale Übergange nur an einem definierten Punkt erfolgen. Somit können Umwege das Zusammenschalten von Netzwerken verhindert werden. Diese Übergänge bedürfen einen hohen Schutzbedarf, da an diesen Punkte oft Systeme von verschiedenen Unternehmen und Lieferanten verbunden werden müssen. Somit kann sich bei einem ungenügenden Schutz, eine Schwachstelle in einem System auf das benachbarte System Auswirkungen haben.

c) Sectormatrix erstellen und Bewertung der Verbindungen und Übergänge

(1) Um ein Bild über die gesamten möglichen und nötigen Verbindungen und Kommunikationen im ICS-Netzwerk zu erhalten, ist die Erstellung einer gesamthaften Kommunikationsmatrix über die einzelnen Zonen und Segmenten zwingend erforderlich. Somit können alle Vorgänge analysiert und bewertet werden. Mit einer Kommunikationsmatrix werden nötige Zonenübergänge bestimmt, die anschliessend beurteilt und bewertet werden können. Es ist zwingend notwendig, dass in dieser Kommunikationsmatrix alle nötigen und möglichen Verbindungen und Kommunikationsmöglichleiten abgebildet werden. Mit dieser Methode können Schwachstellen bzw. unzureichend geschützte Übergänge zwischen den Sektoren und Zonen bestimmt werden.

(2) In der Kommunikationsmatrix über das gesamte ICS-Umfeld werden die grundsätzlichen Mechanismen für Sektoren- und Zonenübergänge beschrieben. Über die technische Ausführung oder die Dimensionierung müssen detaillierte Vorgaben und Richtlinien erstellt werden.

(3) In der Zonenmatrix über das gesamte ICS-Umfeld müssen zwingend auch alle Umfelder und Umsysteme, zu welchen irgendeine Kommunikation oder Verbindung möglich ist, erfasst und beschrieben werden.

Zonenmatrix über das gesamte ICS-Umfeld

von \ nach		External Workplace Sector E7	Internet-DMZ Sector E5	Enterprise-Business Sector E4	Enterprise-Business HMI Sector E3	Enterprise-Business Metering Sector E3	SCADA-DMZ OT/IT Grid Sector E2	SCADA-DMZ OT/IT Facility Sector E2	SCADA Control Center Grid Sector 1	SCADA Control Center Facility Sector 1	SCADA Frontend DMZ Grid Sector P2	SCADA Frontend DMZ Facility Sector P2	SCADA Frontend DMZ Partner Sector P2	Local HMI LAN Grid Sector P4	Local HMI LAN Facility Sector P4	Controler LAN Grid Sector P5	Controler LAN Facility Sector P5	Field Devices Grid Sector P6	Field Devices Facility Sector P6
External Workplace	Sector E7	x	Ja(1)	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
Internet-DMZ	Sector E5	Ja(2)	x	Ja(2)	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
Enterprise-Business	Sector E4	Ja(2)	Ja(1)	x	Ja(1)	Ja(1)	Ja(1)	Ja(1)	Ja(3)	Ja(3)	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
Enterprise-Business HMI	Sector E3	Nein	Nein	Ja(1)	x	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
Enterprise-Business Metering	Sector E3	Nein	Nein	Ja(1)	Nein	x	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
SCADA-DMZ OT/IT Grid	Sector E2	Nein	Nein	Ja(1)	Nein	Nein	x	Nein	Ja(2)	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
SCADA-DMZ OT/IT Facility	Sector E2	Nein	Nein	Ja(1)	Nein	Nein	Nein	x	Nein	Ja(2)	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
SCADA Control Center Grid	Sector 1	Nein	Nein	Ja(3)	Nein	Nein	Ja(1)	Nein	x	Nein	Ja(1)	Nein	Ja(1)	Ja(3)	Nein	Nein	Nein	Nein	Nein
SCADA Control Center Facility	Sector 1	Nein	Nein	Ja(3)	Nein	Nein	Nein	Ja(1)	Nein	x	Nein	Ja(1)	Ja(1)	Nein	Ja(3)	Nein	Nein	Nein	Nein
SCADA Frontend DMZ Grid	Sector P2	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja(2)	Nein	x	Nein	Nein	Ja(1)	Nein	Nein	Nein	Nein	Nein
SCADA Frontend DMZ Facility	Sector P2	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja(2)	Nein	x	Nein	Nein	Ja(1)	Nein	Nein	Nein	Nein
SCADA Frontend DMZ Partner	Sector P2	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja(2)	Ja(2)	Nein	Nein	x	Nein	Nein	Nein	Nein	Nein	Nein
Local HMI LAN Grid	Sector P4	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja(3)	Nein	Ja(1)	Nein	Ja(1)	x	Nein	Ja(1)	Nein	Ja(1)	Nein
Local HMI LAN Facility	Sector P4	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja(3)	Nein	Ja(1)	Ja(1)	Nein	x	Nein	Ja(1)	Nein	Ja(1)
Controler LAN Grid	Sector P5	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja(3)	Nein	Ja(1)	Nein	Nein	Ja(1)	Nein	x	Nein	Ja(1)	Nein
Controler LAN Facility	Sector P5	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja(3)	Nein	Ja(1)	Nein	Nein	Ja(1)	Nein	x	Nein	Ja(1)
Field Devices Grid	Sector P6	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja(1)	Nein	x	Ja(4)
Field Devices Facility	Sector P6	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja(1)	Ja(4)	x

Ja(1)	nach dem "whitelistening" Verfahren möglich	Ja(4)	Nur IP-less möglich, analog oder binäre Kontakte
Ja(2)	sofern die Quelle ein ALG ist: Approval von Architektur- und Security- Team notwendig, Andere Server: Nein	Nein	nicht erlaubt
Ja(3)	Nur für MFT zu MFT sowie ESB zu ESB Verbindungen	x	nicht möglich

Abbildung 19 Interne Verbindungsmatrix für den Sektor E2, SCADA / DMZ / OT / IT

d) Sonderfälle

(1) Im Energiesektor gibt es einige Kommunikations-Sonderfälle, die speziell betrachtet werden müssen. Als Sonderfälle werden die nötigen Verbindungen zwischen den Schutzgeräte für Fernauslösungen (Distanzschutz und Differentialschutz) betrachtet. Hier kommunizieren Schutzelemente mit Schutzelemente in benachbarten Anlagen. Da diese Verbindungen grosse Anforderungen an die Verfügbarkeit und auch an die maximale Latenzzeit darstellen, kommen hier spezifische und spezielle Kommunikationseinrichtungen zum Einsatz. Wichtig ist, dass die Kommunikationen für diese Verbindungen sicher und zuverlässig sind. Für einen Angreifer bilden diese Verbindungen ein grosses Schadenpotential, da bei Manipulationen Schutzauslösungen und folgenden Leitungsauftrennungen erfolgen. Somit müssen diese Systeme wie auch Verbindungen für diese Systeme „sehr gut geschützt“ werden. Bei einer Übertragung über „unsicher Netze“ ist die Verbindung zwingend zu verschlüsseln.

(2) Folgende Sonderfälle sind bekannt, welche einen besonderen Schutzbedarf aufweisen:

- Schutzgeräte und deren Verbindungen
- Gerätschafften für UFLS[6]

2.8.3 Fernzugriffe und Authentifizierung

a) Fernzugriffe

(1) Industrielle Steuerungssysteme spielen eine wichtige Rolle in kritischen Infrastrukturen der Stromversorgung. In der Vergangenheit wurde das Risiko für diese Systeme durch die Sicherstellung einer vollständigen Trennung von betrieblichen Umgebungen von externen Netzwerken verringert und der Zugriff auf die Kontrollfunktion auf autorisierte Benutzer mit physischem Zugang zu einer Einrichtung beschränkt. Heute haben die geschäftlichen Anforderungen die Vernetzung dieser einmal isolierten Systeme beschleunigt. Diese neuen Verbindungsmöglichkeiten haben den Anlagen-Inhabern ermöglicht, die Betriebsabläufe zu maximieren und die Kosten, welche mit der Überwachung, dem Upgrade und der Wartung von Geräten verbunden sind, zu senken. Gleichzeitig schaffen sie neue Sicherheitsanforderungen für den Schutz von OT-Systemen in kritischen Anlagen für die Stromversorgung vor ungewollten Zugriffen aus Fremdnetzen und auch dem Internet.

(2) Bei der Einführung von Fernzugriffen muss eine Sicherheitsbalance gefunden werden, wie die OT-Systeme verwaltet bzw. auf diese zugegriffen und wie die Cyber-Sicherheitsposition OT-Systems dennoch gewahrt werden kann. Eine grosse Gefahr besteht darin, dass Fernzugriffe oft von Unternehmen nicht verstanden oder schlecht ausgeführt sind. Die Anwendung bewährter und akzeptierter Fernzugriffslösungen kann jedoch nicht optimal auf die Steuerung von Systemumgebungen abstimmt werden. Die Anforderungen an Verfügbarkeit und Integrität, kombiniert mit den einzigartigen Nuancen und Attributen, die oft in "speziell entwickelten" Systemen zu finden sind, führen zu einem neuen Anforderungsprofil bei der Erstellung von sicheren Fernzugriffslösungen für System in der OT-Umgebung.

(3) Remotezugriffe auf OT-Systeme für kritische Infrastrukturen der Stromversorgung stellen die Anlagenbetreiber vor eine grosse Herausforderung. Wenn von einem externen Workplace eine direkte verschlüsselte Verbindung in kritische Infrastrukturenteile der Stromversorgung aufgebaut wird, wird das gesamte Segment den Gefahren der externen Umgebung ausgesetzt. Dies ist unabhängig

[6] UFLS: Under Frequency Load Shedding, übersetzt unterfrequenzabhängiger Lastabwurf

ob es sich dabei um einen Lieferantenzugang oder externen Zugang eines Servicemitarbeiters handelt. Oft werden diese externen Workplaces für den Zugang zu mehreren Anlagen genutzt. Somit stellen diese ideale Punkte für die Verteilung von Schadsoftware und einen idealen zentralen Punkt für Zugriffe auf alle Anlagen dar. Genau diese Workplaces werden zu einem priorisierten Ziel eines potentiellen Angreifers. Abhilfe für diese Probleme schaffen Zugriffe auf Jump-Stationen, auf welche nur eine Verbindung zur Übertragung von Video, Tastatur und Maus aufgebaut werden können, dies kann durch Remotedesktop-Verbindungsarten (RDP, TeamViewer, pcAnywehre usw.), erstellt werden. Auf der Jump-Station kann dann eine Verbindung zur kritischen Anlage der Stromversorgung erstellt werden. Somit werden direkte Verbindungen zwischen externen Workplaces und versorgungskritischen Anlagen unterbunden. Wichtig ist, dass bei diesen Verbindungarten, das automatische Kopieren oder Übertragen von Dateien unterbunden oder kontrolliert wird. Diese Daten müssen nach den Richtlinien der betreibenden Organisation geprüft werden. Durch die Verwendung von Jump-Stationen, welche auch mit virtuellen Rechnern ausgeführt werden können, kann auch das Problem der Authentisierung gelöst werden. Die Zugriffe auf die Jump-Stationen können mittels Zweifaktor-Authentisierung erfolgen und jederzeit überwacht und kontrolliert werden. Weiter können auf diesen Jump-Stationen die Rechte und Möglichkeiten für den jeweiligen Nutzer nach dem Prinzip „nur was unbedingt nötig“ vergeben werden. Viele Firewall-Infrastrukturen bieten komplette Lösungen für Remote-Zugänge, über welche die Authentisierung und der Zugang gesteuert und überwacht wird.

Beispiel für eine sicheren Fernzugang

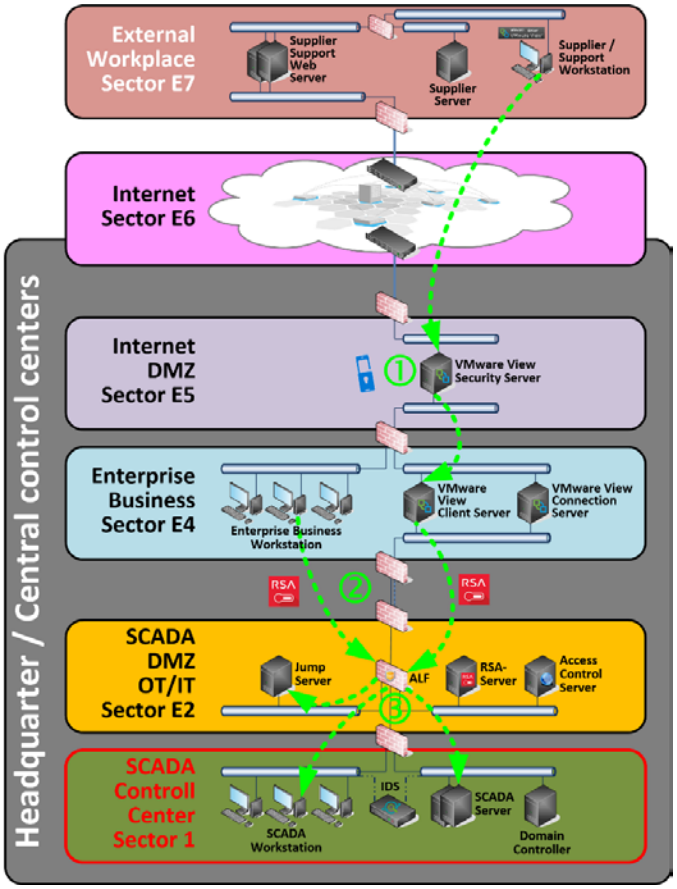

Abbildung 20 Beispiel sicherer Fernzugang

① Der externe Zugriff auf einen Client im Business-IT-Umfeld erfolgt mittels verschlüsselter Verbindung über das Web. Der Zugang erfolgt über eine starke 2-Faktor-Authentisierung mittels z.B. dem AD FS in Kombination mit Anmeldung am Client durch einen Business-IT-Accounts. Hier kann der Standart-Zugang der Business-IT verwendet werden.

② Vom Client im Business-IT-Umfeld wird mittels einer SSL-VPN-Verbindung über den Web-Browser eine Verbindung zur ALF-Firewall erstellt. Die Authentisierung auf dem Remote-Desktop-Dienst auf der Firewall erfolgt mittels 2-Faktor-Authentisierung. Dabei ist zu empfehlen, dass sich der zweite Faktor z.B. der RSA-Token beim Systemadministrator der OT-Umgebung befindet und dieser Faktor bei diesem nachgefragt werden muss.

③ Nach der Freigabe durch den Systemadministrator kann eine Remote-Session zum gewünschten OT-Element aufgebaut werden. Die Anmeldung auf dem OT-Element erfolgt nach den Richtlinien und Vorgaben des OT-Systembetreibers.

(4) Es wird empfohlen, dass Remote-Zugänge zu kritischen Anlagen der Stromversorgung von der Betreiberorganisation autorisiert und freigegeben werden muss. Dies kann idealerweise durch Freischalten des Anschlusses mittels Fernsteuerung in den Anlagen durch die Betreiberorganisation erfolgen. Somit ist auch jederzeit sichergestellt, dass die betreibende Organisation Kenntnisse über Remote-Zugriffe auf die Anlagen haben und diese im Notfall auch unterbinden kann. Von automatisierten Remote-Zugriffen wird abgeraten. Viele Lieferanten erwarten einen uneingeschränkten Zugriff auf Anlagen, damit sie Wartungsarbeiten und Entstörungen durchführen können. Dies birgt sehr grosse Gefahren, weil somit die Zugriffskontrolle und Überwachung nicht mehr gewährleistet werden kann. Somit sind automatisierte Remote-Verbindungen strikte zu unterbinden.

(5) Folgende Grundsätze sind bei der Einführung eines Fernzugriffes auf die OT-Systeme einzuhalten:

- Administration, Wartung und Konfiguration aller Komponenten muss auch über ein Out-of-Band-Netz, z.B. Zugriff lokal, via serielle Schnittstelle, Netzwerk oder direkter Steuerung der Eingabegeräte (KVM[7]), möglich sein
- Fernzugriffe müssen über zentral verwaltete Zugangsserver durchgeführt werden. Die Zugangs-Server müssen in einer DMZ betrieben werden und eine Isolation der OT-Netzwerke sicherstellen. Es muss ein starkes 2-Faktor- Authentifizierungsverfahren benutzt werden.
- Direkte Einwahl Zugänge in Endgeräte sind grundsätzlich nicht erlaubt, der Aufbau von direkten VPN-Verbindungen ist zu verhindern.
- Es ist zwingend darauf zu achten, dass Fernzugänge nur mittels „Protokollbrüchen“ und Jump-Stationen ausgeführt werden. So kann eine direkte Verbindung zwischen verschiedenen Netzwerken unterbunden werden.
- Die Verwendung von Fernzugriffen muss (zentral) geloggt werden, wiederholte Fehlversuche müssen gemeldet werden.

(6) Anlagenbetreiber sollten nur autorisierten externen Benutzern erlauben, eine Remote-Verbindung zu zwischengeschalteten Authentifizierungsservern in einer DMZ herzustellen. Neben der Verwendung von Multifaktor-Authentifizierungsmethoden sollten definitive Regeln und Verbindungszustände klar identifiziert und aufrechterhalten werden. Diese Server (oft als "Sprungkästen" bezeichnet) bieten Verbindungen zu entfernten Computern, die wahrscheinlich weniger sicher sind als die Sprungboxen selbst. Zusätzlich zu Multifaktor-Authentifizierung und spezifischer Sicherheit, die sich

[7] KVM: Keyboard, Video und Maus

auf Benutzerrollen und kleinste Berechtigungen bezieht, sollten Anlagenbetreiber Jump-Boxen und alle Anwendungen oder Dienste härten, die keinen sicheren Remotezugriff ermöglichen.

b) Authentisierung

(1) Vor bestimmten sicherheitsrelevanten oder kritischen Aktionen muss die Autorisierung des anfordernden Benutzers bzw. der anfordernden Systemkomponente überprüft werden. Zu den relevanten Aktionen können auch das Auslesen von Prozess-Datenpunkten oder Konfigurationsparametern gehören.

(2) In den meisten ICS-Netzwerken werden viele verschiedene Systeme von einer Anzahl von verschiedenen Benutzern verwendet. Die Systeme müssen schnell aufgerufen werden, wenn Systemoperationen erforderlich sind. Corporate-Authentifizierung, Autorisierung und Account Management-Praktiken können für ICS problematisch sein, denn ICS‘s sind "immer in Betrieb", das Stoppen des Systems für Benutzer bzw. sich abzumelden und sich einzuloggen, ist in der Regel keine praktikable Option. Auch die von ICS-Lieferanten bereitgestellten Authentifizierungsprozesse können begrenzt sein. Das Verwalten vieler Benutzer mit verschiedenen definierten Rollen an verschiedenen Standorten wird zu einer Herausforderung. Abhilfe schafft da eigentlich nur eine zentrale Benutzerverwaltung. Der gleiche Authentifizierungsprozess kann den Zugriff auf viele Systeme (HMIs, Feldgeräte, SCADA-Server) und Netzwerke (Remote-Umspannungs-LANs) steuern, die die Verwendung gemeinsamer Anmeldeinformationen erfordern. Betreiber von Anlagen können den Zugang zu ICS-Systemen mit einem dezentralen, lokalen oder zentralisierten Ansatz steuern und überwachen. Das dezentrale Zugriffsmanagement erfordert, dass jedes System die Authentifizierung separat durchführt. Jedes System verwendet einen separaten Bereich von Benutzerkonten, Anmeldeinformationen und Rollen. Dieser Ansatz wäre eine gute Lösung für kleine ICS-Implementierungen, ist aber nicht gut skalierbar für grosse Unternehmen. Grosse Unternehmen verwenden normalerweise eine zentrale Benutzerverwaltung, um eine grosse Anzahl von Benutzern und Konten zu behandeln. Normalerweise wird es ein zentrales Authentifizierungssystem (z. B. Active Directory oder Lightweight Directory Access Protocol (LDAP) eingesetzt, welches die Konten verwalten. Ein Authentifizierungsprotokoll (z. B. Kerberos, Remote Authentication Dial-In User Service (RADIUS) oder Terminal Access Controller Access-Control System (TACACS)) kommuniziert zwischen dem Authentifizierungsserver und den ICS-Elementen. Ein zentraler Ansatz ist auch auf grosse Systemimplementierungen skalierbar. Allerdings kann es zu einer Schwachstelle oder Risiko werden, wenn es in ICS-Umgebungen verwendet wird. Die zentralisierten Server müssen sehr sicher sein, denn wenn der Authentifizierungsserver kompromittiert wird, kann die gesamte ICS-Umgebung kompromittiert werden. Das System muss auch im Notfall zur Verfügung stehen, somit werden redundante Server benötigt. Weiter muss eine lokale Benutzerverwaltung zur Verfügung stehen, da sonst bei Kommunikationsausfällen zur zentralen Benutzerverwaltung kein Zugriff auf die Systeme möglich ist. Diese Punkte stellen den Betreiber von versorgungskritischen Anlagen vor eine grosse Herausforderung. Eine Lösung könnte sein, dass die zentralen Benutzerdaten jeweils auf eine lokale Benutzerverwaltung kopiert werden und somit eine lokale Benutzerverwaltung erstellt wird, welche zentral administriert werden kann. Da jede stehende Verbindung ein potentielles Risiko darstellt, sollte die Verbindung zur zentralen Benutzerverwaltung speziell geschützt und überwacht werden. Es wird empfohlen, dass diese Verbindung nur aktiv ist, wenn ein Abgleich der Datenstände erfolgen muss, somit ferngesteuert unterbrochen werden kann.

Beispiel für System-Aufbau einer versorgungskritischen Anlage mit integrierten Sicherheitsfunktionen

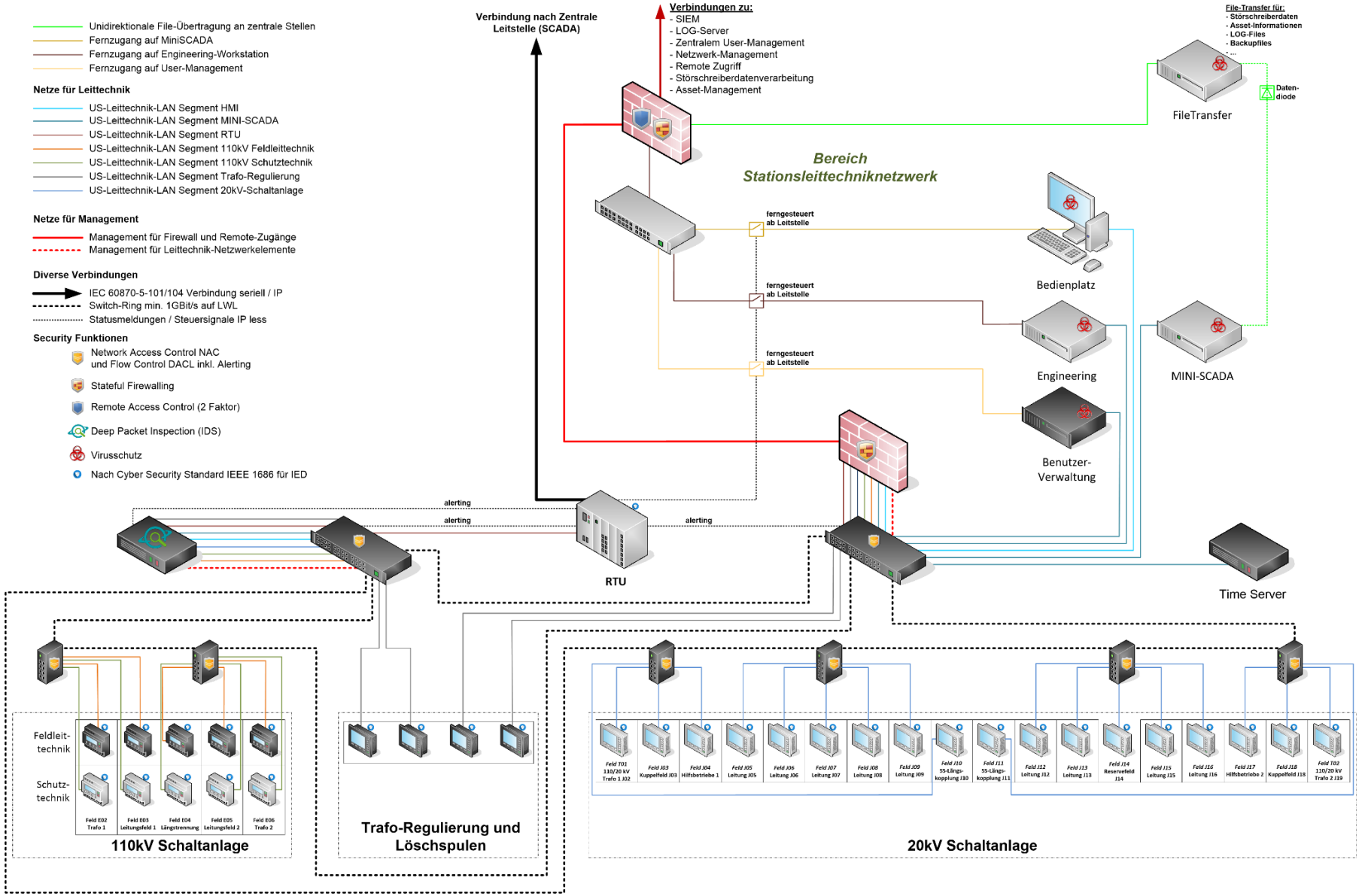

Abbildung 21 Beispiel für System-Aufbau einer versorgungskritischen Anlage

2.9 Systeme- und Komponenten-Sicherheit

2.9.1 Betriebssystem-, Firmware- und Applikations-Sicherheit

(1) Die Host- oder Workstation-Ebene implementiert eine andere Sicherheitsschicht. Firewalls schützen die meisten Geräte in einem Netzwerk vor einem Eindringen von aussen; ein gutes Sicherheitsmodell erfordert jedoch weitere Schichten der Verteidigung. Dies ist besonders wichtig für HMI-Clients, die sich über eine VPN-Verbindung oder auf andere Weise von ausserhalb der vertrauenswürdigen ICS-Netzwerkgrenze verbinden. Wie eine Kette, die so stark ist wie das schwächste Glied, ist ein Netzwerk so stark wie der schwächste Host.

(2) Viele empfohlene hostbasierte Schutzpraktiken und Sicherheitsmechanismen sind in PLCs und anderen industriellen Leittechnologien im Grossen und Ganzen - wenn überhaupt - nur wenig unterstützt. Defense-in-Depth-Kontrollmechanismen für diese Geräte gelten in der Regel auf der Netzebene. Viele HMI-Systeme basieren jedoch auf Standard-X86-Plattformen, welche die Administratoren so weit wie möglich „härten“ sollten (z.B. unbenutzte Dienste deaktivieren, nicht benötigte Ports deaktivieren, keine unnötigen Accounts, Zugriff beschränken, Kernelsperren verwenden), um die ursprüngliche Funktionalität gewährleisten zu können. Alle mitgelieferte Software, die auf dem System nicht benötigt wird, sollte entfernt werden. Ein HMI für Steuerungs- und Leitsysteme benötigt zum Beispiel keine Standard-Softwarepakete wie Textverarbeitung, Tabellenkalkulationen oder E-Mail-Clients, die normalerweise auf Standard-PC automatisch mitgeliefert werden.

(3) Systemkonfigurationen sollten während des gesamten Systemlebenszyklus aktiv verwaltet werden. Es gibt eine Anzahl von Techniken, die Unternehmen verwenden können, wie zum Beispiel das Erstellen eines sicheren „Images“, um neue Geräte zu konfigurieren bzw. Geräte neu zu erstellen, die nur die erforderliche Software enthalten und deren Konfiguration nur die erforderlichen Diensten und Ports aufweisen.

(4) Typische Komponentensicherheitsmassnahmen umfassen:

- Starke Kennwörter für alle Benutzerkonten und Standard- bzw. bekannte Benutzerkonten auf dem Gerät werden geändert (vorzugsweise sind starke Kennwörter und das Ablaufen von Kennwörtern durch das Betriebssystem unterstützt).
- Wo möglich sind Bildschirmschoner mit Passworteingabe installiert.
- Betriebssystem- und Hardware-Firmware-Patches sind installiert und werden aktuell gehalten.
- Protokolle auf den Geräten werden konfiguriert und überwacht.
- Nicht verwendete Dienste und Konten oder nicht mehr benötigte Dienste werden deaktiviert.
- Unsichere Dienste (wie telnet, remote shell (RSH) oder rlogin) sind durch sicherere Alternativen wie SSH ersetzt.
- Der Zugriff auf Dienste, die nicht deaktiviert werden können, sind beschränkt.
- Backups des Systems sind konsistent erstellt und getestet.
- Laptops und andere mobile Geräte, die nicht ständig mit dem Netzwerk verbunden sind, werden gesondert betrachtet und gesichert und allenfalls isoliert.

2.9.2 Malware-Schutz

(1) Schadsoftware (Viren und vor allem Trojaner) ist eine permanente, zentrale Bedrohung für jede ICS-Infrastruktur. Es sind Vorsichtsmassnahmen notwendig, um deren Einschleusen zu erkennen und zu verhindern. Die Software und die Komponenten der informationsverarbeitenden SCADA-Systemen der Netz-, Stations-, und Kraftwerksleittechnik sind durch die Schadsoftware verwundbar. Nebst Systemausfällen können auch Schäden durch Verfälschung von Daten und Systemfunktionen oder durch Ausspähen vertraulicher Informationen entstehen. Die Benutzenden dieser Systeme sind auf die Gefahren durch Schadsoftware hinzuweisen.

(2) Verantwortungsträger haben, soweit erforderlich, Massnahmen zum Schutz vor bzw. zum Erkennen und Entfernen von Schadsoftware und zur Überwachung zu treffen. Auf allen Systemen im Perimeter sowie auf allen Arbeitsplatzrechnern ist ein geeigneter Malwareschutz zu implementieren.

(3) Das Online-Scannen eines Rechners benötigt einiges an Rechenkapazität. Dies kann das Echtzeitverhalten von SCADA-Systemen nachteilig beeinflussen. Durch das sogenannte Blacklist-Verfahren werden definierte Anwendungen von der Ausführung ausgeschlossen. Beim Ansatz des Whitelist-Verfahrens verhält es sich umgekehrt, es dürfen nur definierte Anwendungen ausgeführt werden. Hier entfallen das ständige Scannen und die damit verbundene Rechnerbelastung.

(4) Folgende Punkte müssen für den Malware-Schutz beachtet werden:

- Auf ICS-Systemen mit Universalbetriebssystemen (z.B. Windows, Linux) sind nur gehärtete Betriebssysteme einzusetzen.
- Embedded Betriebssysteme sind, wenn möglich, so zu konfigurieren, dass nur die benötigten Services aktiv sind.
- Auf allen Systemen im Perimeter und auf allen Arbeitsplatzrechnern ist Malwareschutz zu implementieren.
- Die Sicherheits-Patches sind zeitnah einzuspielen und im Patch-Management priorisiert zu behandeln.
- Die ICS-Systeme sind zu überwachen, um mögliche Malware- und Hacking-Aktivitäten möglichst zeitnah zu erkennen.

2.9.3 Patch- und Schwachstellen-Management

(1) Mit dem Einspielen von Patches werden bekannt gewordene Sicherheitslücken geschlossen. Dies stellt eine Herausforderung für Systemadministratoren dar, da Systemupdates und Patches die ICS-Funktion stören können. Ein Patch zu einer ICS-Komponente kann die Funktionsweise ändern, was zu Komponentenversagen oder Funktionsverlust führen kann. Um festzustellen, ob das Patch unbeabsichtigte Konsequenzen hat, müssen alle Patches offline in einer Testumgebung mit identischer Hard- und Software wie in der Produktion getestet werden. Viele ICS verwenden ferner ältere Betriebssystemversionen, die der Hersteller möglicherweise nicht mehr unterstützt.

(2) Unternehmen sollten einen systematischen Patch- und Schwachstellen-Management-Ansatz für ICS entwickeln. Es sind regelmässig standardisierte Verfahren anzuwenden, um technische Schwachstellen in der Infrastruktur (Netzwerk, Clients, Server, Anwendungen etc.) systematisch zu erkennen und zu beheben.

(3) Administratoren sollten Verfahren für regelmässige Softwareupgrades und Patches einplanen. Die Entwicklung von Prozeduren, um Sicherheits-Patches zeitnah und aktuelle Software-Empfehlungen regelmässig zu applizieren, können die Angriffsfläche für Delinquenten entscheidend einschränken.

(4) Alle Komponenten des gesamten Prozesssystems müssen patchfähig sein. Das Einspielen eines Patches sollte möglichst ohne Unterbrechung des normalen Betriebs und mit geringen Auswirkungen auf die Verfügbarkeit des Gesamtsystems erfolgen. Beispielsweise ist eine primärtechnische Ausserbetriebnahme der kompletten Anlage zum Patchen der sekundärtechnischen Komponenten zu vermeiden. Bevorzugt werden die Patches zuerst auf den redundanten, passiven Komponenten eingespielt und nach einem Switch-Over-Prozess (Wechsel zur aktiven Komponente im Redundanzsystem) und einem darauffolgenden Test auf den restlichen Komponenten installiert. Der Hersteller muss einen Patchmanagement-Prozess für das gesamte System unterstützen, anhand dessen das Testen, Installieren und Dokumentieren von Sicherheitspatches und Updates gesteuert und verwaltet werden kann. Die Updates sollen vom Betriebspersonal, das diese Systeme administriert, eingespielt werden. Das Installieren bzw. Deinstallieren von Patches muss vom Anlagenbetreiber autorisiert werden und darf nicht automatisch geschehen.

(5) Grundsätze aus dem Change Management sind in der Regel auch im Patch Management anwendbar. Erfolgreiches Patch- und Schwachstellen-Managements umfasst zudem typischerweise:

- Regelmässige und standardisierte Verfahren, um technische Schwachstellen in der Infrastruktur zu erkennen und zu beheben, sind dokumentiert.
- Patches zur Schwachstellenbehebung werden zeitnah eingespielt und im Patch-Management priorisiert zu behandeln.
- Ein entsprechendes Konzept beschreibt die technischen Verfahren und Werkzeuge zur Schwachstellenerkennung und regelt die Rollen sowie Verantwortlichkeiten bei Risikobewertung, Patching, Nachführen von Inventar und Dokumentation.
- Gefundene Schwachstellen werden dokumentiert und im Rahmen der betrieblichen Verantwortung bezüglich Schweregrad eingestuft und behandelt.
- Wenn ein Patch zur Schwachstellenbehebung verfügbar ist, werden die Risiken vor der Einspielung bewertet und mit den Risiken der Schwachstelle verglichen.
- Neue Patches werden in einer adäquaten Test-Umgebung, die bezüglich Soft- und Firmware Releases möglichst identisch mit der produktiven Umgebung ist, getestet.
- Mit den Herstellern finden regelmässige Austausche statt.

2.9.4 Zugriffsmanagement und Zugriffskontrolle

(1) In vielen ICS-Netzen werden verschiedene Systeme von einer Vielzahl unterschiedlicher Benutzer verwendet. Die Systeme müssen oft auch schnell zugänglich sein, wie es z.B. der Systembetrieb erfordert. Unternehmenssichere Authentifizierungs-, Berechtigungs- und Kontoverwaltungsmethoden können für ICS herausfordernd sein, da ICSs "immer eingeschaltet" sind. Oftmals sind auch Authentifizierungsmechanismen, die von ICS-Lieferanten bereitgestellt werden, begrenzt; z.B. sind Passwörter nicht selten auf wenige Buchstaben beschränkt. Heute gängige Anforderungen an sichere Passwörter wird von der Hard- bzw. Firmware vielfach nicht oder nur teilweise unterstützt. Das Verwalten vieler Benutzer an verschiedenen Standorten wird zu einer Herausforderung, wenn man Systemzugriff und Benutzerrollenänderungen hinzufügt, ändert und entfernt. Der gleiche Authentifizierungsprozess kann den Zugriff auf viele Systeme (HMIs, Feldgeräte, SCADA-Server) und

Netzwerke (entfernte Subsystem-LANs) steuern, welche die Verwendung von gemeinsam genutzten Anmeldeinformationen erfordern.

(2) Diese Anforderungen seitens der Benutzer stehen zudem vielfach in Gegensatz zu den Anforderungen aus der Bedrohung bzw. Sicherheit: Mit zunehmender Vernetzung steigt auch die Gefahr einer grossflächigen und rasanten Verbreitung von Schadsoftware, was höhere Sicherheitshürden verlangt. Rollenbasierte Zugriffsmechanismen werden heute quasi standardmässig von Herstellern verlangt (siehe z.B. BDEW Whitepaper), und der Trend geht mit wachsender Virtualisierung und weiter steigender Bedrohung gar Richtung „Zero Trust“-Modell (Zero Trust-Sicherheit verlangt, das alte Paradigma „vertraue, aber kontrolliere“ aufzugeben und zu einem neuen, fast paranoiden Paradigma „vertraue nie, kontrolliere immer“ überzugehen).

(3) Grundsätzlich kann der Zugang zu ICS-Systemen entweder verteilt oder zentral gesteuert werden. Für die verteilte Zugriffsverwaltung muss jedes System die Authentifizierung separat durchführen. Jedes System verwendet einen separaten Satz von Benutzerkonten, Anmeldeinformationen und Rollen. Dieser Ansatz, welcher eine gute Lösung für kleine ICS-Implementierungen ist, skaliert nicht gut in grossen Unternehmen.

(4) Meist wird ein zentrales Konto Management System verwendet, um eine grosse Anzahl Benutzer und Konten zu verwalten. Normalerweise benötigt es ein zentrales Authentifizierungssystem (z.B. Active Directory oder Lightweight Directory Access Protocol - LDAP), um die Konten zu verwalten. Ein Authentifizierungsprotokoll (z.B. Kerberos, Remote Authentication Dial-In User Service (RADIUS) oder das Terminal Access Controller Access Control System (TACACS)) kommuniziert zwischen dem Authentifizierungsserver und dem ICS. Ein zentralisierter Ansatz ist für grosse Systemimplementierungen skalierbar, führt in ICS-Umgebungen jedoch auch zu zusätzlichen Risiken wie „Single Point of Failure“: Die zentralen Server müssen sehr sicher sein, da das gesamte Steuerleitsystem kompromittiert werden kann, wenn der Authentifizierungsserver gefährdet wird. Diese zentralen Server sind auch im Notfall erforderlich und könnten ohne Redundanz zu Verfügbarkeitseinbussen führen.

(5) Zusammenfassend müssen folgende Punkte berücksichtigt werden:

- Aufgrund von Geschäfts- und Informationssicherheitsanforderungen wird eine Richtlinie zur Zugangskontrolle dokumentiert und umgesetzt.
- Rollenbasiertes Berechtigungskonzept definieren und implementieren; sämtliche Zugriffe auf Anwendungen und Systeme gemäss rollenbasiertem Berechtigungskonzept implementieren.
- Die Anwendung von Bedingungen und Vorschriften für die Verwendung von Gruppenkonten, wo die Verwendung von persönlichen Benutzerkonten nicht möglich ist, muss genaue Regeln für Ausnahmen sowie ergänzende Massnahmen beschreiben, um ein ausreichendes Mass an Zugangssicherheit und Rückverfolgbarkeit zu gewährleisten.
- Bedingungen und Vorschriften, die für Systeme gelten, die keine starke Kennwortrichtlinie unterstützen oder eine solche aus betrieblichen Gründen nicht möglich ist, sollten insbesondere ergänzende Massnahmen festgelegen, um eine ausreichende Zugangssicherheit zu gewährleisten.
- Der Benutzer darf nur Zugang zum Netz und den Dienstleistungen haben, die ausdrücklich zugelassen sind.
- Ein formaler Benutzerregistrierungs- und Abmeldeprozess ist implementiert, um die Zuweisung von Zugriffsrechten zu ermöglichen.

- Ein formaler Nutzerzugriffsvorbereitungsprozess soll durchgeführt werden, um die Zuweisung oder das Widerrufen von Zugriffsrechten für alle Benutzertypen auf alle Systeme und Dienstleistungen zu ermöglichen.
- Die Zuteilung und Nutzung von privilegierten Zugriffsrechten ist eingeschränkt und kontrolliert.
- Die Zuordnung der geheimen Authentifizierungsinformationen wird durch einen formalen Managementprozess kontrolliert.
- Anlageneigner müssen die Zugriffsrechte der Nutzer in regelmässigen Abständen überprüfen.
- Die Zugriffsrechte aller Mitarbeitenden und externen Dienstleistenden auf Informations- und Informationsverarbeitungseinrichtungen werden nach Beendigung ihres Arbeitsverhältnisses, Vertrages oder einer Vereinbarung entfernt oder einer Änderung angepasst.
- Die Benutzer müssen die vorgeschriebenen Praktiken in der Verwendung von Passwörtern befolgen und anwenden.
- In der Prozesskontrolldomäne ist es nicht immer möglich, die Verwendung von sicheren Passwörtern zu gewährleisten, z. B. Legacy-Systeme erlauben oft keine individuellen Passwörter und / oder Passwörter mit notwendiger Stärke
- Es ist häufig unmöglich, Systeme mit zentralen Verzeichnisdiensten zu betreiben, die in dezentralen Anlagen wie Umspannwerken oder verteilten Erzeugungseinheiten betrieben werden, was bedeutet, dass lokale Konten und Passwörter verwendet werden müssen. Dies macht es praktisch unmöglich, Passwörter regelmässig zu wechseln.
- Es sollte daher dem Benutzer eindeutig angezeigt werden, wann die allgemeine Kennwortrichtlinie gilt, wo verschiedene Passwörter verwendet werden sollen oder wo es überhaupt nicht möglich ist, irgendwelche Passwörter zu verwenden (Legacy-Systeme).
- Vor allem in Situationen, in denen nur ein einziges Passwort für den allgemeinen Systemzugang verwendet wird, sollte das Passwort so sicher wie möglich gewählt werden. Insbesondere sollten die von den Systemanbietern verwendeten Standardpasswörter als unsicher und weithin bekannt angesehen werden. Passwörter sollten nur Personen zugänglich sein, die am Betrieb des Systems beteiligt sind.
- Diese Situationen sind zu dokumentieren und periodisch zu überprüfen.
- Der Zugang zu Informationen und Anwendungssystemen muss eingeschränkt in Übereinstimmung mit der Zutrittsrichtlinie erfolgen.
- Passwortmanagement-Systeme sollen interaktiv sein und müssen qualitativ geforderte Passwortregeln unterstützen bzw. erzwingen.
- Falls durch die Zutrittskontrollrichtlinie erforderlich, soll der Zugang zu Systemen und Anwendungen durch ein sicheres Anmeldeverfahren kontrolliert werden.

2.9.5 Backup-Management und Systemwiederherstellung

(1) Das Erstellen von Backups kann verschiedene Gründe und Absichten beinhalten: Daten und Informationen werden gegen Verlust oder Manipulation gesichert oder langzeitig auf verschiedenen Medien archiviert; Software und deren Konfiguration können konserviert werden oder dienen der Resilienz im Falle eines Schadsoftware Angriffs (z.B. Verschlüsselung); schnelle Wiederherstellung im Falle eines physischen Unterbruches etc. Solche Backups wurden in der Vergangenheit meist auf kostengünstigen Medien wie Tapes erstellt. Mit dem Preiszerfall von physischen Platten werden sie zunehmend auch online auf hierarchisch zur Verfügung gestellten Platten erstellt. Während im ersten Fall meist sogenannte Grosseltern- Eltern- Kinder-Generationen abgesetzt gesichert und über längere Zeit gelagert wurden, werden sie im zweiten Fall oft nur noch über eine definierte Periode wie typischerweise 3 Monate online aufbewahrt. Dies kann jedoch gerade im Falle eines

Schadsoftwarebefalls (typisch Ransomware), der erst nach einer längeren Zeit realisiert wird, zum vollständigen Verlust von Daten, Informationen, Software und Konfiguration führen. Deshalb ist es wichtig, dass in solchen Fällen allenfalls Archivierungssysteme zur Anwendung gelangen, damit Daten nicht verloren gehen, gestohlen oder durch Ransomware verschlüsselt, so unzugänglich gemacht, und letztlich verlustig werden.

(2) Backups müssen sowohl in der Übermittlung als auch in der Lagerung sicher gegen alle Risiken, die auch auf Daten und Systeme im produktiven Betrieb anwendbar sind, aufbewahrt werden. Dasselbe gilt auch während möglicher Wiederherstellungsphasen, während derer gesicherte Backups wieder in einer produktiven, temporären oder übergangsmässigen Umgebung hergestellt werden müssen.

(3) Im Rahmen des unternehmensweiten Geschäftskontinuitätsplanes (Business Continuity Plan) muss auch ein Plan zur Wiederherstellung der IT- und OT-Mittel erarbeitet werden. Ein solcher Disaster Recovery Plan basiert auf der Kritikalität aus den geschäftlichen Anforderungen, welche definieren, was in welchem Zeitraum und in welcher Reihenfolge wiederhergestellt werden muss. Darauf aufbauend werden detaillierte Pläne erstellt, die „handbuchmässig“ Anleitungen zum Wiederanlauf geben, so dass auch Personen, welche die notwendigen technischen Grundkenntnisse haben aber vielleicht nicht über die unternehmensspezifischen Detailkenntnisse verfügen, eine Umgebung wieder herstellen können. Solche Pläne müssen kontinuierlich nachgeführt werden, wenn Änderungen an Umgebungen gemacht werden, und sie müssen auch periodisch trainiert und überprüft werden. Dies geschieht typischerweise jährlich in Recovery-Tests und kann von reinen papierbasierten „Walkthroughs“ bis hin zu umfänglichen Notfallszenario-Simulationen durchgeführt werden.

(4) Backup und Recovery Massnahmen umfassen:

- Daten Backup: Das Erstellen von Sicherungskopien von Daten sowie Software und Konfigurationen werden definiert, regelmässig durchgeführt und nach einem vereinbarten Zyklus getestet.
- Backup-Medien werden in einer entfernten Lokation sicher gegen Umwelteinflüsse (Temperatur, Feuer, Feuchtigkeit, elektromagnetische Strahlung etc.) sowie gegen Diebstahl, Manipulation oder Vernichtung aufbewahrt.
- Die Kontinuität der Informationssicherheit ist im unternehmensweiten Business Continuity Management System integriert.
- Das Unternehmen bestimmt ihre Anforderungen an die Informationssicherheit und die Kontinuität im Normalfall und in Notfall-, Katastrophen- und Krisensituationen und setzt diese um.
- Um die Anforderungen an die Kontinuität gewährleisten zu können, muss das Unternehmen Prozesse, Verfahren und Kontrollen dokumentieren, umsetzen und pflegen.
- Das Unternehmen überprüft die etablierten und umgesetzten Massnahmen zur Informationssicherheit und deren Kontinuität in regelmässigen Abständen, um sicherzustellen, dass sie gültig und wirksam sind.
- Gesetzliche, regulatorische und unternehmerische Anforderungen an die Langzeitarchivierung sind definiert, umgesetzt und werden regelmässig überprüft.
- Disaster Recovery Plan (DRP): Ein Gesamtplan mit personellen Verantwortlichkeiten, Erreichbarkeitsplänen, alternativen Einrichtungen und detaillierten Wiederanlaufplänen ist erstellt.

2.9.6 Spezialfälle (Feldgeräte, virtuelle Elemente usw.)

a) Feldgeräte

(1) Viele Feldgeräte (intelligente Feld-/Schutz-Geräte IED, ältere SPS und RTU) verfügen oft nicht oder nur eingeschränkt über die Sicherheitsfunktionen, die andere Komponenten wie zum Beispiel Windows PC aufweisen. Sie können daher nicht zentral verwaltet werden. Meistens werden diese Geräte nur physisch geschützt, indem sie in verschlossenen Räumen oder Schränken betrieben werden. Wichtig wäre jedoch auch der Schutz der Geräte-Konfiguration ohne die benötigte Funktionalität einzuschränken.

b) Mobile Geräte (Smartphones, Tablets)

(1) Zunehmend werden auch Smartphones, Tablets und ähnliche Geräte für die lokale Steuerung/Überwachung eingesetzt. Damit über diese keine Malware in die Stationsleittechnik gelangen kann, müssen die mobilen Geräte so weit wie möglich gesichert werden. Weiter sollte eine Stelle die verwendeten Geräte verwalten, um sicherzustellen, dass die Sicherheitsstandards des Unternehmens erfüllt werden. Zu beachten sind auch die verwendeten Schnittstellen zur Stationsleittechnik (z.B. WLAN). Diese erfordern entsprechende Sicherungsmassnahmen, damit sie nicht für den unberechtigten Zugang auf die Stationsleittechnik genutzt werden können.

2.10 Sicherheits-Monitoring

„Sicherheit ist kein Zustand, Sicherheit ist ein Prozess!“

(1) Dieser Merksatz gilt je länger je mehr. Ein als „sicher“ bezeichnetes System beschreibt immer nur den Zustand zu diesem Zeitpunkt. Der Gedanke der „Sicherheit als kontinuierlicher Prozess“ anerkennt hingegen, dass es eine absolute Sicherheit nicht gibt und deswegen immer mit neuen sicherheitsrelevanten Vorfällen zu rechnen ist. Entscheidend dabei ist, dass in der Organisation vorgängig die Kapazitäten aufgebaut werden, um neu auftretende Sicherheitsvorfälle rechtzeitig entdecken zu können.

2.10.1 Grundsätze und Grundlagen

(1) Der Einsatz von Monitoring-Systeme und Netzwerke für Anpassungen um anomale Verhaltensweisen oder Angriffssignaturen zu erkennen, kann in einer ICS-Umgebung schwierig sein. Die Überwachungs- und Erkennungsfunktionen sind jedoch für das Defense-in-Depth-Konzept zum Schutz kritischer Infrastrukturen unerlässlich. Absolut gehärtete und überwachte Übergänge in andere Netze reichen nicht aus, um kritische Assets vor unberechtigtem Zugriff wirksam zu schützen. Denn für jeden Schutz, der in einer Netzwerkumgebung eingesetzt wird, kennen Bedrohungsakteure eine Methode, um sie zu umgehen. Das Konzept der Verteidigung in der Tiefe sagt, dass ein System eines Unternehmens das Eindringens frühzeitig erkennt und eskaliert, damit defensive Massnahmen ergriffen werden, bevor die Funktionen der kritische Infrastrukturen beeinträchtigt werden. Die meisten IT-Unternehmen haben ein gewisses Mass an Monitoring auf Unternehmensebene, aber sie setzen sie nur selten in die ICS-Netze ein.

(2) Ohne Systemüberwachung könnten Eindringlinge das System verletzen und niemand würde von dem Eindringen wissen, bevor sie ihr Ziel erreicht haben. Während die ICS-Vendor-Community sich der Notwendigkeit einer zentralen Überwachung der ICS-Sicherheit bewusst wird, steht die Integration von Standard-Monitoring-Funktionen in das ICS in den Kinderschuhen. Anlagenbetreiber können und sollten Massnahmen ergreifen, um sicherzustellen, dass Sicherheitspersonal und OT-

Betreiber über Änderungen an Systemen oder Verhaltensweisen wissen, die auf ein potenzielles Eindringen in die ICS-Umgebung hinweisen.

(3) Unternehmen können ihre Netzwerke überwachen und Informationen über Netzwerke in vielerlei Hinsicht sammeln, wie z. B. die Verwendung zentralisierter Syslog-Server für Linux- und Netzwerkgeräte und die zentrale Erfassung von Windows Events mit WinRM (Windows Remote Management) und WEVTUTIL (Windows Event Log Tool). Allerdings müssen diese Ereignisse (Protokolle) permanent überprüft werden. Lösungen, wie z. B. Sicherheitsinformations- und Eventmanagement (SIEM), kombinieren das Sicherheitsinformationsmanagement (SIM) und das Sicherheitsereignismanagement (SEM) und können Informationen aus mehreren Quellen sammeln, protokollieren und korrelieren und auf anomale oder spezifizierte Aktivitäten aufmerksam machen. Weiter können diese Systeme eine Echtzeitanalyse zur Verfügung stellen. Canary‘s und Honeypots / Honeynets können auch jede nicht autorisierte Intrusion markieren, und Anlagenbetreiber sollten sie für den Einsatz in Bereichen mit hohem Kritikalitäts- / Hochrisiko berücksichtigen. Für die IT-Forensik ist die Einführung eines SIEM unerlässlich. So können erfolgte Angriffe und ausgenutzte Schwachstellen erforscht und gefunden werden.

2.10.2 Intrusion Detection und Präventionssysteme

(1) ICS-Umgebungen bieten eine einmalige Gelegenheit um Schutzmechanismen im Netzwerk zu überwachen. Trotz erheblichem Netzwerkverkehr ist der Verkehr sehr einfach, da es sich um eher statische Netze handelt. Beispielsweise kommuniziert die PLC in einer typischen ICS-Umgebung standardisiert mit dem HMI und dem Archivierungsserver. Alle Anwendungen und Dienste auf dem Prozessleitsystem (PCS) sind bekannt und die Protokolle, Verbindungen und der nötige Netzwerkverkehr sind definiert und vorhersehbar. Anlagenbetreiber können eine IDS-Lösung verwenden, um so problemlos die gesamte ICS-Umgebung zu überwachen und eine Alarmierung für jegliches Ereignis, auch ausserhalb des normalen Betriebs, zu implementieren. Ein IDS basiert auf der passiven Überwachung des Netzwerkverkehrs. Der erwartete Netzwerkverkehr ist deterministisch, und Abweichungen werden als Auslöser für die Alarmierung verwendet. Einfache Regeln können geschrieben werden, umso IP-Quellen und Ziele, Protokolle, Längen von Paketen usw. zu überwachen. Auch viele ICS-Anbieter können Definitionen und Beschreibungen für ihre IDS-Systeme bereitstellen.

(2) IPS-Lösungen kommen immer in Verbindung mit Firewalls oder ICS-Geräten zum Einsatz und haben die Möglichkeit, den Netzwerkverkehr zu blockieren, welcher die definierten Regeln nicht erfüllt. Viele Anbieter und Anlagenbetreiber werden bei der Verwendung von IPS unsicher und vorsichtig, weil das Blockieren eines Dienstes die Funktion der Anlagen beeinträchtigen kann und somit der kontinuierliche Betrieb nicht mehr gewährleistet ist. Aufgrund der deterministischen Natur des ICS-Verkehrs können sie jedoch nur auf extreme Anomalien abgestimmt werden. IDS und IPS sind ein wichtiger Teil der Defense-in-Depth-Strategie. In einem ICS-Netzwerk können sich viele unvermutete Schwachstellen befinden. Ein IDS / IPS bietet eine automatisierte Möglichkeit, auf das Unerwartete zu achten und darauf zu reagieren. Mit IDS / IPS System können aber nicht alle Probleme eliminiert werden. IDS und IPS können wie folgt grob umschrieben werden:

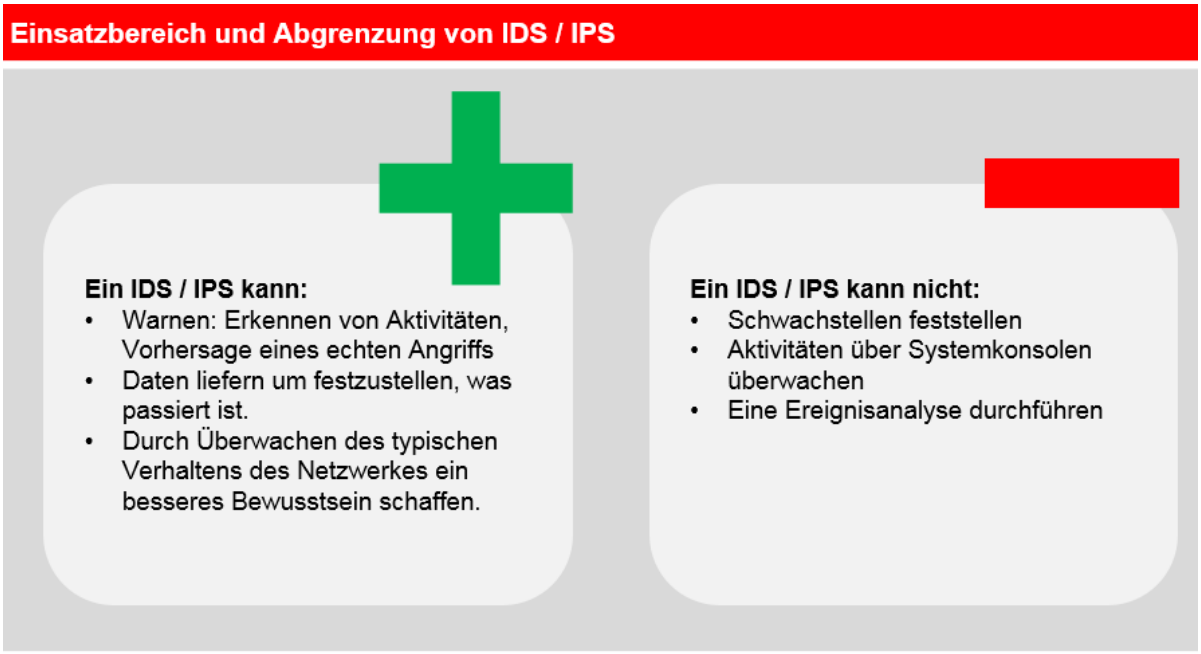

Abbildung 22 Einsatzbereich und Abgrenzung von IDS / IPS

Funktion	Beschreibung
IDS	Ein Intrusion Detection System (englisch intrusion „Eindringen“, IDS) bzw. Angrifferkennungssystem ist ein System zur Erkennung von Angriffen, die gegen ein Computersystem oder Rechnernetz gerichtet sind. Das IDS kann eine Firewall ergänzen oder auch direkt auf dem zu überwachenden Computersystem laufen und so die Sicherheit von Netzwerken und Computersysteme erhöhen. Erkannte Angriffe werden meistens aufgesammelt in Log-Dateien und dem Benutzer oder Administrator mitgeteilt; hier grenzt sich der Begriff von Intrusion Prevention System (englisch prevention „Verhindern“, IPS) ab, welches ein System beschreibt, dass Angriffe automatisiert und aktiv verhindert.
IPS	Intrusion Detection und Intrusion Prevention Systeme sind Werkzeuge, die IT-Systeme oder Netze aktiv überwachen. Das Ziel ist es, Ereignisse herauszufiltern, die auf Angriffe, Missbrauchsversuche oder Sicherheitsverletzungen hindeuten. Ereignisse sollen dabei zeitnah erkannt und gemeldet werden. Die Verfahren basieren auf Mustererkennung, um ein Abweichen von einem Normalzustand zu signalisieren. Mit heuristischen Methoden sollen auch bisher unbekannte Angriffe erkannt werden. Während IDS Angriffe nur erkennen, sollen IPS diese auch abwehren bzw. verhindern. Allerdings wurde der Begriff ursprünglich durch das Marketing geprägt, was dazu führte, dass teilweise kontroverse Vorstellungen darüber existieren, inwiefern von einem Intrusion-Prevention-System gesprochen werden kann.

Tabelle 11 Funktionsbeschreibungen von IDS und IPS

(3) Intrusion Detection System (IDS) sind autarke Systeme, die Eindringlinge erkennen und Attacken auf IT-Systeme und Netze vermeiden. Diese IDS-Überwachungssysteme sollten nicht bekannt sein, keine Dienste anbieten, Angriffe protokollieren, Eindringlinge erkennen und nach Möglichkeit Gegenmassnahmen einleiten. Alles was im Netzwerk anormal ist, sollte von dem IDS-System erkannt und protokolliert werden. Dazu benutzen IDS-Verfahren Sensoren resp. Sniffer, die anormalen Datenverkehr aufspüren und mit vorgegebenen Mustern vergleichen. Dabei unterscheidet man zwischen dem Erkennen von Missbrauch, dem Misuse Detection, und dem Aufspüren von Anomalien, dem Anomaly Detection.

(4) Das Misuse Detection basiert auf dem Vergleich von Mustern oder Signaturen. Dazu werden die erfassten Muster mit anderen Mustern aus einer Datenbank verglichen, die vorwiegend von den Eindringlingen benutzt werden. Bei dieser Methode, dem sogenannten Pattern Matching, werden nur bereits bekannte Angriffsmuster erkannt. Neue Angriffe, von denen noch kein Muster vorliegt, bleiben unerkannt.

(5) Beim Anomaly Detection wird hingegen jedes Verhaltensmuster, das sich ausserhalb des normalen Datenverkehrs bewegt, als Angriff gewertet. Dadurch werden auch Abweichungen von bisherigen Angriffen erkannt. Eine Pflege der Angriffsmuster in einer Datenbank entfällt. Allerdings muss beim Anomaly Detection definiert werden, welches Muster zum normalen Datenverkehr gehört, wodurch sich die Schwelle für Fehlalarme erhöhen kann.

(6) Die beiden Verfahren verdeutlichen die Entwicklung vom IDS-System hin zu Intrusion Prevention Systems (IPS), die bestimmte Datenpakete erst gar nicht passieren lassen.

Nachweisverfahren	
Signaturbasierte Erkennung	- Überwacht bestimmte Ereignisse - Kontrolliert nur das, was ihm gesagt wurde - Kann mit jeder bekannten Bedrohung umgehen - Erkennt keine Netzwerkkonfigurationsänderungen - Hohe objektive Inspektion - Vorhersagbares Verhalten - Einfache Handhabung
Anomalie-basierte Erkennung	- Überwacht Trendveränderungen - Lernt von allmählichen Veränderungen - Kann mit unbekannten Bedrohungen umgehen, jede Intrusion führt zu einem Alarm - Empfindlich auf Änderungen in Netzwerken - Subjektiv, anfällig für Fehlinterpretationen - Unvorhersehbares Verhalten - Das System muss vollständig vertrauenswürdig sein

Tabelle 12 Unterschiede zwischen signaturbasierter- und Anomalie-basierter Erkennung

Auswahlkriterien	
Signaturbasierte Erkennung	- Scannt den Netzwerkverkehr (Pakete) auf bekannte Muster - Scannt nur den Verkehr auf oder von seinem eignen Netzwerk - Kann beide Seiten einer Verbindung scannen - Kann reagieren und Verkehr blocken (IPS-Modus) - Unterscheidet den Verkehr nicht - oft weiss er nicht, ob ein System Windows, Linux oder eine SPS ist
Anomalie-basierte Erkennung	- Muss das System lehren, den "normalen" Netzwerkverkehr zu identifizieren (und was ist, wenn Lernzeit Angriffe beinhaltet?) - Erkennt Abweichungen vom normalen Verhalten - Schwieriger manipulierbar oder zu täuschen - Keine Kenntnisse von Angriffssignaturen erforderlich - Kann mehr Fehlalarme hervorrufen - in einer dynamischen Umgebung sehr schwer und aufwendig zu implementieren

Tabelle 13 Grundlagen der Erkennung für signatur- und Anomalie-basierte Systeme

(7) Für die IDS-Technologie gibt es auch netzwerkbasierte Lösungen, Network Intrusion Detection (NIDS) und hostbasierte, Host Intrusion Detection System (HIDS).

(8) Im Gegensatz zu einem Intrusion Detection System (IDS) hat das Intrusion Prevention System (IPS) keine überwachende und alarmauslösende Funktion, sondern kontrolliert unmittelbar den Traffic. Das IPS-System ist direkt in die Datenleitungen geschaltet und überwacht die ein- und ausgehenden Datenpakete der Netzwerk-Komponenten. Angriffe und vom normalen Datenverkehr abweichende Bitmuster werden über Signaturen erkannt und blockieren den Datenverkehr. Unterstützt wird diese Sperrfunktion durch intelligente Verhaltensmuster und anomale Algorithmen, die auf der Applikationsebene arbeiten.

(9) IPS-Systeme sollten die Datenanalyse in Hochgeschwindigkeit ausführen können und dürfen selbst unter Hochlast nicht den legitimen Datenverkehr blockieren. Die Schutzmechanismen wie Signaturanalysen, das Erkennen von Protokollabweichungen, Firewall-Funktionen und Zugriffskontrollen müssen robust sein.

2.10.3 Sicherheitsvorfall und Ereignisüberwachung

(1) Sicherheitsüberwachungsprotokolle enthalten Informationen über die Anmeldungsaktivität, Ressourcennutzung, Dateiänderungen und andere sicherheitsrelevante Informationen. Ohne ordnungsgemäss konfigurierte und gepflegte Audit- und Protokollierungspraktiken können Incident Response Teams oft nicht die Bedeutung eines potenziellen Ereignisses bestimmen. Richtig konfigurierte Überwachungsprotokolle auf Netzwerk-, Host- und Anwendungsebene liefern kritische Informationen, um festzustellen, wie ein Ereignis aufgetreten ist, welche Auswirkungen und welchen Umfang das Problem hat und wie die zukünftigen Ereignisse am besten abgewehrt werden können.

(2) Umfassende Protokollmanagement- und Analyserichtlinien legen die Mindestanforderungen an Geräte, Betriebssysteme und Anwendungen fest. Sicherheitseinstellungen und Benutzerzugriffskontrollen erzwingen diese Anforderungen. Wenn Anlagenbetreiber Systeme und Anwendungen nicht zum Erfassen von Schlüsselereignissen konfigurieren, können sie keine wichtigen Ereignisdaten erfassen und Incident-Response-Teams haben möglicherweise keine ausreichenden Informationen, um die Ursache eines Ereignisses zu ermitteln.

(3) Die Festlegung eine Baseline der erwarteten Verkehrs- und Prozessfunktionalität für normale und aussergewöhnliche Operationen und die Systemnutzung ermöglicht es, dass die Prozesssteuerung und die Steuerung von Betriebssystemen von ungewöhnliche Datenverkehrs- oder Benutzeraktionen isoliert werden umso möglicherweise auf potenzielle sicherheitsrelevante Ereignisse hinweisen können.

(4) Neuere Betriebssysteme und Anwendungen bieten detailliertere Konfigurations- und Event-Auditing-Optionen. Die Verwendung der Standardkonfiguration für die meisten Betriebs- und Anwendungsprotokolle bietet jedoch nur minimale Überwachungs-und Log-Funktionen und Betreiber können ein kritisches Ereignis verpassen. Es ist wichtig, dass das Betriebs- und Sicherheitspersonal im ICS-Umfeld eine Überprüfung aller Überwachung- und Log-Fähigkeiten durchführt und die Systeme so konfiguriert, dass sie nur die Daten bereitstellt, die für die Erfassung aller potenziell relevanten Ereignisse erforderlich sind. Es ist sicherzustellen, dass die Einstellungen keine nicht benötigten Protokolle generieren, welche die Systemspeicherkapazitäten überfordern können. Bei Standardkonfigurationen können Daten überschrieben werden. Daher exportieren Sie alle Logs und Protokolle zu einem zentralen Server oder Event-Management-System, um sicherzustellen, dass sie wenn nötig verfügbar sind.

2.10.4 Sicherheitsvorfall und Ereignisüberwachung SIEM (SIM und SEM)

(1) SIEM-Technologien unterstützen nicht nur den Incident-Response-Prozess, sondern können auch ICS-Betreiber unterstützen. Wenn sie korrekt konfiguriert und analysiert werden, können die Daten bei der Vorhersage von Geräteausfällen, Ausrüstungskapazitäten und Ausfallpunkten sowie bei der Bereitstellung von Sicherheitsinformationen helfen. Anlagenbetreiber können sie so konfigurieren, dass sie Warnungen bereitstellen, wenn ein potenzieller Sicherheitsvorfall eintritt. Sie können eine grosse Menge an nötigen Event- und Log-Daten zusammenfassen, die sich von den ICS-Komponenten ansammeln. Durch die Bereitstellung von Sichtbarkeit in aggregierte Sicherheitsdaten können SIEM die Reaktionszeit des Auftretens minimieren.

(2) Ein SIEM zentralisiert Daten von Netzwerkgeräten, Betriebssystemen, Applikationen und Datenbanken in komplexen ICS-Umgebungen. Es rationalisiert den Prüfprotokoll-Überprüfungsprozess, indem er Protokolle von mehreren Systemen in eine Lösung portiert, welche die Zeit und den Aufwand für manuelle Log-Auswertungen eliminiert. Betreiber können ein SIEM so einrichten, dass mehrere Log-Formate aus weit verteilten Quellen integriert werden. Die nötigen Informationen können somit remote und automatisch gesammelt werden.

(3) Das SIEM kann auch IDS / IPS-Informationen und Scan-Ergebnisse integrieren und anschliessend Warnungen auf identifizierten Verkehrsmustern generieren. Die SIEM-Analyse-Engine beschleunigt die Datenverarbeitung und die Formatierungszeit und macht diese Prozesse somit preiswerter. Weiter wird es somit einfacher Funktions-, Betriebs- und Sicherheitsdaten zu überprüfen. Darüber hinaus bietet die Verwendung eines SIEM die Möglichkeit, bestimmte Ereignisse für Compliance-Reporting, Ursachenfehleranalyse und Incident-Erkennung auszuwählen.

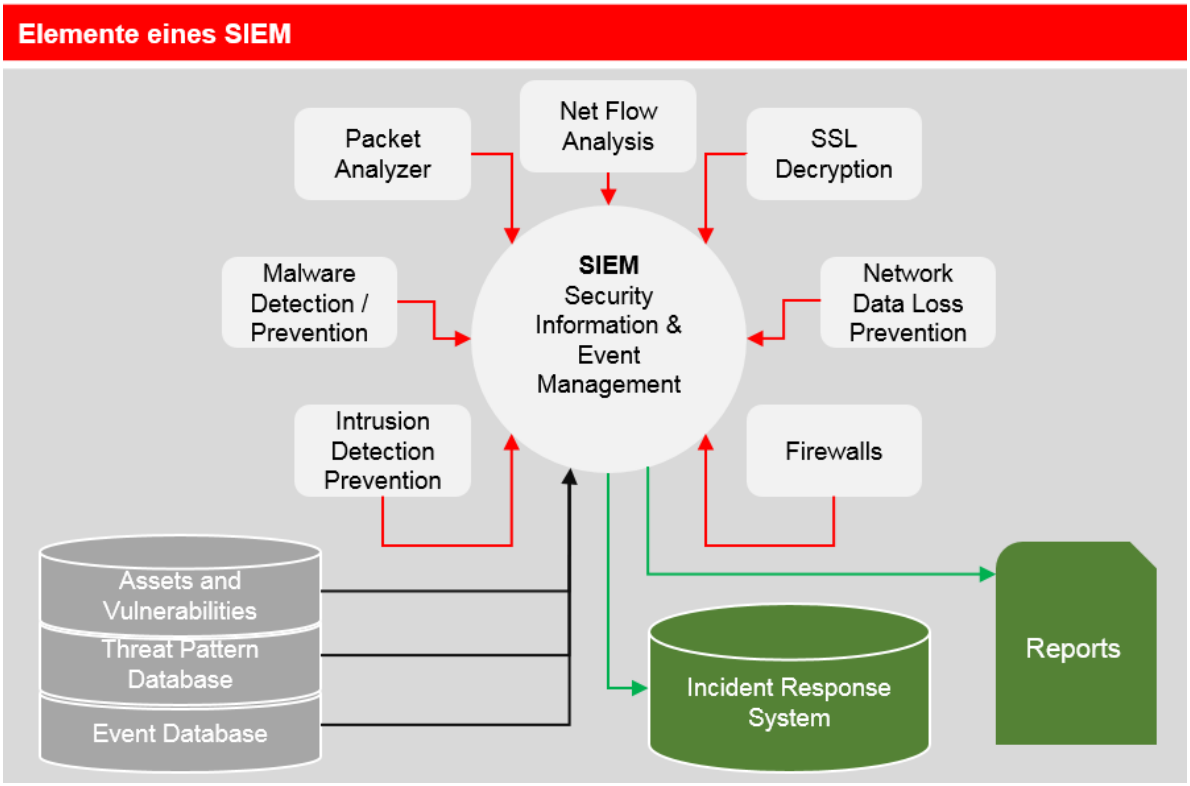

Abbildung 23 Elemente eines SIEM (1)

Abbildung 24 Funktionen eines SIEM (2)

a) SIM (Security Information Management)

(1) Security Information Management (SIM) sind Systeme in denen Ereignisse und Logfiles von den verschiedensten Stellen in Kommunikationssystemen gesammelt werden, um sie in Echtzeit zu verknüpfen, archivieren, verarbeiten, analysieren und um daraus aktuelle und historische Berichte zu erstellen. Ein solches Security Information Management (SIM) entspricht dem Log-Management.

(2) Das SIM-Management überwacht das Netz in Echtzeit und untersucht es auf kritische Ereignisse. Der Ansatz für die Bewertung der Ereignisse kann aus verschiedenen Sichtweisen erfolgen, so beispielsweise aus Benutzersicht, bei der sich die Fragen nach dem wo, wann und wie sich jemand eingeloggt hat, auf welche Systeme er zugegriffen hat und welche Ereignisse dadurch ausgelöst wurden.

(3) Da die Daten der SIM-Systeme aus verschiedenen Quellen stammen, von Netzwerkkomponenten, Systemen, Firewalls, Anwendungen oder Virenscannern, ist deren Inhalt auf die eigene Funktion ausgerichtet. Sie bewerten daher die auftretenden Ereignisse aus vollkommen unterschiedlichen Betrachtungswinkeln. Darüber hinaus haben sie die verschiedensten Formate, die eine SIM-Plattform verarbeiten muss.

(4) Gemeinsam mit dem Security Event Management (SEM) bildet das Security Information Management (SIM) das Security Information and Event Management (SIEM).

(5) Log Management entspricht dem Begriff SIM (Security Information Management) und steht für die zentrale Sammlung, Übertragung, Speicherung, Analyse und Weiterleitung von Log-Daten aus Netzwerk-Komponenten, Betriebssystemen und Applikationen. Typische Funktionen sind richtlinienorientierte Analysen, auch zu Trends, periodische Berichte und Basisfunktionen für Alarm-Meldungen. Damit ist es die Grundlage für die IT-Forensik und das Service Level Management. Je nach Anbieter bietet Log Management die revisionssichere Log-Daten-Speicherung und berücksichtigt bei der Datendarstellung die Richtlinien des Datenschutzes.

b) SEM (Security Event Management)

(1) Das Security Event Management (SEM) ist durch Echtzeitüberwachung, die Korrelation von Logfiles nach vorgegebenen Richtlinien, die Benachrichtigung und die Darstellung auf der Konsole und die Alarmfunktionen gekennzeichnet. Das Security Event Management deckt Funktionen von IDS- und IPS-Systemen für die Erkennung und den Schutz vor Eindringlingen ab und überwacht den Netzwerkverkehr auf Anomalien und sich wiederholende Muster.

(2) SEM (Security Event Management) übernimmt die Korrelation von Logs anhand definierter Richtlinien, gleicht sie automatisiert mit Standards wie ITIL, COBIT, SOX oder ISO ab und verfügt über leistungsfähige Echtzeit-Alarmfunktionen. SEM deckt sich teilweise mit IDS/IPS (Intrusion Detection und Intrusion Prevention System). Netzwerk-basierend überwachen diese die Auslastung und Kommunikation im Netz sowie Ports und erkennen Muster respektive Abweichungen im Netzwerkverkehr. Als Host-basierende Lösungen kontrollieren sie Manipulationen von Dateien und überwachen beispielsweise Gruppenrichtlinien und Benutzerkonten.

Vorgehensweise zu mehr Cybersecurity

3. Bestimmung des implementierten Sicherheitslevel (Assessment)

(1) Um das Risiko für ICS-Netze und -Systeme zu reduzieren, reicht es nicht aus, bloss Sicherheitstechnologien in ICS-Umgebungen einzusetzen. Obwohl neuere ICSs oft dieselben zugrundeliegenden Protokolle verwenden, die in IT- und Business-Netzwerken eingesetzt werden, kann die Art der Steuerung bzw. die Funktionalität der Steuerungssysteme (kombiniert mit den Anforderungen an den Betrieb und den Verfügbarkeiten) auch allgegenwärtige Sicherheitstechnologien wie Antivirenprogramme unangemessen machen. ICS-Systeme in der Energie-, Transport- und Chemie-Sektor sind empfindlich für zeitliche Verzögerungen (Latenzzeiten, Datendurchsatz) die durch Sicherheitslösungen entstehen und eine optimale Systemleistung beeinträchtigen können. Da sich die Steuerungsnetze von eigenständigen Domänen zu miteinander verbundenen Netzwerken entwickeln, die mit Unternehmens-IT-Umgebungen koexistieren, müssen Systemverantwortliche Gegenmassnahmen implementieren, welche die Funktionalität nicht beeinträchtigen. Das Verständnis von Schwachstellen und den damit verbundenen Angriffs-Vektoren und deren Ausnutzung ist für den Aufbau einer effektiven Strategie zur Sicherheitsminderung unerlässlich.

3.1 Proaktives Sicherheitsmodell

(1) Beim Schutz einer Informationsinfrastruktur beginnen Sicherheits-Praktiken mit einem proaktiven Sicherheitsmodell (siehe Abbildung 25). Die meisten Sicherheitsprogramme sind reaktive Anwendung von Sicherheitsarchitekturen und reagieren nach einem Vorfall oder machen Kompromisse. Sie sind meist teuer und können den laufenden Betrieb von versorgungskritischen Anlagen unterbrechen.

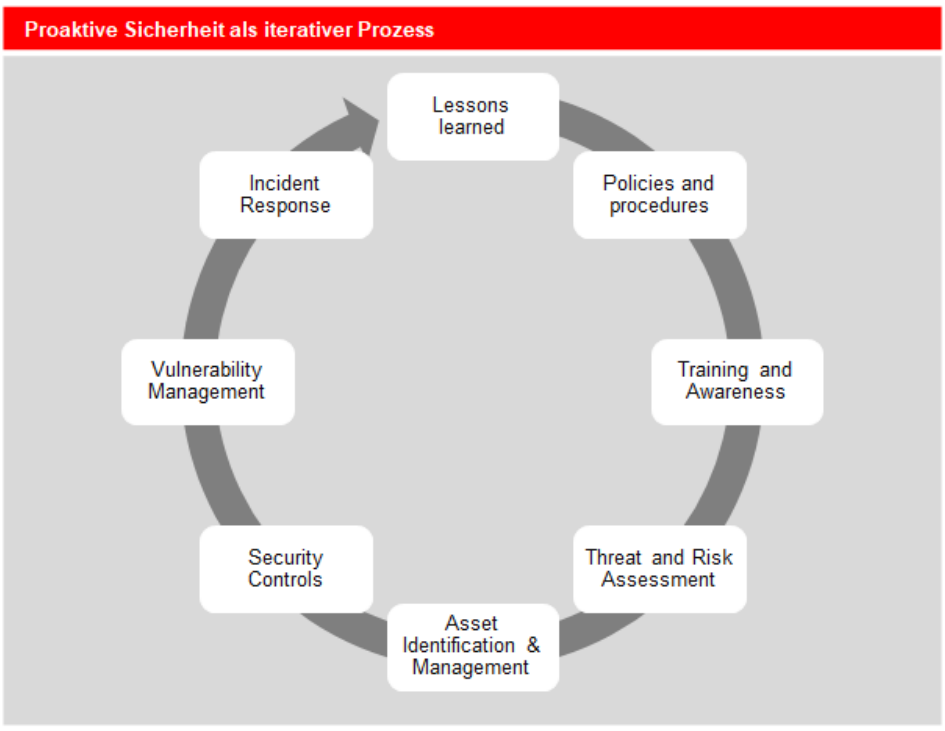

Abbildung 25 Proaktive Sicherheit als iterativer Prozess

(2) Die Entwicklung einer robusten Defense-in-Depth-Strategie beginnt mit der Sicherstellung, dass Richtlinien und Verfahren vorhanden sind, welche die erwarteten Verhaltensweisen begleiten. Es sind Richtlinien für die Ausbildung von Einzelpersonen festzulegen, um sicherzustellen, dass sie ihre Arbeit sicher machen. Eine robuste Defense-in-Depth-Strategie erkennt Bedrohungen und Risiken und kann diese Bedrohungen und Risiken betreffend ihrer Auswirkungen beurteilen. Die Strategie bildet auch die ICS-Architektur ab und beinhaltet ein umfassendes Inventar aller ICS-Assets. Ein genau und gut dokumentiertes Inventar ermöglicht es dem Unternehmen, eine realistische Risikoanalyse durch die Systemverantwortlichen durchzuführen, dafür sind Sicherheits-Kontrollen auf der Grundlage von Asset-Priorität anzuwenden und effektive Sicherheits-Gegenmassnahmen zur Verwaltung von Schwachstellen bereitzustellen. Anlagenbesitzer sollten Vorfälle nach ihren Auswirkungen beurteilen und lernen damit umzugehen oder entsprechende Gegenmassnahmen einzuleiten. Erkenntnisse, welche während des gesamten Prozesses erarbeitet werden, sollen in die laufende Anpassung von Programm-und Sicherheits-Kontrollen eingepflegt werden, um so eine kontinuierliche Verbesserung im Bewusstsein der aufkommenden Bedrohungen und folgenden System-Modifikationen zu gewährleisten.

4. Umzusetzende Massnahmen

(1) Ziel des NIST Framework for Improving Critical Infrastructure Cybersecurity und seiner Empfehlungen ist es, den Betreibern von kritischen Infrastrukturen ein Instrument bereitzustellen, mit dem diese selbständig und eigenverantwortlich ihre Resilienz erhöhen können. Dabei berücksichtigt es auch das Streben nach Wirtschaftlichkeit und Effizienz sowie Vertraulichkeit und Datenschutz. Um Weiterentwicklung und technische Innovation zu ermöglichen, ist das NIST-Framework technologieneutral. Das Framework basiert auf einer Auswahl an existierenden Standards, Richtlinien und Best-Practice-Vorgaben.

Core / Überblick

(2) Das NIST Framework Core ist ein risikobasierter Ansatz um Cybersecurity-Risiken zu adressieren und zu managen. Es besteht aus fünf Funktionen:

1. *Identifizieren (Identify)*
2. *Schützen (Protect)*
3. *Erkennen (Detect)*
4. *Reagieren (Respond)*
5. *Widerherstellen (Recover)*

(3) Diese fünf Funktionen bilden gemeinsam eine strategische Sicht auf das Management von Cybersecurity-Risiken einer Organisation.

Implementation Tiers

(4) Die Framework Implementation Tiers (dt. „Stufen“) bieten den übergeordneten Kontext zur Bewältigung des Cybersecurity-Risikos und der Organisation der dazugehörigen Prozesse. Die verschiedenen Stufen beschreiben den Grad oder die Ausbaustufe, welche ein Unternehmen umgesetzt hat. (z. B. Risiko und Bedrohung, die wiederholbar und anpassungsfähig sind). Die Stufen charakterisieren die Ausbaustufe einer Organisation welche von Teilweise (Tier 1) bis Adaptiv (Tier 4) reichen. Die Stufen spiegeln eine Progression von informalen und reaktiven Ansätzen wider, die agil und risikoorientiert sind. Während des Tierselektionsprozesses sollte eine Organisation ihre derzeitigen Risikomanagementpraktiken, Bedrohungsumgebung, rechtlichen und regulatorischen Anforderungen, Geschäftsziele und organisatorischen Vorgaben genau kennen.

Profiles

(5) Das Profil kann als eine Angleichung von Standards, Richtlinien und Praktiken aus dem Framework Core mit einem individuellen Implementierungsszenario charakterisiert werden. Profile können verwendet werden, um Optionen zur Verbesserung der Cybersecurity zu identifizieren, indem sie ein "Ist" Profil mit einem "Ziel" Profil verknüpfen. Um ein solches Profil zu entwickeln, kann eine Organisation alle Kategorien und Unterkategorien überprüfen und auf der Grundlage von Geschäftszielen und einer Risikobewertung bewerten. Sie können Kategorien und Unterkategorien hinzufügen, um die Risiken der Organisation anzugleichen und anzugehen. Das Profil kann auch zur Selbsteinschätzung innerhalb oder zwischen Organisationen und zur Illustration des Fortschrittes vom Ist- zum Soll-Profil genutzt werden.

(6) Die vorgegebenen Kapitelüberschriften decken die zu behandelnden Themen ab. Inhalte dieser Kapitel können aus dem publizierten Cybersecurity Minimalstandard der Wirtschaftlichen Landesversorgung eingesehen, übernommen oder referenziert werden.

4.1 Sicherheitsstrategie – Identify

Inventar Management (Assest Management)

(1) Die Daten, Personen, Geräte, Systeme und Anlagen, einer Organisation sind in einer Art und Weise identifiziert, katalogisiert und bewertet, die ihrer Kritikalität hinsichtlich der zu erfüllenden Geschäftsprozesse, sowie der Risikostrategie der Organisation entspricht.

Bezeichnung	Aufgabe
ID.AM-1	Erarbeiten Sie einen Inventarisierungsprozess welcher sicherstellt, dass zu jedem Zeitpunkt ein vollständiges Inventar ihrer ICT-Betriebsmittel (Assets) vorhanden ist.
ID.AM-2	Inventarisieren Sie all Ihre Softwareplattformen / -Lizenzen und Applikationen innerhalb ihrer Organisation.
ID.AM-3	Katalogisieren Sie all Ihre internen Kommunikations- und Datenflüsse.
ID.AM-4	Katalogisieren Sie alle externen ICT-Systeme, die für ihre Organisation relevant sind.
ID.AM-5	Priorisieren Sie die inventarisierten Ressourcen (Geräte, Anwendungen, Daten) hinsichtlich ihrer Kritikalität.
ID.AM-6	Definieren Sie klare Rollen und Verantwortlichkeiten im Bereich der Cybersecurity.

Tabelle 14 Aufgaben ID.AM

Geschäftsumfeld (Business Environment)

(2) Die Ziele, Aufgaben und Aktivitäten des Unternehmens sind priorisiert und bewertet. Diese Informationen dienen als Grundlage für die Zuweisung der Verantwortlichkeiten hinsichtlich Cybersecurity und Risikomanagement.

Bezeichnung	Aufgabe
ID.BE-1	Identifizieren, dokumentieren und kommunizieren Sie die exakte Rolle ihres Unternehmens innerhalb der (kritischen) Versorgungskette.
ID.BE-2	Die Bedeutung der Organisation als kritische Infrastruktur und ihre Position innerhalb des kritischen Sektors ist identifiziert und kommuniziert.
ID.BE-3	Die Ziele, Aufgaben und Aktivitäten innerhalb der Organisation sind bewertet und priorisiert.
ID.BE-4	Abhängigkeiten und kritische Funktionen für kritische Dienstleistungensind etabliert.
ID.BE-5	Resilienz Anforderungen für kritische Dienstleistungen sind etabliert.

Tabelle 15 Aufgaben ID.BE

Governance

(3) Die Governance bildet den Ordnungsrahmen für die Leitung und Überwachung der Cybersecurity. Sie setzt sich zusammen aus Weisungen, Abläufen und Prozessen. Sie regelt Zuständigkeiten, überwacht und stellt sicher, dass regulatorische und rechtliche Anforderungen aus dem Geschäftsumfeld sowie operationelle Anforderungen richtig verstanden werden und informiert das Management entsprechend.

Bezeichnung	Aufgabe
ID.GV-1	Erlassen Sie Vorgaben zur Informationssicherheit in Ihrem Unternehmen.
ID.GV-2	Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit sind mit internen Rollen (z.B. aus dem Risikomanagement) sowie externen Partnern koordiniert.
ID.GV-3	Stellen Sie sicher, dass Ihre Organisation alle gesetzlichen und regulatorischen Vorgaben im Bereich der Cybersecurity erfüllt, inkl. Vorgaben zum Datenschutz.
ID.GV-4	Stellen Sie sicher, dass Cyberrisiken Teil des unternehmensweiten Risikomanagements sind.

Tabelle 16 Aufgaben ID.GV

Risikomanagement (Risk Assessment)

(4) Die Organisation kennt die Auswirkungen von Cybersecurity-Risiken auf die Geschäftstätigkeit, auf Betriebsmittel und Individuen, inklusive Reputationsrisiken.

Bezeichnung	Aufgabe
ID.RA-1	Identifizieren Sie die (technischen) Verwundbarkeiten ihrer Betriebsmittel und dokumentieren Sie diese.
ID.RA-2	Tauschen Sie sich regelmässig in Foren und Gremien aus, um aktuelle Informationen über Cyber-Bedrohungen zu erhalten.
ID.RA-3	Identifizieren und dokumentieren Sie interne und externe Cyberbedrohungen.
ID.RA-4	Identifizieren Sie mögliche Auswirkungen auf die Geschäftstätigkeit und bewerten Sie ihre Eintretenswahrscheinlichkeit.
ID.RA-5	Bewerten Sie die Risiken für Ihre Organisation, basierend auf den Bedrohungen, Verwundbarkeiten, Auswirkungen (auf die Geschäftstätigkeit) und Eintretenswahrscheinlichkeiten.
ID.RA-6	Definieren Sie mögliche Sofortmassnahmen bei Eintritt eines Risikos und priorisieren Sie diese.

Tabelle 17 Aufgaben ID.RA

Risikomanagement Strategy (Risk Management Strategy)

(5) Legen Sie die Prioritäten, Einschränkungen und maximal tragbaren Risiken Ihrer Organisation fest. Nutzen Sie diese Definitionen als Grundlage zur Beurteilung operativer Risiken.

Bezeichnung	Aufgabe
ID.RM-1	Definieren und etablieren Sie Risikomanagementprozesse, lassen Sie sie durch die involvierten Stakeholder vereinbaren und akzeptieren und managen Sie sie aktiv.
ID.RM-2	Definieren und kommunizieren Sie das maximal tragbare Risiko ihrer Organisation.
ID.RM-3	Stellen Sie sicher, dass die Definition des maximal tragbaren Risikos unter der Berücksichtigung der Bedeutung als kritischer Infrastruktur und unter Einbezug von Sektor spezifischen Risikoanalysen erstellt wurde.

Tabelle 18 Aufgaben ID.RM

Lieferketten Risikomanagement (Supply Chain Riskmanagement)

(6) Legen Sie die Prioritäten, Einschränkungen und maximalen Risiken fest, die Ihre Organisation in Zusammenhang mit Lieferantenrisiken zu tragen gewillt ist. Verwenden Sie die Definition der Lieferantenrisiken als Grundlage zur Beurteilung operativer Risiken.

Bezeichnung	Aufgabe
ID.SC-1	Etablieren Sie klare Prozesse zum Management der Supply-Chain Risiken. Lassen Sie diese Prozesse durch alle beteiligten Anspruchsgruppen überprüfen und holen Sie ihre Zustimmung ein.
ID.SC-2	Identifizieren und priorisieren Sie Lieferanten und Dienstleistungsanbieter ihrer kritischen Systeme, Komponenten und Diensten unter Anwendung der definierten Prozesse aus ID.SC-1.
ID.SC-3	Verpflichten Sie ihre Lieferanten und Dienstleister vertraglich dazu, angemessene Massnahmen zu entwickeln und zu implementieren, um die Ziele und Vorgaben aus dem Supply-Chain-Riskmanagement-Prozess zu erfüllen.
ID.SC-4	Etablieren Sie ein Monitoring um sicherzustellen, dass all Ihre Lieferanten und Dienstleister ihre Verpflichtungen gemäss den Vorgaben erfüllen. Lassen Sie sich dies regelmässig durch Audit-Berichte oder technische Prüfergebnisse bestätigen.
ID.SC-5	Definieren Sie mit Ihren Lieferanten und Dienstleistern Reaktions- und Widerherstellungsprozesse nach Cybersecurity-Vorfällen. Testen Sie diese Prozesse in Übungen.

Tabelle 19 Aufgaben ID.SC

4.2 Sicherheitsstrategie – Protect

Zugriffsmanagement und -steuerung (Access Control)

(1) Stellen Sie sicher, dass der physische und logische Zugriff auf ICT-Betriebsmittel und -Anlagen nur für autorisierte Personen, Prozesse und Geräte möglich ist und dass der Zugriff nur für als zulässig definierte Aktivitäten möglich ist.

Bezeichnung	Aufgabe
PR.AC-1	Etablieren Sie einen klar definierten Prozess zur Erteilung und Verwaltung von Berechtigungen und Zugangsdaten für Benutzer, Geräte und Prozesse.
PR.AC-2	Stellen Sie sicher, dass nur autorisierte Personen physischen Zugriff auf die ICT-Betriebsmittel haben. Sorgen Sie mit (baulichen) Massnahmen dafür, dass die ICT-Betriebsmittel vor unautorisiertem physischem Zugriff geschützt sind.
PR.AC-3	Etablieren Sie Prozesse zur Verwaltung der Fernzugriffe.
PR.AC-4	Definieren Sie Ihre Berechtigungsstufen nach dem Prinzip der kleinstmöglichen Berechtigung sowie der Trennung von Funktionen.
PR.AC-5	Stellen Sie sicher, dass die Integrität Ihres Netzwerks geschützt ist. Segregieren Sie Ihr Netzwerk logisch und physisch, wo notwendig und sinnvoll.
PR.AC-6	Stellen Sie sicher, dass Identitäten überprüft und bestätigt sind und nur bestätigten Berechtigungsstufen und Zugangsdaten zugeordnet sind.

Tabelle 20 Aufgaben PR.AC

Awareness and Training

(2) Stellen Sie sicher, dass Ihre Mitarbeitenden und externen Partner regelmässig bezüglich aller Belange der Cybersecurity angemessen geschult und ausgebildet werden. Stellen Sie sicher, dass Ihre Mitarbeitenden und externen Partner ihre sicherheitsrelevanten Aufgaben gemäss den zugehörigen Vorgaben und Prozessen ausführen.

Bezeichnung	Aufgabe
PR.AT-1	Stellen Sie sicher, dass alle Mitarbeitenden bezüglich Cybersecurity informiert und geschult sind.
PR.AT-2	Stellen Sie sicher, dass Anwender mit höheren Berechtigungsstufen sich ihrer Rolle und Verantwortung besonders bewusst sind.
PR.AT-3	Stellen Sie sicher, dass sich alle beteiligten Akteure ausserhalb Ihres Unternehmens (Lieferanten, Kunden, Partner) ihrer Rolle und Verantwortung bewusst sind.
PR.AT-4	Stellen Sie sicher, dass sich alle Führungskräfte ihrer besonderen Rolle und Verantwortung bewusst sind.
PR.AT-5	Stellen Sie sicher, dass die Zuständigen für physische Sicherheit und Informationssicherheit sich ihrer besonderen Rolle und Verantwortung bewusst sind.

Tabelle 21 Aufgaben PR.AT

Datensicherheit (Data Security)

(3) Stellen sie sicher, dass Informationen, Daten und Datenträger so gemanaged werden, dass die Vertraulichkeit, Integrität und Verfügbarkeit der Daten gemäss der Risikostrategie der Organisation geschützt werden kann.

Bezeichnung	Aufgabe
PR.DS-1	Stellen Sie sicher, dass gespeicherte Daten geschützt sind (vor Verletzungen der Vertraulichkeit, Integrität und Verfügbarkeit).
PR.DS-2	Stellen Sie sicher, dass Daten während der Übertragung geschützt sind.
PR.DS-3	Stellen Sie sicher, dass für Ihre IT-Betriebsmittel ein formaler Prozess etabliert ist, welcher die Daten bei Entfernung, Verschiebung oder Ersatz der Betriebsmittel schützt.
PR.DS-4	Stellen Sie sicher, dass Sie bezüglich der Verfügbarkeit der Daten über ausreichende Kapazitätsreserven verfügen.
PR.DS-5	Stellen Sie sicher, dass adäquate Massnahmen gegen den Abfluss von Daten (Datenlecks) implementiert sind.
PR.DS-6	Etablieren Sie einen Prozess, um Firmware, Betriebssysteme, Anwendungssoftware und Daten hinsichtlich ihrer Integrität zu verifizieren.
PR.DS-7	Stellen Sie eine IT-Umgebung für das Entwickeln und Testen zur Verfügung, welche komplett unabhängig von den produktiven Systemen ist.
PR.DS-8	Etablieren Sie einen Prozess, um die eingesetzte Hardware hinsichtlich ihrer Integrität zu verifizieren.

Tabelle 22 Aufgaben PR.DS

Schutz von Daten (Information Protection Processes and Procedures)

(4) Erstellen sie Richtlinien zum Schutz von Informationssystemen und Betriebsmitteln. Stellen Sie sicher, dass diese Richtlinien im Minimum den Zweck, den Umfang, die Rollen und die Verantwortlichkeiten sowie die Koordination innerhalb der Organisation. Nutzen Sie diese Richtlinien, um die Informationssysteme und Betriebsmittel zu schützen.

Bezeichnung	Aufgabe
PR.IP-1	Erstellen Sie eine Standardkonfiguration für die Informations- und Kommunikationsinfrastruktur, sowie für die industriellen Kontrollsysteme. Stellen Sie sicher, dass diese Standardkonfiguration typische Security-Prinzipien (z.B. N-1 Redundanz, Minimalkonfiguration, etc.) erfüllt.
PR.IP-2	Etablieren Sie einen Lebenszyklus-Prozess für die Entwicklung von Systemen.
PR.IP-3	Etablieren Sie einen Prozess zur Kontrolle von Konfigurationsänderungen.
PR.IP-4	Stellen Sie sicher, dass Sicherungen (Backups) ihrer Informationen regelmässig durchgeführt, bewirtschaftet und getestet werden (Rückspielbarkeit der Backups testen).

Bezeichnung	Aufgabe
PR.IP-5	Stellen Sie sicher, dass alle (regulatorischen) Vorgaben und Richtlinien hinsichtlich der physischen Betriebsmittel erfüllt sind.
PR.IP-6	Stellen Sie sicher, dass Daten gemäss den Vorgaben vernichtet werden.
PR.IP-7	Stellen Sie sicher, dass Ihre Informationsschutzprozesse kontinuierlich weiterentwickelt und verbessert werden.
PR.IP-8	Tauschen Sie sich bezüglich der Effektivität verschiedener Schutztechnologien mit ihren Partnern aus.
PR.IP-9	Etablieren Sie Prozesse zur Reaktion auf eingetretene Cyber-Vorfälle. (Incident Response-Planning, Business Continuity Management, Incident Recovery, Disaster Recovery).
PR.IP-10	Testen Sie die Reaktions- und Widerherstellungspläne.
PR.IP-11	Etablieren Sie Aspekte der Cybersecurity bereits in den Personalrekrutierungsprozess (z.B. durch die Etablierung von Backgroundchecks / Personensicherheitsprüfungen).
PR.IP-12	Entwickeln und implementieren Sie einen Prozess zum Umgang mit erkannten Schwachstellen.

Tabelle 23 Aufgaben PR.IP

Maintenance

(5) Stellen Sie sicher, dass Unterhalts- und Reparaturarbeiten an Komponenten des IT-Systems und / oder des ICS gemäss den geltenden Richtlinien und Prozessen durchgeführt werden.

Bezeichnung	Aufgabe
PR.MA-1	Stellen Sie sicher, dass der Betrieb, die Wartung und allfällige Reparaturen an den Betriebsmitteln aufgezeichnet und dokumentiert werden (Logfiles). Stellen Sie sicher, dass diese zeitnah durchgeführt werden und nur unter Einsatz von geprüften und freigegebenen Mitteln erfolgen.
PR.MA-2	Stellen Sie sicher, dass Unterhaltsarbeiten an ihren Systemen, die über Fernzugriffe erfolgen, aufgezeichnet und dokumentiert werden. Stellen Sie sicher, dass kein unautorisierter Zugriff möglich ist.

Tabelle 24 Aufgaben PR.MA

Protective Technology

(6) Installieren Sie technische Security-Lösungen um die Sicherheit und Resilienz Ihres Systems und Ihrer Daten gemäss den Vorgaben und Prozessen zu garantieren.

Bezeichnung	Aufgabe
PR.PT-1	Definieren Sie Vorgaben zu Audits und Log-Aufzeichnungen. Erstellen und prüfen Sie die regelmässigen Logs gemäss den Vorgaben und Richtlinien.
PR.PT-2	Stellen Sie sicher, dass Wechseldatenträger geschützt sind und dass sie nur gemäss den Richtlinien eingesetzt werden.
PR.PT-3	Stellen Sie sicher, dass Ihr System so konfiguriert ist, dass jederzeit eine Minimalfunktionalität gewährleistet wird.
PR.PT-4	Stellen Sie sicher, dass Ihre Kommunikations- und Steuernetzwerke geschützt sind.
PR.PT-5	Stellen Sie sicher, dass Ihre Systeme gemäss vordefinierten Szenarien funktionieren. Z.B: Funktionalität während eines Angriffs, Funktionalität in der Widerherstellungsphase, Funktionalität in der normalen Betriebsphase.

Tabelle 25 Aufgaben PR.PT

4.3 Sicherheitsstrategie – Detect

Vorfälle (Anomalies and Events)

(1) Stellen Sie sicher, dass Anomalien und sicherheitsrelevante Ereignisse zeitgerecht erkannt werden und dass potenzielle Auswirkungen des Vorfalls verstanden werden.

Bezeichnung	Aufgabe
DE.AE-1	Definieren Sie Standardwerte für zulässige Netzwerkoperationen und die zu erwartenden Datenflüsse für Anwender und Systeme. Managen Sie diese Werte fortlaufend.
DE.AE-2	Stellen Sie sicher, dass entdeckte Cybersecurity-Vorfälle hinsichtlich ihrer Ziele und ihrer Methoden analysiert werden.
DE.AE-3	Stellen Sie sicher, dass Informationen zu Cybersecurity-Vorfällen aus verschiedenen Quellen und Sensoren aggregiert und aufbereitet werden.
DE.AE-4	Determinieren Sie die Auswirkungen möglicher Events.
DE.AE-5	Definieren Sie die Schwellenwerte, ab denen Cybersecurity-Vorfälle zu einer Alarmierung führen.

Tabelle 26 Aufgaben DE.AE

Überwachung (Security Continuous Monitoring)

(2) Stellen Sie sicher, dass das ICT-System inkl. aller Betriebsmittel in regelmässigen Intervallen überwacht wird, um einerseits Cybersecurity Vorfälle zu entdecken und anderseits die Effektivität der Gegenmassnahmen sicherstellen zu können.

Bezeichnung	Aufgabe
DE.CM-1	Etablieren sie ein kontinuierliches Netzwerkmonitoring, um potentielle Cybersecurity-Vorfälle zu entdecken.
DE.CM-2	Etablieren Sie ein kontinuierliches Monitoring / Überwachung aller physischen Betriebsmittel und Gebäude, um Cybersecurity-Vorfälle entdecken zu können.
DE.CM-3	Etablieren Sie ein Monitoring der Cyber-Aktivitäten der Mitarbeitenden, um potentielle Cybersecurity-Vorfälle zu entdecken.
DE.CM-4	Stellen Sie sicher, dass Schadsoftware entdeckt werden kann.
DE.CM-5	Stellen Sie sicher, dass ausführbare Programme in E-Mail Attachments, Makros, USB-Speichergeräten oder Mobilgeräten erkannt werden können.
DE.CM-6	Stellen Sie sicher, dass die Aktivitäten von externen Dienstleistern monitored / überwacht werden, so dass Cybersecurity-Vorfälle entdeckt werden können.
DE.CM-7	Überwachen Sie Ihr System laufend, um sicherzustellen, dass Aktivitäten / Zugriffe von unberechtigten Personen, Geräten und Software erkannt werden können.
DE.CM-8	Führen Sie regelmässig Verwundbarkeitsscans durch.

Tabelle 27 Aufgaben DE.CM

Detection Processes

(3) Prozesse und Handlungsanweisungen zur Detektion von Cybersecurity-Events werden gepflegt, getestet und unterhalten, so dass Cybersecurity-Vorfälle zeitnah erkannt werden.

Bezeichnung	Aufgabe
DE.DP-1	Definieren Sie klare Rollen und Verantwortlichkeiten, so dass klar ist, wer wofür zuständig ist und wer welche Kompetenzen hat.
DE.DP-2	Stellen Sie sicher, dass die Detektionsprozesse all ihre Vorgaben und Bedingungen erfüllen.
DE.DP-3	Testen Sie ihre Detektionsprozesse.
DE.DP-4	Kommunizieren Sie detektierte Events an die zuständigen Stellen (z.B. Lieferanten, Kunden, Partner, Behörden, etc.).
DE.DP-5	Verbessern Sie Ihre Detektionsprozesse kontinuierlich.

Tabelle 28 Aufgaben DE.DP

4.4 Sicherheitsstrategie – Respond

Response Planning

(1) Erarbeiten Sie einen Reaktionsplan zur Adressierung erkannter Cybersecurity-Vorfälle. Stellen Sie sicher, dass dieser Reaktionsplan im Ereignisfall korrekt und zeitgerecht ausgeführt wird.

Bezeichnung	Aufgabe
RS.RP-1	Stellen Sie sicher, dass der Reaktionsplan während oder nach einem detektierten Cybersecurity-Vorfall korrekt und zeitnah durchgeführt wird.

Tabelle 29 Aufgaben RS.RP

Kommunikation

(2) Stellen Sie sicher, dass Ihre Reaktionsprozesse mit den internen und externen Anspruchsgruppen abgestimmt sind. Stellen Sie sicher, dass Sie im Ereignisfall Unterstützung durch staatliche Stellen erhalten, falls notwendig und angemessen.

Bezeichnung	Aufgabe
RS.CO-1	Stellen Sie sicher, dass alle Personen ihre Aufgaben und die Reihenfolge ihrer Handlungen kennen bezüglich der Reaktion auf eingetretene Cybersecurity-Vorfälle.
RS.CO-2	Definieren Sie Kriterien für das Reporting und stellen Sie sicher, dass Cybersecurity-Vorfälle gemäss diesen Kriterien gemeldet und bearbeitet werden.
RS.CO-3	Teilen Sie Informationen und Erkenntnisse zu detektierten Cybersecurity-Vorfällen gemäss den definierten Kriterien.
RS.CO-4	Koordinieren Sie sich mit all ihren Anspruchsgruppen gemäss den vordefinierten Kriterien.
RS.CO-5	Sorgen Sie für ein gesteigertes Bewusstsein hinsichtlich Cybersecurity-Vorfällen, in dem Sie sich regelmässig mit Ihren Partnern austauschen.

Tabelle 30 Aufgaben RS.CO

Analyse (Analysis)

(3) Stellen Sie sicher, dass regelmässig Analysen durchgeführt werden, die Ihnen eine adäquate Reaktion auf Cybersecurity-Vorfälle ermöglichen.

Bezeichnung	Aufgabe
RS.AN-1	Stellen Sie sicher, dass Benachrichtigungen aus Detektionssystemen berücksichtigt werden und Nachforschungen ausgelöst werden.
RS.AN-2	Stellen Sie sicher, dass die Auswirkungen eines Cybersecurity-Vorfalls korrekt erkannt werden können.
RS.AN-3	Führen Sie nach einem eingetretenen Vorfall forensische Analysen durch.
RS.AN-4	Kategorisieren Sie eingetretene Vorfälle gemäss den Vorgaben im Reaktionsplan.

Tabelle 31 Aufgaben RS.AN

Mitigation (Mitigation)

(4) Führen Sie Handlungen aus, die die weitere Ausbreitung eines Cybersecurity-Vorfalls verhindern, seine Auswirkungen eindämmen und die Ursache beseitigen.

Bezeichnung	Aufgabe
RS.MI-1	Stellen Sie sicher, dass Cybersecurity-Vorfälle eingegrenzt werden können und die weitere Ausbreitung unterbrochen wird.
RS.MI-2	Stellen Sie sicher, dass die Auswirkungen von Cybersecurity-Vorfällen gemindert werden können.
RS.MI-3	Stellen Sie sicher, dass neu identifizierte Verwundbarkeiten reduziert oder als akzeptierte Risiken dokumentiert werden.

Tabelle 32 Aufgaben RS.MI

Verbesserungen (Improvements)

(5) Stellen Sie sicher, dass die Reaktionsfähigkeit ihrer Organisation auf eingetretene Cybersecurity-Vorfälle laufend verbessert wird, indem die Lehren aus vorangegangenen Vorfällen gezogen werden.

Bezeichnung	Aufgabe
RS.IM-1	Stellen Sie sicher, dass Erkenntnisse und Lehren aus vorangegangenen Cybersecurity-Vorfällen in ihre Reaktionspläne einfliessen.
RS.IM-2	Aktualisieren Sie Ihre Reaktionsstrategien.

Tabelle 33 Aufgaben RS.IM

4.5 Sicherheitsstrategie - Recover

Wiederherstellungsplanung (Recovery Planning)

(1) Stellen Sie sicher, dass die Wiederherstellungsprozesse so gepflegt und durchgeführt werden (können), dass eine zeitnahe Wiederherstellung der Systeme sichergestellt werden kann.

Bezeichnung	Aufgabe
RC.RP-1	Stellen Sie sicher, dass der Wiederherstellungsplan nach einem eingetretenen Cybersecurity-Vorfall korrekt durchgeführt wird.

Tabelle 34 Aufgaben RC.RP

Verbesserungen (Improvements)

(2) Stellen Sie sicher, dass Ihre Wiederherstellungsprozesse laufend verbessert werden, indem Lehren aus vorangegangenen Wiederherstellungen gezogen werden.

Bezeichnung	Aufgabe
RC.IM-1	Stellen Sie sicher, dass Erkenntnisse und Lehren aus vorangegangenen Cybersecurity-Vorfällen in ihre Wiederherstellungspläne einfliessen.
RC.IM-2	Aktualisieren Sie Ihre Wiederherstellungsstrategie.

Tabelle 35 Aufgaben RC.IM

Kommunikation (Communications)

(3) Koordinieren Sie Ihre Wiederherstellungsaktivitäten mit internen und externen Partnern, z.B. Internet Service Providern, CERTS, Behörden, Systemintegratoren, etc.

Bezeichnung	Aufgabe
RC.CO-1	Stellen Sie sicher, dass Ihre öffentliche Wahrnehmung aktiv gemanaged wird.
RC.CO-2	Stellen Sie sicher, dass Ihre Reputation nach einem eingetretenen Cybersecurity-Vorfall wiederhergestellt wird.
RC.CO-3	Kommunizieren Sie alle Ihre Wiederherstellungsaktivitäten an die internen Anspruchsgruppen, insbesondere auch an das Management / die Geschäftsleitung

Tabelle 36 Aufgaben RC.CO

4.6 21 Schritte zur Erhöhung der Cyber Security in OT-Netzwerken

(1) Diese 21 Schritte basieren auf den Ausführungen des US-Amerikanischen „Department of Energy“ und haben das Ziel, kritische Infrastrukturen in der Stromversorgung zu schützen.

(2) **Die folgenden Schritte konzentrieren sich auf spezifische Massnahmen, die getroffen werden müssen, um die Sicherheit in OT-Netzwerken für kritische Infrastrukturen in der Stromversorgung zu erhöhen:**

Spezifische Massnahmen zur Erhöhung der Sicherheit in den OT-Netzwerken	NIST Framework
1. Identifizieren Sie alle Verbindungen zu den OT-Netzwerken für kritische Infrastrukturen in der Stromversorgung Führen Sie eine gründliche Risikoanalyse durch, um das Risiko und die Notwendigkeit jeder Verbindung zu den OT-Netzwerken für kritische Infrastrukturen in der Stromversorgung zu beurteilen. Entwickeln Sie ein umfassendes Verständnis aller Verbindungen zu den OT-Netzwerken für kritische Infrastrukturen in der Stromversorgung und wie gut diese Verbindungen geschützt sind. Identifizieren und Auswerten der folgenden Arten von Verbindungen: - Interne lokale und weiträumige Netzwerke, einschliesslich Business-Netzwerke - Das Internet - Drahtlose Netzwerkgeräte, einschliesslich Satelliten-Uplinks - Modem- oder DFÜ-Verbindungen - Verbindungen zu Geschäftspartnern, Lieferanten oder Regulierungsbehörden	ID.AM ID.GV ID.RA ID.RM PR.AC PR.DS PR.MA PR.PT
2. Löschen Sie alle unnötigen Verbindungen zu den OT-Netzwerken für kritische Infrastrukturen in der Stromversorgung Um ein Höchstmass an Sicherheit von Systemen in den OT-Netzwerken für kritische Infrastrukturen in der Stromversorgung zu gewährleisten, isolieren sie die OT-Netzwerke von anderen Netzwerken so weit wie möglich. Jede Verbindung zu einem anderen Netzwerk führt Sicherheitsrisiken ein, insbesondere wenn die Verbindung einen Pfad von oder zum Internet schafft. Obwohl mit direkten Verbindungen zu anderen Netzwerken wichtige Informationen effizient und bequem übergeben werden können, sind unsichere Verbindungen einfach nicht ein mögliches Risiko wert. Die Isolierung der OT-Netzwerke für kritische Infrastrukturen in der Stromversorgung muss ein primäres Ziel sein, um so den erforderlichen Schutz zu bieten. Strategien wie die Nutzung von "demilitarisierten Zonen" (DMZs), Datendioden und Data Warehousing können die sichere Datenübertragung innerhalb der OT-Netzwerke für kritische Infrastrukturen in der Stromversorgung und zu Business-Netzwerken erleichtern. Sie müssen jedoch ordnungsgemäss konstruiert und umgesetzt werden, um die Einführung zusätzlicher Risiken durch unsachgemässe Konfiguration zu vermeiden.	ID.BE PR.DS PR.IP PR.MA PR.PT

Spezifische Massnahmen zur Erhöhung der Sicherheit in den OT-Netzwerken	NIST Framework
3. Bewerten und Stärken der Sicherheit aller verbleibenden Verbindungen innerhalb der OT-Netzwerke für kritische Infrastrukturen in der Stromversorgung und zu den anderen Netzwerken. Führen Sie Penetrationstests oder Schwachstellenanalyse auf allen verbleibenden Verbindungen innerhalb der OT-Netzwerke für kritische Infrastrukturen in der Stromversorgung und zu den anderen Netzwerken zur Bewertung der mit diesen Pfaden verbundenen Schutzmassnahmen durch. Nutzen Sie diese Informationen in Verbindung mit Risikomanagementprozessen, um eine robuste Schutzstrategie für alle möglichen Verbindungen innerhalb der OT-Netzwerke für kritische Infrastrukturen in der Stromversorgung und zu den anderen Netzwerken zu entwickeln. Da die OT-Netzwerke für kritische Infrastrukturen in der Stromversorgung nur so sicher sind wie der schwächste Verbindungspunkt, ist es notwendig, Firewalls, Intrusion Detection Systeme (IDSs) und andere geeignete Sicherheitsmassnahmen an jedem Einstiegspunkt zu implementieren. Konfigurieren Sie Firewall-Regeln, um den Zugriff von und zu den OT-Netzwerken für kritische Infrastrukturen in der Stromversorgung zu verhindern und stellen Sie sicher, dass nur die absolut nötigen Verbindungen zugelassen werden. Zum Beispiel sollte ein unabhängiger Systembetreiber (ISO) keinen "Allumfassender“-Netzwerkzugriff gewährt werden, nur weil es notwendig ist, eine Verbindung zu bestimmten Komponenten des SCADA-Systems herzustellen. Strategische Platzierungen von IDSs an jedem Einstiegspunkt, um das Sicherheitspersonal auf mögliche Verletzungen der Netzwerksicherheit zu informieren, sind zwingend einzuführen. Die Unternehmensleitung muss die Verantwortung für Risiken im Zusammenhang mit der Verbindung innerhalb der OT-Netzwerke für kritische Infrastrukturen in der Stromversorgung und zu den anderen Netzwerken verstehen und übernehmen.	ID.AM PR.AT PR.DS PR.IP PR.MA PR.PT
4. Härten der OT-Netzwerke für kritische Infrastrukturen in der Stromversorgung, indem unnötige Dienste entfernen oder deaktivieren werden. SCADA-Steuerungsserver, die auf kommerziellen oder Open-Source-Betriebssystemen aufgebaut sind, können durch Standardnetzwerkdienste angegriffen werden. Wenn immer möglich, entfernen oder deaktivieren Sie unbenutzte Dienste und Netzwerk-Domains, um das Risiko eines direkten Angriffs zu reduzieren. Dies ist besonders wichtig, wenn OT-Netzwerke für kritische Infrastrukturen in der Stromversorgung mit anderen Netzwerken verknüpft sind. Lassen sie keine Dienste und Funktion auf dem SCADA-Netzwerk zu, welche nicht direkt mit der Kernaufgabe des SCADA in Einklang zu bringen ist. Wägen sie gut ab, welche Dienste und Funktionen einen wirklichen Mehrwert bringen und nicht nur unnötig das Gesamtsystem schwächen. Beispiele für Dienste, die von OT-Netzwerke für kritische Infrastrukturen in der Stromversorgung entfernt werden sollten, sind Zählerablese- und Fernabrechnungssysteme, E-Mail-Dienste und Internet-Zugänge usw. Eine weitere Funktion, welche deaktiviert werden sollte, ist die Fernwartung. Zahlreiche sichere Konfigurationsleitfaden für kommerzielle und Open-Source-Betriebssysteme sind öffentlichen zugänglich, wie „National Security Agency’s series of security guides“. Arbeiten Sie eng mit den SCADA-Anbietern zusammen, um sichere Konfigurationen festzulegen und alle Änderungen an Betriebssystemen zu koordinieren. Somit stellen sie sicher, dass das Entfernen oder Deaktivieren von Diensten keine Ausfälle, Unterbrüche oder Verlust des Supportes verursacht.	PR.DS PR.IP PR.MA PR.PT

Spezifische Massnahmen zur Erhöhung der Sicherheit in den OT-Netzwerken	NIST Framework
5. Verlassen Sie sich nicht auf proprietäre Protokolle, um Ihr System zu schützen. Einige OT-Systeme für kritische Infrastrukturen in der Stromversorgung verwenden eindeutige und proprietäre Protokolle für die Kommunikation zwischen Feldgeräten und Servern. Oft basiert die Sicherheit der OT-Systeme für kritische Infrastrukturen in der Stromversorgung ausschliesslich auf der Geheimhaltung dieser Protokolle. Leider sind obskure Protokolle keine "echte" Sicherheit. Verlassen Sie sich nicht auf proprietäre Protokolle oder werkseitige Standardeinstellungen, um Ihr System zu schützen. Darüber hinaus verlangen sie, dass die Anbieter von SCADA-Systemen und Leittechnikkomponenten alle Backdoors- oder Hersteller-Schnittstellen zu Ihren OT-Systemen für kritische Infrastrukturen in der Stromversorgung offenlegen. Fordern sie, dass diese Systeme bereitstellen, die gesichert und überwacht werden können.	PR.AT PR.DS PR.IP PR.MA PR.PT
6. Implementieren Sie die Sicherheitsmerkmale von Geräte- und Systemanbietern. Die meisten älteren OT-Systeme für kritische Infrastrukturen in der Stromversorgung (die meisten verwendeten Systeme) haben keine Sicherheitsfunktionen. Betreiber von OT-Systemen für kritische Infrastrukturen in der Stromversorgung müssen darauf bestehen, dass ihr Systemhersteller Sicherheitsfunktionen in Form von Produkt-Patches oder Upgrades implementiert. Einige neuere OT-Systeme für kritische Infrastrukturen in der Stromversorgung werden mit grundlegenden Sicherheitsfunktionen ausgeliefert, aber diese sind in der Regel deaktiviert, um eine einfache Installation zu gewährleisten. Analysieren sie jedes Gerät in den OT-Systemen für kritische Infrastrukturen in der Stromversorgung, um festzustellen, ob Sicherheitsfunktionen vorhanden und aktiviert sind. Darüber hinaus sind die werkseitigen Standardeinstellungen (z. B. in Computernetzwerk-Firewalls) oft so eingestellt, dass sie maximale Benutzerfreundlichkeit bieten, aber minimale Sicherheit. Setzen Sie alle Sicherheitsfunktionen ein, um das maximale Sicherheitsniveau zu gewährleisten. Erlaube sie Einstellungen unterhalb der maximalen Sicherheit nur dann, wenn nach einer gründlichen Risikobewertung der Konsequenzen die Verringerung der Sicherheitsstufe zugelassen werden darf.	ID.RA ID.RM PR.AC PR.AT PR.DS PR.IP PR.MA PR.PT
7. Stellen Sie starke Kontrollen über jedes Medium her, welches für Backdoors- oder Hersteller-Verbindungen in die OT-Netzwerke für kritische Infrastrukturen in der Stromversorgung verwendet wird. Wo Backdoors- oder Hersteller-Verbindungen in die OT-Systeme für kritische Infrastrukturen in der Stromversorgung vorhanden sind, muss eine starke Authentifizierung implementiert werden, um eine sichere Kommunikation zu gewährleisten. Modems, drahtlose und drahtgebundene Netzwerke, die für Kommunikation und Wartung verwendet werden, stellen eine signifikante Anfälligkeit für die OT-Netzwerke für kritische Infrastrukturen in der Stromversorgung und entfernte Standorte dar. Mit erfolgreichen "Wardialing"- oder "Wardriving" -Attacken könnte es einem Angreifer gelingen, alle anderen Kontrollen und Schutzmassnahmen zu umgehen und so einen direkten Zugriff auf die OT-Netzwerke für kritische Infrastrukturen in der Stromversorgung oder die Ressourcen zu erlangen. Um das Risiko solcher Angriffe zu minimieren, deaktivieren Sie den eingehenden Zugriff und ersetzen Sie es durch eine Rückruffunktion.	PR.AC PR.AT PR.DS PR.MA PR.PT

Spezifische Massnahmen zur Erhöhung der Sicherheit in den OT-Netzwerken	NIST Framework
8. Implementieren Sie interne und externe Intrusion Detection Systeme und stellen Sie eine 24-Stunden-Tages-Überwachung sicher. Um auf Cyber-Angriffe effektiv reagieren zu können, richten Sie eine Intrusion Detection-Strategie ein, welche eine Benachrichtigung an Netzwerkadministratoren über schädliche Netzwerkaktivitäten aus internen oder externen Quellen umfasst. Intrusion Detection System Monitoring ist rund um die Uhr wichtig. Diese Funktion kann durch ein Alarming mittels Pager eingerichtet werden. Darüber hinaus müssen Incident-Response-Verfahren vorhanden sein, um eine effektive Reaktion auf jeden Angriff zu ermöglichen. Um die Netzwerküberwachung zu ergänzen, aktivieren Sie die Protokollierung aller Systeme und Audit-Systemprotokolle täglich, um verdächtige Aktivitäten so schnell wie möglich zu erkennen.	PR.DS PR.IP PR.MA PR.PT DE.CM RS.RP RS.CO RS.AN
9. Führen Sie technische Audits an Geräten und Netzwerken der OT-Umgebung für kritische Infrastrukturen in der Stromversorgung sowie alle anderen angeschlossenen Netzwerken durch, um Sicherheitsbedenken zu ermitteln. Technische Audits von Geräten und Netzwerken der OT-Umgebung für kritische Infrastrukturen in der Stromversorgung sind entscheidend für die laufende Sicherheitseffektivität. Es sind viele kommerzielle und Open-Source-Sicherheitstools verfügbar, die es Systemadministratoren ermöglichen, Audits ihrer Systeme / Netzwerke durchzuführen, um aktive Dienste, Patch-Level und gemeinsame Schwachstellen zu identifizieren. Die Verwendung dieser Werkzeuge wird keine systembedingten Probleme lösen, sondern die "Wege des geringsten Widerstands" beseitigen, die ein Angreifer ausnutzen könnte. Analysieren Sie identifizierte Schwachstellen, um ihre Bedeutung zu bestimmen und Korrekturmassnahmen zu ergreifen. Verfolgen Sie Korrekturmassnahmen und analysieren Sie diese Informationen, um Trends zu identifizieren. Darüber hinaus sind Testwiederholungen nach Korrekturmassnahmen einzuführen, um sicherzustellen, dass die Schwachstellen tatsächlich beseitigt wurden. Es sollen auch nicht Nicht-Produktionsumgebungen gescannt werden, um potenzielle Probleme aktiv zu identifizieren und zu adressieren.	PR.AC PR.DS PR.IP PR.MA PR.PT
10. Durchführung von physischen Sicherheits-Bestandsaufnahmen und -Bewertung aller Standorte, die mit den OT-Netzwerken für kritische Infrastrukturen in der Stromversorgung in Zusammenhang stehen, um ihre Sicherheit zu bewerten. Jeder Ort, der ein Element der OT-Netzwerke für kritische Infrastrukturen in der Stromversorgung in Zusammenhang aufweist, ist ein mögliches Ziel für Angriffe. Vor allem unbemannte oder unbewachte entfernte Standorte weisen ein grosses Risiko auf. Führen Sie in jeder Einrichtung, die ein Element der OT-Netzwerke für kritische Infrastrukturen in der Stromversorgung in Zusammenhang enthält, eine physische Sicherheitsanalyse, besonders an möglichen Eintrittspunkten, durch. Identifizieren und beurteilen Sie jeden möglichen Eintrittspunk einschliesslich Remote-Telefon / Computer-Netzwerk / Glasfaser-Kabel, wo ein Abgriff erfolgen könnte; auch Wireless- und Funkverbindungen können ausgenutzt werden; Computer-Terminals, auf die zugegriffen werden könnte; und drahtlose lokale Netzwerk-Zugangspunkte. Identifizieren und Beseitigen sie einzelne Fehlerpunkte gründlich. Die Sicherheit der Orte muss ausreichend sein, um einen unbefugten Zugriff zu erkennen oder zu verhindern. Erlauben sie keine Zugänge mittels Wireless Access Points auf OT-Netzwerke für kritische Infrastrukturen in der Stromversorgung in entfernten und unbewachten Anlagen einfach aus Bequemlichkeit.	ID.AM ID.GV ID.RA PR.AC PR.AT PR.DS PR.IP PR.PT

Spezifische Massnahmen zur Erhöhung der Sicherheit in den OT-Netzwerken	NIST Framework
11. Stellen Sie "Red Teams" bezüglich der OT-Umgebung für kritische Infrastrukturen in der Stromversorgung auf, um mögliche Angriffsszenarien zu identifizieren und zu bewerten. Stellen Sie ein "Red Team" auf, um mögliche Angriffsszenarien zu identifizieren und mögliche Schwachstellen des Systems zu bewerten. Verwenden Sie eine Vielzahl von Personen, die Einblicke in Schwächen der gesamten OT-Umgebung für kritische Infrastrukturen in der Stromversorgung, physikalische Systeme und Sicherheitskontrollen geben können. Menschen, die jeden Tag am System arbeiten, haben einen guten Einblick in die Schwachstellen ihrer OT-Umgebung für kritische Infrastrukturen in der Stromversorgung und sollten bei der Ermittlung möglicher Angriffsszenarien und möglichen Konsequenzen konsultiert und einbezogen werden. Stellen Sie ausserdem sicher, dass das Risiko eines böswilligen Insiders vollständig ausgewertet wird, da dies eine der grössten Bedrohungen für ein Unternehmen darstellt. Fügen sie Erkenntnisse vom "Red Team" in Risikomanagement-Prozesse ein, um die Informationen zu bewerten und geeignete Schutzstrategien zu entwickeln.	ID.RA DE.CM PR.AC PR.AT PR.DS PR.IP PR.PT

Tabelle 37 Spezifische Massnahmen zur Erhöhung der Sicherheit in OT-Netzwerken

(3) **Die folgenden Schritte konzentrieren sich auf Management-Aktionen, um ein effektives Cybersecurity-Programm zu etablieren:**

Spezifische Massnahmen zur Erhöhung der Sicherheit in den OT-Netzwerken	NIST Framework
12. Definieren von klaren Cybersecurity-Rollen bezüglich Zuständigkeiten und Verantwortlichkeiten für das Management, für Systemadministratoren und die Benutzer. Die Mitarbeiter eines Unternehmens müssen die spezifischen Erwartungen und Pflichten verstehen, die mit dem Schutz der Informationstechnologie-Ressourcen verbunden sind. Dies hat durch eine Definition klarer und logischer Rollen und Verantwortlichkeiten zu erfolgen. Darüber hinaus müssen Schlüsselpersonen genügend Rechte erhalten, um ihre Aufgaben zu erfüllen. Zu oft wird eine gute Cyber-Sicherheit einer individuellen Initiative überlassen, was in der Regel zu inkonsistenten Implementierungen und zu ineffizienter Sicherheit führt. Stellen Sie eine organisatorische Struktur der Cyber-Sicherheit her, welche Rollen und Verantwortlichkeiten definiert und identifiziert, wie Cyber-Sicherheitsprobleme eskaliert werden und wer im Notfall benachrichtigt wird.	ID.AM ID.GV DE.DP PR.AC PR.AT PR.DS

Spezifische Massnahmen zur Erhöhung der Sicherheit in den OT-Netzwerken	NIST Framework
13. Dokumentieren Sie die Netzwerkarchitektur und identifizieren Sie Systeme, die kritische Funktionen ausführen oder sensible Informationen enthalten und somit zusätzlichen Schutzstufen erfordern. Entwickeln und dokumentieren Sie eine robuste Informationssicherheitsarchitektur als Teil eines Prozesses, um eine effektive Schutzstrategie zu etablieren. Es ist wichtig, dass Unternehmen ihre Netzwerke-Sicherheit stetig überwachen und periodisch überprüfen, um so ein aktuelles Verständnis der Netzwerkarchitektur mit dem Bewusstsein für die Sicherheit während des gesamten Lebenszyklus gewährleisten zu können. Von besonderer Bedeutung ist ein fundiertes Verständnis der Funktionen, welche die Systeme durchführen, wie auch der erforderlichen Sensibilität gegenüber den gespeicherten Informationen. Ohne dieses Verständnis kann das Risiko nicht ordnungsgemäss beurteilt werden und Schutzstrategien können nicht ausreichen. Die Dokumentation der Informationssicherheitsarchitektur und ihrer Komponenten sind entscheidend für das Verständnis der Gesamtschutzstrategie und die Identifizierung einzelner Fehlerpunkte.	ID.AM PR.DS PR.IP PR.MA PR.PT
14. Festlegung eines rigorosen, laufenden Risikomanagementprozesses. Ein gründliches Verständnis der Risiken von Netzwerk-Computing-Ressourcen bezüglich Denial-of-Service-Angriffen und die Anfälligkeit sensibler Informationen durch Kompromittierung, ist für ein effektives Cybersecurity-Programm unerlässlich. Risikobewertungen bilden die technische Grundlage dieses Verständnisses und sind entscheidend für die Formulierung effektiver Strategien zur Minderung von Schwachstellen und zur Wahrung der Integrität von Rechenressourcen. Anfänglich führen Sie eine Baseline-Risikoanalyse durch, die auf einer aktuellen Bedrohungsanalyse basiert, die für die Entwicklung einer Netzwerkschutzstrategie verwendet wird. Durch die sich schnell verändernde Technologie und die Entstehung neuer Bedrohungen auf einer täglichen Basis ist auch ein laufendes Risikobewertungsverfahren erforderlich, damit routinemässige Änderungen an der Schutzstrategie vorgenommen werden können. So kann sichergestellt werden, dass diese auch wirksam bleibt. Grundlegend für das Risikomanagement ist die Identifizierung des Restrisikos mit einer Netzwerk-Schutzstrategie und der Akzeptanz dieses Risikos durch das Management eines Unternehmens.	ID.RA ID.RM PR.IP
15. Aufbau einer Netzwerk-Schutzstrategie, die auf dem Prinzip der Verteidigung basiert. Ein Grundprinzip, das Teil einer Netzwerk-Schutzstrategie sein muss, ist verteidigungsorientiert. Die Verteidigung muss in der Entwurfsphase des Entwicklungsprozesses frühzeitig berücksichtigt werden und muss in allen technischen Entscheidungen, die mit dem Netzwerk verbunden sind, ein integraler Aspekt sein. Nutzen Sie technische und administrative Kontrollen, um Bedrohungen von identifizierten Risiken so weit wie möglich auf allen Ebenen des Netzwerks abzuschwächen. Single points of failure müssen vermieden werden, die Verteidigung der Cyber-Sicherheit muss überlagert sein, um so die Auswirkungen von Sicherheitsvorfällen zu begrenzen und zu verhindern. Zusätzlich muss jede Ebene gegen andere Systeme auf der gleichen Ebene geschützt werden. Beispielsweise sollen Nutzern nur diese Privilegien und Ressourcen zur Verfügung gestellt werden, welche für ihre Job-Funktion wirklich benötigen.	PR.AC PR.DS PR.IP PR.MA PR.PT

Spezifische Massnahmen zur Erhöhung der Sicherheit in den OT-Netzwerken	NIST Framework
16. Erkennung von Cyber-Sicherheitsanforderungen. Organisationen und Unternehmen benötigen strukturierte Sicherheitsprogramme mit vorgeschriebenen Anforderungen, um Erwartungen zu begründen und das Personal zur Rechenschaft zu ziehen. Formalisierte Richtlinien und Verfahren werden typischerweise verwendet, um ein Cyber-Sicherheitsprogramm zu etablieren und zu institutionalisieren. Ein formales Programm ist für die Festlegung eines konsequenten, standardbasierten Ansatzes für die Cyber-Sicherheit in einem Unternehmen unerlässlich und eliminiert die alleinige Abhängigkeit von der individuellen Initiative. Vorgaben und Prozesse informieren die Mitarbeiter auch über ihre spezifischen Verantwortlichkeiten im Bereich der Informations-Sicherheit und die Konsequenzen, wenn sie diese nicht erfüllen oder erfüllen können. Sie geben auch Leitlinien für Massnahmen, die während eines Cybersecurity-Vorfalls getroffen werden sollen, und fördern wirksame und effektive Massnahmen während einer Zeit der Krise. Als Teil der Identifizierung der Cyber-Sicherheitsanforderungen, gehören Benutzervereinbarungen und Benachrichtigung. Es müssen Anforderungen und Regeln festgelegt werden, welche die Bedrohung durch böswillige Insider minimieren, einschliesslich der Notwendigkeit, Hintergrundkontrollen durchzuführen und Netzwerkprivilegien auf die absolut notwendigen zu beschränken.	PR.AC PR.AT PR.DS PR.IP PR.MA PR.PT
17. Schaffung effektiver Konfigurationsmanagementprozesse. Um ein sicheres Netzwerk unterhalten zu können, ist ein grundlegender Management-Prozess das Konfigurationsmanagement. Das Konfigurationsmanagement muss sowohl Hardwarekonfigurationen als auch Softwarekonfigurationen abdecken. Änderungen an Hardware oder Software können leicht Schwachstellen einführen, die die Netzwerksicherheit untergraben. Prozesse sind erforderlich, um jede Änderung zu bewerten und zu kontrollieren, um sicherzustellen, dass das Netzwerk sicher bleibt. Das Konfigurationsmanagement beginnt mit bewährten und dokumentierten Sicherheitsgrundlagen für die verschiedenen Systeme.	PR.DS PR.IP PR.MA PR.PT
18. Durchführung von Routine-Selbsteinschätzungen. Robuste Performance-Evaluationsprozesse sind erforderlich, um Unternehmen eine Rückmeldung über die Wirksamkeit der Cybersecurity-Politik und die technische Umsetzung zu geben. Eine gute Organisation zeichnet sich aus, indem sie in der Lage ist, Probleme zu identifizieren, Ursachenanalysen durchzuführen und effektive Korrekturmassnahmen durchzuführen, die individuelle und systemische Probleme betreffen. Self-Assessment-Prozesse, die normalerweise Teil eines effektiven Cybersecurity-Programms sind, beinhalten das Routine-Scannen nach Schwachstellen, die automatisierte Auditierung des Netzwerks und die Selbsteinschätzung der organisatorischen und individuellen Leistung.	PR.AC PR.AT PR.DS PR.IP PR.PT
19. Erstellen Sie System-Backups und Notfall-Wiederherstellungspläne. Stellen Sie einen Notfall-Wiederherstellungsplan her, der eine rasche Wiederherstellung von jedem Notfall (einschliesslich eines Cyber-Angriffs) ermöglicht. System-Backups sind ein wesentlicher Bestandteil von nötigen Massnahmen und ermöglichen einen schnellen Wiederaufbau des Netzwerks. Überprüfen sie routinemässig Disaster Recovery Pläne, um sicherzustellen, dass sie funktionieren und somit die Systembetreuer und Nutzer mit diesen vertraut sind. Pflegen sie auf der Grundlage von Lehren aus Übungen kontinuierlich sinnvolle Änderungen in Notfall-Wiederherstellungspläne ein.	PR.DS PR.IP PR.MA PR.PT RC.RP RC.CO RC.IM

Spezifische Massnahmen zur Erhöhung der Sicherheit in den OT-Netzwerken	NIST Framework
20. Die Führungsebene bzw. das Management formulieren Erwartungen für Cybersecurity-Performance und halten Einzelpersonen verantwortlich für ihre Leistung. Effektive Cybersecurity-Performance erfordert Engagement und Führung von Führungskräften in den Unternehmen. Es ist wichtig, dass das oberste Management eine Erwartung für eine starke Cybersecurity festlegt und diese an ihre untergeordneten Führungskräfte in der gesamten Organisation weitergibt. Es ist auch wichtig, dass die oberste organisatorische Führung eine Struktur für die Umsetzung eines Cybersicherheitsprogramms aufbaut. Diese Struktur bildet die Fähigkeit, dass ein starkes Cybersecurity-Programm unterstützt wird. Es ist wichtig, dass einzelne Mitarbeiter für ihre Handlungen verantwortlich gemacht werden, da sie sich auf Cyber-Sicherheit bezieht. Dazu gehören Manager, Systemadministratoren, Techniker und Anwender / Betreiber.	PR.AC PR.AT PR.IP
21. Festlegung von Richtlinien und Durchführung von Schulungen, um die Wahrscheinlichkeit zu minimieren, dass das organisatorische Personal versehentlich vertrauliche Informationen über das Systemdesign der OT-Umgebung für kritische Infrastrukturen in der Stromversorgung, Operationen oder Sicherheitskontrollen offenlegt. Das Freigeben von Daten im Zusammenhang mit den OT-Netzwerken für kritische Infrastrukturen in der Stromversorgung obliegt einer strengen, Notwendigkeit-zu-wissen-Basis und ist nur für Personen, die ausdrücklich berechtigt sind solche Informationen zu erhalten. "Social Engineering", das Sammeln von Informationen über einen Computer oder Computernetzwerk über Fragen an naive Benutzer, ist oft der erste Schritt bei einem bösartigen Angriff auf Computernetzwerke. Je mehr Informationen über einen Computer oder ein Computernetzwerk bekannt sind, desto anfälliger ist der Computer bzw. das Netzwerk. Veröffentlichen Sie niemals Daten, die sich auf OT-Netzwerk für kritische Infrastrukturen in der Stromversorgung beziehen, einschliesslich der Namen und Kontaktinformationen zu den Systembetreibern und Administratoren, Computerbetriebssystemen und / oder physischen und logischen Standorten von Computern und Netzwerksystemen über Telefone oder Personal, sofern sie nicht explizit autorisiert sind, solche Information weiterzugeben. Jegliche Anforderung von Informationen durch unbekannte Personen muss an eine zuständige Stelle zur Überprüfung gemeldet werden. Menschen können eine schwache Verbindung in einem ansonsten sicheren Netzwerk sein. Das Durchführen von Schulungs- und Informationskampagnen ist zwingend notwendig, damit sichergestellt wird, dass das Personal mit dem Umgang mit sensiblen Netzwerkinformationen, insbesondere ihrer Passwörter, genügend Vorsicht schenkt.	PR.AC PR.AT PR.IP

Tabelle 38 Management-Aktionen, um ein effektives Cybersecurity-Programm zu etablieren

5. Weitere Tools und Hilfen zur Überprüfung und Bewertung

(1) Es gibt verschiedene Tools und Hilfen zur Überprüfung und Bewertung der eigenen implementierten Architektur.

5.1 Common Vulnerability Scoring System CVSS

(1) Das Common Vulnerability Scoring System (wörtlich übersetzt: „Allgemeines Verwundbarkeitsbewertungssystem“), abgekürzt CVSS, ist ein Industriestandard zur Bewertung des Schweregrades von möglichen oder tatsächlichen Sicherheitslücken in Computer-Systemen. Im CVSS werden Sicherheitslücken nach verschiedenen Kriterien, sogenannten Metrics, bewertet und miteinander verglichen, so dass eine Prioritätenliste für Gegenmassnahmen erstellt werden kann. CVSS ist selbst kein System zur Warnung vor Sicherheitslücken, sondern ein Standard, um verschiedene Beschreibungs- und Messsysteme miteinander kompatibel und allgemein verständlich zu machen.

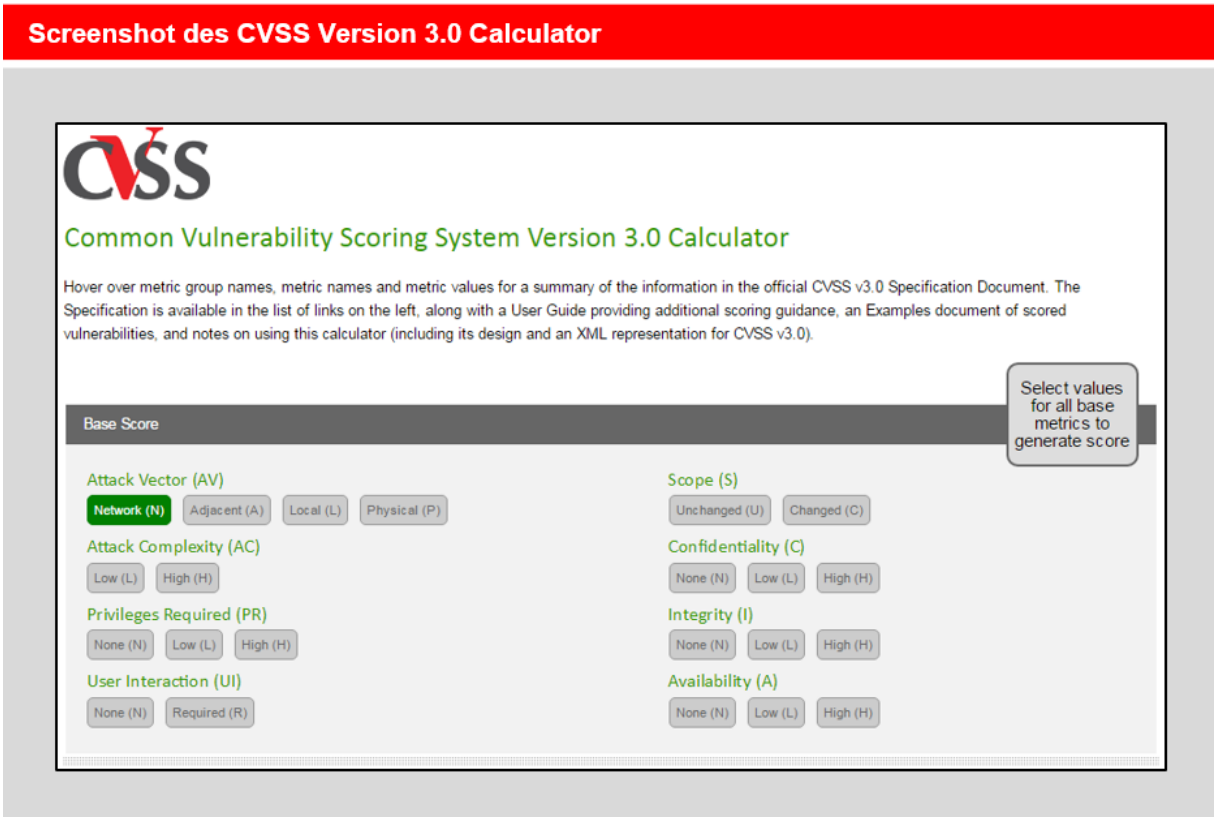

Abbildung 26 Screenshot des CVSS Version 3.0 Calculator

(2) CVSS wurde 2005 vom National Infrastructure Advisory Council (NIAC), einer Arbeitsgruppe des US-Ministeriums für Innere Sicherheit, in Auftrag gegeben und wird derzeit durch das Forum of Incident Response and Security Teams betreut. Den derzeitigen Vorsitz der Arbeitsgruppe CVSS-SIG Team hat David Ahmad von Symantec. In die Entwicklung von CVSS sind eingebunden: CERT, Cisco, DHS/MITRE, eBay, IBM, Microsoft, Qualys, Symantec. CVSS wird ferner unterstützt von HP, McAfee, Oracle, und Skype. Im Juni 2007 wurde die zweite Version des Scoring Systems veröffentlicht. Überarbeitungen. Mit CVSSv3.0 wurde das System im Juni 2015 neu aufgelegt und beinhaltet neben diversen Überarbeitungen der Metrik die Einführung von Schlüsselwörtern für die

Schweregrade (Kein / Niedrig / Mittel / Hoch / Kritisch) sowie eine Bedienungsanleitung und daran gekoppelte Beispielberichte.

5.2 Light and Right Security ICS (LARS ICS)

(1) Light and Right Security ICS (LARS ICS) ist ein kostenfreies Werkzeug des BSI Deutschland (Bundesamt für Sicherheit in der Informationstechnik), mit dem der Einstieg in die Cyber-Sicherheit für kleine und mittlere Unternehmen aus dem Umfeld industrieller Steuerungsanlagen erleichtert wird. Es bietet eine fragengeleitete Selbsteinschätzung des aktuellen Stands der Cybersecurity und gibt Empfehlungen, welche Massnahmen in welchen Bereichen als nächstes umgesetzt werden sollten.

Screenshot LARS ICS User Interface

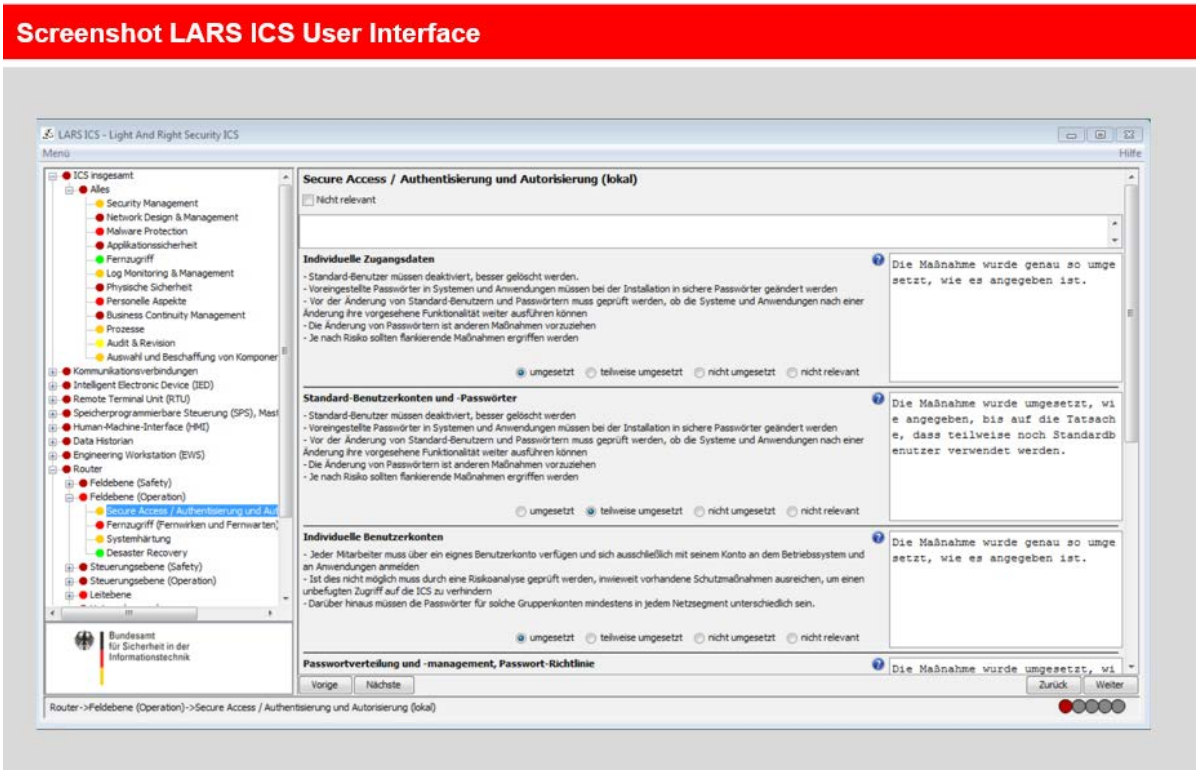

Abbildung 27 Screenshot LARS ICS User Interface

(2) Alle Massnahmen sind entsprechenden Teilen der Normen und Vorgehensweisen IT-Grundschutz, ISO 27001, IEC62443 und BSI ICS Security-Kompendium zugeordnet, was den Übergang zur Nutzung eines ganzheitlichen Managementsystems für Informationssicherheit erleichtert.

(3) Das Archiv beinhaltet neben dem eigentlichen Programm noch ein Handbuch und den vollständigen Quelltext von LARS ICS.

5.3 Cybersecurity Evaluation Tool CSET®

(1) Das Cybersecurity Evaluation Tool (CSET®) bietet einem systematischen, disziplinierten und wiederholbaren Ansatz zur Bewertung die Sicherheitssituation in einem Unternehmen. Es ist ein Software-Tool, welches Anlagen-Inhaber und -Betreiber mittels eines sequenziellen Prozesses ihre implementierten Sicherheit-Praktiken in industriellen Steuerung (ICS) und Informationstechnologie (IT) Netzwerken bewerten lässt. Die Nutzer können so ihre eigene Cybersecurity-Richtlinien und -Vorgaben gegenüber vielen anerkannte Regierungs- und Industriestandards und Empfehlungen vergleichen und bewerten. Die U.S. Amerikanische Homeland Security (DHS) und U.S. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) entwickelte die CSET-Anwendung und bietet es ohne Kostenfolgen für Endverbraucher an.

(2) CSET hilft Anlagen-Besitzer und -Betreiber, ihre Informationen und betrieblichen Systeme betreffend eingeführten Cybersicherheit-Massnahmen zu beurteilen, indem sie eine Reihe von detaillierten Fragen zu Systemkomponenten und Architekturen, sowie operative Massnahmen und Verfahren beantworten. Diese Fragen stammen aus anerkannten Industrie Cybersecurity Standards. Wenn die Fragebögen abgeschlossen sind, bietet CSET ein Dashboard mit Diagrammen an, in welchem Bereiche von Stärken und Schwächen aufgezeigt werden. Weiter erhält man eine priorisierte Liste von Empfehlungen zur Erhöhung der der Cybersicherheit im eignen Unternehmen und Systemen. CSET beinhaltet Lösungen, gemeinsame Praktiken, Kompensationsmassnahmen und Komponentenerweiterungen

(3) Die untenstehende Abbildung zeigt den High-Level-Prozess, der CSET-Bewertungen folgen.

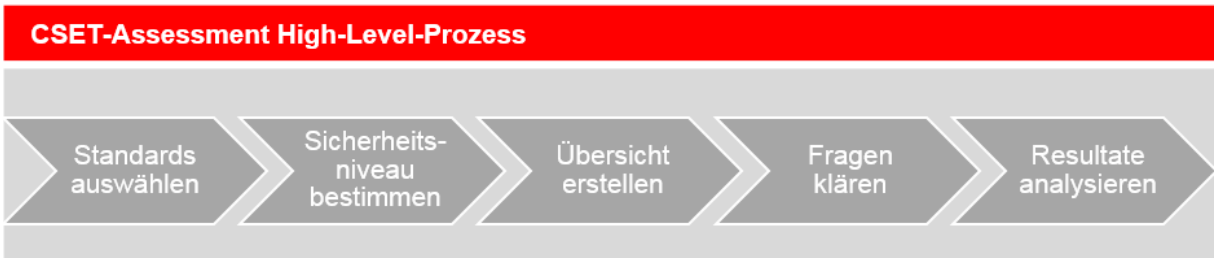

Abbildung 28 CSET-Assessment High-Level-Prozess

(4) Eine CSET-Auswertung dauert in der Regel etwa einen Tag. Typischerweise umfasst die CSET-Bewertung sowohl eine Schlüsselanforderungsbewertung als auch eine Komponentenbewertung. Das Tool nutzt integrierte Netzwerkübersichten, um eine visuelle Darstellung des aktuellen Sicherheitszustands des Systems zu liefern, die Komponentenziele für die Bewertung zu identifizieren und Anleitungen darüber zu geben, wo die Schutzmechanismen für die Cyber-Sicherheit platziert werden sollen. So sollen den Unternehmen den grössten Nutzen geboten werden.

6. Anhang

6.1 Grundlagen Dokumente und Standards

(1) Dieses Dokument berücksichtigt Konzepte, Empfehlungen und Massnahmen von verschiedenen Standards und anderen normativen Dokumenten, siehe untenstehende Tabelle.

Titel	Jahr	Herausgeber & Beschreibung
Massnahmen zum Schutz von industriellen Kontrollsystemen (ICS)	2013	**Melde- und Analysestelle Informationssicherung MELANI** Diese Anleitung beschreibt basierend auf US amerikanischen Unterlagen vom Department of Homeland Security, Industrial Control Systems - Cyber Emergency Response Team (ICS-CERT) sowie dem National Institute of Standards and Technology (NIST) knapp und pragmatisch auf 8 Seiten die wichtigsten 11 Massnahmen, die ICS-Betreiber gewährleisten müssen.
Risiko- und Verwundbarkeitsanalyse des Teilsektors Stromversorgung	2016	**Bundesamt für wirtschaftliche Landesversorgung (BWL)** Die Risiko- und Verwundbarkeitsanalyse ist basierend auf der Nationalen Cyber-Strategie (NCS) und der Strategie zum Schutz kritischer Infrastrukturen (SKI) entwickelt worden. Ziel ist die Analyse der Verwundbarkeit gegenüber Ausfällen oder Störungen der IKT im kritischen Teilsektor „Stromversorgung“.
Leitfaden Schutz kritischer Infrastrukturen (Leitfaden SKI)	2015	**Bundesamt für Bevölkerungsschutz (BABS)** Der Leitfaden stellt ein Instrument zur Überprüfung und gegebenenfalls Verbesserung der Resilienz der kritischen Infrastrukturen dar. Insbesondere ist er in Hinblick auf die Anwendung in kritischen Teilsektoren (z.B. Stromversorgung) durch Betreiber, Branchenverbänden (wie VSE) und Fachbehörden konzipiert. Im Wesentlichen beschreibt der Leitfaden ein mögliches Risikomanagement-Vorgehen: Analyse (Ressourcen-Identifikation, Verwundbarkeiten, Risiken), Bewertung, Massnahmen sowie deren Sicherstellung (Umsetzung, Überprüfung, Verbesserung). Das Vorgehen kann durchaus bzw. sollte gar in bestehende Managementprozesse integriert oder darauf aufbauend ausgeführt werden.
Nationale Strategie zum Schutz kritischer Infrastrukturen (SKI)	2012	**Bundesamt für Bevölkerungsschutz (BABS)** Die Strategie umschreibt den Geltungsbereich, bezeichnet die kritischen Infrastrukturen (u.a. Stromversorgung mit sehr grosser Kritikalität) und hält die übergeordneten Grundsätze beim Schutz kritischer Infrastrukturen fest. Die nationale SKI-Strategie richtet sich an alle Stellen, die im Um-feld des Schutzes kritischer Infrastrukturen Verantwortlichkeiten aufweisen, insbesondere an die jeweils zuständigen Behörden, die politischen Entscheidungsträger und die Betreiber von kritischen Infrastrukturen (z.B. Energieversorgungsunternehmen EVU).

Titel	Jahr	Herausgeber & Beschreibung
Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)	**2012**	Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) **Da der Schutz der Informations- und Kommunikationsinfrastrukturen vor Cyber-Risiken im nationalen Interesse der Schweiz liegt, hat der Bundesrat die nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken in Auftrag gegeben. Diese Strategie soll aufzeigen, wie diese Risiken heute aussehen, wie die Schweiz dagegen gerüstet ist, wo die Mängel liegen und wie diese am wirksamsten und effizientesten zu beheben sind.** **Die Strategie identifiziert vorhandene Strukturen, definiert Zielsetzungen sowie 7 Handlungsfelder mit entsprechenden Massnahmen (z.B. Risiko- und Verwundbarkeitsanalysen eines Teilsektors wie Stromversorgung – siehe weiter oben).**
ICT Continuity	2011	**Verband Schweizersicher Elektrizitätsunternehmen (VSE)** Ist ein Schlüsseldokument des Branchenverbandes mit Umsetzungsempfehlungen zur Gewährleistung der ständigen Disponibilität der Informatik- und der Kommunikationstechnologie zwecks Sicherstellung der Versorgung.
BDEW und oe: White Paper und Ausführungshinweise: Anforderungen an sichere Steuerungs- und Telekommunikationssysteme	2015	**Bundesverband der Energie- und Wasserwirtschaft (BDEW) und Österreichs E-Wirtschaft (oe)** Die beiden Dokumente beschreiben technische und betriebliche Sicherheitsmassnahmen für neu zu beschaffende bzw. neu einzuführende IT-gestützte Steuerungs- und Telekommunikationssysteme im Prozessbereich von Energieversorgungsunternehmen. Ziel ist die positive Beeinflussung der Produktentwicklung und die Vermittlung eines gemeinsamen Verständnisses. Adressaten sind potenzielle Auftragnehmer sowie unternehmensinterne Planer und Betreiber. Referenzen auf die internationalen Standards ISO 27002 und 27019 dienen lediglich als Hinweis, verbindlich umzusetzen sind immer nur die explizit aufgeführten Forderungen der vorliegenden Dokumente. Die Systematik unterscheidet sich denn auch etwas von den ISO-Standards.

Titel	Jahr	Herausgeber & Beschreibung
IT-Sicherheitskatalog gemäss §11 Absatz 1a Energiewirtschaftsgesetz	2015	**Bundesnetzagentur (BNetzA)** Deutsche Energieversorger müssen per Gesetz (EnWG 2011 in §11) bis spätestens 31. Januar 2018 einen angemessenen Schutz ihrer ICT-Systeme, die für einen sicheren Netzbetrieb notwendig sind, nachweisen und die an sie gestellten Anforderungen gegenüber der Bundesnetzagentur (BNetzA) durch ein Zertifikat belegen. Dazu veröffentlichte die BNetzA in Abstimmung mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) den IT-Sicherheitskatalog. Kernforderung des Sicherheitskatalogs ist die Einführung eines Informationssicherheits-Managementsystems (ISMS) gemäss DIN ISO/IEC 27001. Die Anforderungen des Sicherheitskatalogs sind von allen Netzbetreibern unabhängig von Grösse oder Anzahl angeschlossener Kunden zu erfüllen. Der Katalog enthält konkrete Anforderungen an Netzbetreiber, die unter Verweis auf die internationalen Standards umzusetzen sind.
ISO/IEC 27001:2013 **Information technology - Security techniques - Information security management systems - Requirements**	2013	**International Standard Organization (ISO) / International Electrotechnical Commission (IEC)** Detailliert die Anforderungen an ein Information Security Management System (ISMS). Die ISO 27k Serie umfasst eine Reihe von Information Security Standards, wovon folgende hier von Interesse sind: 27000:2016 Übersicht und Vokabular (:2016 indiziert Jahr der Herausgabe) 27001:2013 Anforderungen: Grundlagen mit Kontrollen und Kontrollzielen im Anhang 27002:2013 Leitfaden für Kontrollen 27003:2010 Anleitung zur Implementation 27005:2011 Risiko Management 27019:2013 Technischer Bericht mit Ergänzungen spezifisch für Prozesskontrollen in der Elektrizitätsversorgung Die ISO 27000 Security Standards sind mittlerweile die am meisten verbreiteten und dürften sich in den kommenden Jahren als die massgebenden erweisen. Schon heute liegt durchaus richtig, wer ISO Security Standards befolgt. Im Gegensatz zu anderen Standards, wie IT Grundschutz, NERC, ANSI/ISA oder NIST, sind sie nicht so sehr detailliert, dementsprechend flexibel anwendbar und können über eine längere Zeitspanne kontinuierlich verbessert und erweitert werden.
ISO/IEC 27002:2013 **Information technology - Security techniques - Code of practice for information security controls**		
ISO/IEC TR 27019:2013 **Information technology - Security techniques - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry**		

Titel	Jahr	Herausgeber & Beschreibung
NERC CIP – Critical Infrastructure Protection	2006 ff	**North American Electric Reliability Corporation (NERC)** Die NERC Critical Infrastructure Protection Standards sind derzeit in Version 5 und teilweise Version 6. Es sind die einzigen Standards in den USA, die nicht freiwillig, sondern zwingend durch die „Bulk Electric Systems“ (BES) bzw. deren Betreiber umgesetzt werden müssen. Es wird verlangt, dass die BES mindestens eine Security Policy definieren und implementieren, die vier Bereiche umfasst: Security Awareness, physische Sicherheit, Remote Access und Incident Response. Dabei reicht es nicht, Policies bloss zu dokumentieren, sondern Prozesse, Prozeduren und Kontrollen müssen implementiert und auch in einem Audit geprüft werden.
Guide to Industrial Control Systems (ICS) Security SP 800-82 Rev.2	2015	**National Institute of Standards and Technology (NIST)** Dieser Leitfaden gibt eine umfassende Einführung in ICS, Topologien und Architekturen, identifiziert Bedrohungen und Verwundbarkeiten und gibt Empfehlungen zu Gegenmassnahmen und Risikominderung. Zudem werden ICS-spezifische Kontrollen basierend auf dem NIST 800-53 Framework präsentiert.
ISA/IEC 62443 **Industrial Communication Networks - Network and System Security**	2009 ff	**International Society of Automation (ISA) / International Electrotechnical Commission (IEC)** Serie von insgesamt 13 Industrial Automation and Control System (IACS) Security Standards und technischen Berichten. Diese Normen sind allgemein anwendbar im Bereich industrieller Automation und nicht stromversorgungsspezifisch. Sie basieren auf den ISO 27000 Standards und erweitern diese mit Unterschieden und Spezifika industrieller Automation. Speziell zu erwähnen ist die Behandlung von Netzwerk- und Zonenarchitektur, die sich in anderen Standards kaum oder nicht so detailliert findet.
IEC 62351 **Power Systems Management and Associated Information Exchange - Data and Communications Security**	2007 ff	**International Electrotechnical Commission (IEC)** Dies ist ein stromversorgungsspezifischer Standard und ergänzt den IEC 62443 mit Unterschieden und Erweiterungen aus der Stromerzeugung, Übertragung und Verteilung. Er reiht sich mit weiteren Standards wie IEC 61850 zur Automation von Unterwerken sowie 60870 zu ICCP/TASE.2 mit seriellen und IP-basierten Kommunikationsprotokollen ein. Die IEC 62351 Standards (mittlerweile 13 Teile) sind technisch detailliert und können schwer mit konzeptionellen Sicherheitsstandards verglichen werden.

Titel	Jahr	Herausgeber & Beschreibung
IEEE 1686 **IEEE Standard for Intelligent Electronic Devices Cybersecurity Capabilities**	2013	**Institute of Electrical and Electronics Engineers (IEEE)** Funktionen und Konfigurationen, die in intelligenten elektronischen Geräten (IEDs) zwecks OT Sicherheit kritischer Infrastruktur zur Verfügung gestellt werden sollen, sind in dieser Norm definiert. Sicherheit in Bezug auf Zugriff, Betrieb, Konfiguration, Firmware-Revision und Datenabruf von einem IED sowie Datenverschlüsselung von und zu IEDs werden adressiert. Kommunikationen zum Zwecke des Stromschutzes (Teleprotektion) oder zum Schutz von Leben, Leib und Umwelt werden in dieser Norm nicht behandelt. Der Standard baut gewissermassen auf NERC-CIP (Critical Infrastructure Protection) auf und ergänzt diese auf IED Stufe, so dass elektronische Geräte nicht NERC-CIP Anforderungen unterlaufen.
Recommended Practice: **Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies**	2016	**Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)** Eine erweiterte und erneuerte Ausgabe einer früheren Veröffentlichung aus dem Jahre 2006. Umfassende Einführung in die Defense-in-Depth-Securitystrategie für industrielle Kontrollsysteme.
BSI IT-Grundschutz BSI-Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz (V1.2 2014) BSI Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz	2014 ff	**Bundesamt für Sicherheit in der Informationstechnik (BSI)** Der IT-Grundschutz beschreibt mit Hilfe der BSI-Standards 100-1 bis 100-3 eine Vorgehensweise zum Aufbau und zur Aufrechterhaltung eines Informations-Sicherheits-Management-Systems (ISMS). Die IT-Grundschutz-Kataloge bzw. das IT-Grundschutz-Kompendium beschreiben die Umsetzung der damit einhergehenden Massnahmen und Ziele. Das damit auf-gebaute ISMS erfüllt die Anforderungen von ISO 27001 und verfügt über ein Äquivalent zu den Handlungsempfehlungen von ISO 27002. Sicherheit kann nach den vom BSI entwickelten Vorgehensweisen des IT-Grundschutzes, aber auch nach Standards der ISO 27000-Familie eingeführt und kontrolliert werden. Beide Möglichkeiten sind von ihrem Ansatz her kompatibel. Mit beiden wird ein ISMS aufgebaut und betrieben, mit dem Risiken im Bereich der Informationssicherheit ermittelt und durch geeignete Massnahmen auf ein akzeptables Mass reduziert werden. Ein wesentlicher Bestandteil eines ISMS nach ISO 27001 ist die Risikoanalyse und -bewertung, wohingegen eine Risikoanalyse beim BSI-Grundschutz nur in besonderen Fällen erforderlich ist. In den BSI-Grundschutzkatalogen wird die detaillierte Vorgehens-weise zur Minimierung von Risiken beschrieben. Demnach lassen die ISO-Standards mehr Interpretation offen und sind flexibler, geben aber auch entsprechend weniger detailliert Anleitung und Unterstützung. Für den IT-Grundschutz-Ansatz gilt demnach entsprechend das Gegenteil und bietet, wie der Name aussagt, einen „Grundschutz“. Der Aufwand für eine ISO-basierte Zertifizierung ist geringer.

Titel	Jahr	Herausgeber & Beschreibung
BSI ICS Security - Kompendium	2013	**Bundesamt für Sicherheit in der Informationstechnik (BSI)** Das Kompendium stellt ein Grundlagenwerk dar und soll einen einfachen Zugang zur ICS IT Security ermöglichen. Erläutert werden die notwendigen ICS-Grundlagen, Abläufe, relevante Standards und ein konkreter Zusammenhang zum IT-Grundschutz, wobei auch Unterschiede und Lücken etablierter Standards und insbesondere des IT-Grundschutzes im Bereich ICS-Security aufgezeigt werden.
BSI-Standard 200-1 Managementsysteme für Informationssicherheit (ISMS)	**2017**	Bundesamt für Sicherheit in der Informationstechnik (BSI) **Der Standard beschreibt ISMS-relevante Methoden, Aufgaben und Aktivitäten, welche ein erfolgreiches ISMS ausmachen und welche Aufgaben auf die Führungsebene zukommen. Bei der Umsetzung der Empfehlungen hilft die Methodik des IT-Grundschutzes, die eine Schritt-für-Schritt-Anleitung für die Entwicklung eines ISMS in der Praxis gibt und konkrete Massnahmen für alle Aspekte der Informationssicherheit nennt. Der Standard 200-1 richtet sich an Verantwortliche für den IT-Betrieb, Sicherheitsbeauftragte, -experten und -berater, welche mit dem Management für Informationssicherheit betraut sind.**
BSI-Standard 200-2 IT-Grundschutz Vorgehensweise	2017	**Bundesamt für Sicherheit in der Informationstechnik (BSI)** Die IT-Grundschutz-Vorgehensweise beschreibt Schritt für Schritt, wie ein Managementsystem für Informationssicherheit in der Praxis und mit Hilfe der Grundschutzkataloge aufgebaut und betrieben werden kann. Es wird sehr ausführlich darauf eingegangen, wie ein Sicherheitskonzept in der Praxis erstellt wird, wie angemessene Sicherheitsmassnahmen ausgewählt werden und was bei der Umsetzung zu beachten ist.
BSI-Standard 200-3 Risikoanalyse	2017	**Bundesamt für Sicherheit in der Informationstechnik (BSI)** Dieses Dokument beschreibt eine Methodik zur Durchführung von Risikoanalysen, die ein bestehendes IT Grundschutz Sicherheitskonzept ergänzen. Dabei werden die in den IT-Grundschutz-Katalogen beschriebenen Gefährdungen als Hilfsmittel verwendet. Ein wesentlicher Unterschied zu den meisten anderen Risikoanalysemethoden ist das gänzliche Weglassen von Eintrittswahrscheinlichkeiten von Schadensereignissen.
BSI-Standard 100-4 Notfallorganisation	2008	**Bundesamt für Sicherheit in der Informationstechnik (BSI)** Dieses Dokument beschreibt eine Methodik zur Etablierung eines Notfallmanagements, welche auf die in Standard 100-2 beschriebenen Vorgehensweisen aufsetzt und ergänzt. Beschrieben werden sämtliche Prozesse innerhalb einer Notfallorganisation von Business Impact Analyse über Krisenmanagement bis hin zu Rückführung und kontinuierlichen Prozesstätigkeiten ausserhalb von Krisensituationen.

Titel	Jahr	Herausgeber & Beschreibung
ISA 95 / IEC/ISO 62264 Enterprise Control System Integration	2010 ff	**International Society of Automation (ISA) / International Electrotechnical Commission (IEC)** Eine Normenreihe von insgesamt 5 Standards zur Integration von Unternehmens-IT und Kontroll-Leitsystemen.
Framework for Improving Critical Infrastructure Cybersecurity	2014 Draft v1.1 2017	**National Institute of Standards and Technology (NIST)** Dieses Framework stammt aus der Forderung der US Presidential Executive Order „Improving Critical Infrastructure Cybersecurity“ aus dem Jahre 2013. Es ist eine Zusammenstellung verschiedener Guidelines, um den aktuellen Status in einem Unternehmen zu ermitteln und eine Roadmap zu verbesserten Cybersecurity-Praktiken mit Verweisen zu anderen Frameworks und Standards wie ISO27001, ISA 62443, NIST 800-53 und Cobit zu definieren.
Energy Sector Cybersecurity Framework Implementation Guidance	2015	**Department of Energy (DOE)** Eine Anleitung des DOE zur Implementierung eines Critical Infrastructure Cybersecurity Frameworks in Anlehnung an das Framework vom NIST.
Report on Cybersecurity In-formation Sharing in the Energy Sector	2016	**European Union Agency for Network and Information Security (ENISA)** Ziel dieses Berichtes ist es, die Entwicklung von CSIRTs (Computer Security Incident Response Team), ISACs (Information Sharing and Analysis Center) sowie relevante Initiativen zum Informationsaustausch über Cybersecurity Incidents im Energiesektor zu verstehen und zu erlernen. Sie konzentriert sich auf die in der NIS-Richtlinie (European Parliament and Council, 2016: Netz und Informationssicherheit) identifizierten Teilsektoren Strom, Öl und Gas.
Communication network dependencies for ICS/SCADA Systems	2016	**European Union Agency for Network and Information Security (ENISA)** Dieser Bericht konzentriert sich auf die Aspekte der Kommunikationsnetze und der Interkommunikation zwischen ICS/SCADA und der Erkennung von Schwachstellen, Risiken, Bedrohungen und Sicherheitsauswirkungen, die durch cyberphysikalische Systeme verursacht werden können. Der Bericht enthält auch eine Reihe von Empfehlungen zur Minderung der identifizierten Risiken. Das wichtigste Ergebnis der vorgängigen Studie ist eine Liste von bewährten Praktiken und Richtlinien, um die Angriffsfläche von ICS/SCADA-Systemen so weit wie möglich zu begrenzen. Das Hauptziel des Dokumentes ist es, einen Einblick in die Kommunikationsnetzwerkabhängigkeiten der ICS/SCADA-Systeme zu geben sowie kritische Sicherheitsressourcen und realistische Angriffsszenarien und Bedrohungen gegen diese Kommunikationsnetze zu identifizieren.

Titel	Jahr	Herausgeber & Beschreibung
VDI/VDE 2182 **Informationssicherheit in der industriellen Automatisierung**	2011 - 2016	**Verein Deutscher Ingenieure (VDI) / Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE)** Diese Richtlinie beschreibt, wie die Informationssicherheit von automatisierten Maschinen und Anlagen durch die Umsetzung von konkreten Schutzmassnahmen erreicht werden kann. Dazu werden Aspekte der eingesetzten Automatisierungsgeräte, -systeme und -anwendungen betrachtet. Auf der Basis einer zwischen Herstellern von Automatisierungsgeräten und -systemen und deren Nutzern (z.B. Maschinenbauern, Integratoren, Betreibern) abgestimmten gemeinsamen Begriffsdefinition wird eine einheitliche, praktikable Vorgehensweise beschrieben, wie Informationssicherheit im gesamten Lebenszyklus von Automatisierungsgeräten, -systemen und -anwendungen gewährleistet werden kann. Der Lebenszyklus berücksichtigt die Phasen der Entwicklung, Integration, des Betriebs, der Migration und Ausserbetriebsetzung. Die Richtlinie definiert ein einfaches Vorgehensmodell zur Bearbeitung und Darstellung der Informationssicherheit. Das Modell besteht aus mehreren Prozessschritten.

Tabelle 39 Nationale und internationale Standards zur ICT-Sicherheit

6.2 Glossar

Begriffe	Definition
Business Continuity Management (BCM)	Business Continuity Management (BCM) ist ein unternehmensweiter Ansatz, mit dem sichergestellt wird, dass kritische Geschäftsprozesse im Falle von massiven, einschneidenden internen oder externen Ereignissen aufrechterhalten werden können. BCM zielt auf eine Minimierung der operationellen, finanziellen, rechtlichen und reputationsbezogenen Auswirkungen solcher Ereignisse hin (Quelle BCMWeisung)
Cybersecurity	Unter dem Begriff «Cybersecurity» werden alle organisatorischen und technischen Massnahmen zum Schutz der Verfügbarkeit, Unversehrtheit (Integrität) und Vertraulichkeit von Informationen sowohl der IT als auch der OT verstanden.
Datendiode	Eine Datendiode ist ein Netzwerkgerät, welches den Netzwerkverkehr nur in eine Richtung zulässt. Dabei gilt, dass Daten nur aus einer sicheren Netzwerkzone in eine unsichere Netzwerkzone ausgetauscht werden können, jedoch nicht von der unsicheren in die sichere Zone.
Defense-in-depth	Als „Defense-in-Depth“ werden mehrstufige Sicherheitskonzepte verstanden, die über die rein technische IT-Sicherheit hinausgehen. „Defense-In-Depth“-Konzepte berücksichtigen zusätzlich zum Beispiel auch physische Sicherheit, Business Continuity Management, Prozesse, Menschen und externe Dienstleister.
Demilitarized Zone (DMZ)	Unter entmilitarisierte Zone versteht man ein logisch und / oder physisch abgetrenntes Sub-Netz mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten auf die daran angeschlossenen Systeme.
Dienstleistungsvereinbarung (SLA)	Die Abkürzung “SLA” steht für “Service Level Agreement“. Darunter wird eine vertraglich vereinbarte Leistung verstanden, zu deren Erfüllung sich der IT-Dienstleister verpflichtet hat. Üblicherweise werden in SLA maximal zulässige Ausfall- und Reaktionszeiten definiert.
Facilitymanagement	Siehe Gebäudeleittechnik
Feldbus	Ein Feldbus ist ein Netzwerkelement, welches mehrere Geräte in einem OT-Umfeld miteinander verbindet. Feldbus-Geräte sind per Definition echtzeitfähig. Typischerweise werden in einer Anlage Feldgeräte wie Messfühler (Sensoren) und Stellglieder (Aktoren) zwecks Kommunikation mit einem Automatisierungsgerät verbunden.
Feldgerät	Ein Feldgerät ist eine technische Einrichtung im Bereich der Automatisierungstechnik, die mit einem Produktionsprozess in direkter Beziehung steht. „Feld“ bezeichnet in der Automatisierungstechnik den Bereich ausserhalb von Schaltschränken bzw. Leitwarten.
Feldleittechnik	«Vor-Ort»-Steuerung und «Vor-Ort»-Überwachung einzelner Schaltfelder
Fernwirk-Kopf	Datenkonzentrator wird als Fernwirkgerät zur Automatisierung der Ortsnetzstation und zur Erfassung von Zählerdaten angewendet.
Fernwirktechnik	Unter Fernwirken wird die Fernüberwachung und -steuerung räumlich entfernter Objekte mittels signalumsetzender Verfahren, von einem oder mehreren Orten aus, verstanden. (Quelle Wikipedia)

Begriffe	Definition
Field devices	Siehe Feldgerät
Fieldbus	Siehe Feldbus
Firewall	Eine Firewall (besser mit Sicherheitsgateway bezeichnet) ist ein System aus soft- und hardwaretechnischen Komponenten, um IP-Netze sicher zu koppeln. (Quelle BSI)
Frontend	Siehe Fernwirk-Kopf
Gateway	Das Wort Gateway bezeichnet in der Informatik eine Komponente (Hard- und/oder Software), welche zwischen zwei Systemen eine Verbindung herstellt. (Quelle Wikipedia)
Gebäudeleittechnik	Gebäudeleittechnik bezeichnet die Verwaltung und Bewirtschaftung von Gebäuden sowie deren technische Anlagen und Einrichtungen.
Härtung	Unter Härten versteht man in der Computertechnik, die Sicherheit eines Systems zu erhöhen, indem nur dedizierte Software eingesetzt wird, die für den Betrieb des Systems notwendig ist, und deren unter Sicherheitsaspekten korrekter Ablauf garantiert werden kann. Das System soll dadurch besser vor externen Angriffen geschützt sein. (Quelle Wikipedia)
Hausleittechnik	Siehe Gebäudeleittechnik
Human Maschine Interface (HMI)	Die Benutzerschnittstelle wird auch „Mensch-Maschine-Schnittstelle“ (MMS) oder Englisch „Human Machine Interface“ (HMI) oder „Man Machine Interface“ (MMI) genannt und erlaubt dem Bediener unter Umständen über das Bedienen der Maschine hinaus das Beobachten der Anlagenzustände und das Eingreifen in den Prozess.
Industrial Control Systems (ICS)	Industrial Control Systems werden in der Industrie sowie im Bereich kritischer Infrastrukturen für Steuerungs-, Mess- und Regelfunktionalitäten eingesetzt.
Intelligent Electronic Device (IED)	Ein Intelligent Electronic Device (IED) ist ein Begriff, der in der Elektrizitätsindustrie verwendet wird, um mikroprozessorbasierte Steuerungen von Stromversorgungssystemen, wie etwa Leistungsschalter, Transformatoren und Kondensatorbänke, zu beschreiben.
Information Communications Technology (ICT)	Siehe Informations- und Kommunikationstechnik
Information Security Management System (ISMS)	Das Information Security Management ist eine Aufstellung von Verfahren und Regeln innerhalb eines Unternehmens, welche dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.
Informations- und Kommunikationstechnik (IKT)	Informations- und Kommunikationstechnologien (IKT) sind die Methoden und Technologien, die die Übertragung, den Empfang und die Verarbeitung von Informationen (einschliesslich digitaler Technologien) realisieren.

Begriffe	Definition
Integrität	Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf "Informationen" angewendet. Der Begriff "Information" wird dabei für "Daten" verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden. (Quelle: BSI)
Intrusion Detection System (IDS)	Intrusion Detection System ist ein System zur automatisierten Erkennung von Angriffen auf Computernetzwerke.
Intrusion prevention system (IPS)	Ein Intrusion Prevention System ist in der Lage Angriffe auf Netzwerke oder Computersysteme zu erkennen und automatische Abwehrmassnahmen zu ergreifen.
IT-Security	Siehe IT-Sicherheit
IT-Sicherheit	Unter «IT-Sicherheit» werden alle organisatorischen und technischen Massnahmen zum Schutz der Verfügbarkeit, Unversehrtheit (Integrität) und Vertraulichkeit von Informationen verstanden. Information Technology (IT) meint dabei Technologien zur Datenverarbeitung, welche nicht direkt mit der Bereitstellung von Elektrizität zu tun haben (z.B. Kundendatenmanagement, Rechenzentren).
KPI	Der Begriff Key Performance Indicator (KPI) bzw. Leistungskennzahl bezeichnet Kennzahlen, anhand derer der Fortschritt oder der Erfüllungsgrad hinsichtlich wichtiger Zielsetzungen oder kritischer Erfolgsfaktoren innerhalb einer Organisation gemessen und/oder ermittelt werden kann.
Legacy-System	Der Begriff Altsystem bezeichnet in der Informatik eine etablierte, historisch gewachsene Anwendung im Bereich Unternehmenssoftware.
Leittechnik	Die Leittechnik fasst die Datenströme der untergeordneten Ebenen, dem Feld oder einzelner Zellen, wie zum Beispiel Signale der Mess-, Steuer- und Regelungstechnik zusammen, um dadurch den gesamten Fertigungsprozess zu steuern und zu überwachen.
Local Area Network (LAN)	Local area network ist ein Rechnernetz, das Computer und intelligente Geräte in eine limitierte geografische Zone verbindet (normalerweise unter 10 km).
Malware	Computerprogramme, die entwickelt wurden, um unerwünschte oder gegebenenfalls schädlich Funktionen auszuführen.
Man-Machine Interface (MMI)	Siehe Human Maschine Interface
Media Access Control Address (MAC Address)	Media Access Control Address wird die eindeutige Hardware-Adresse in einem Netzwerkadapter genannt. Diese wird vom Hersteller unveränderlich in das ROM eines gebrannt. Die Einträge werden weltweit einmalig vergeben.

Begriffe	Definition
MELANI	Die Melde- und Analysestelle Informationssicherung MELANI ist eine Organisation der Bundesverwaltung der Schweiz. Hauptaufgabe von MELANI ist der Schutz der nationalen kritischen Infrastrukturen.
Mensch-Maschine-Schnittstelle (MMS)	Siehe Human Maschine Interface
Multiprotocol Label Switching - Transport Profile (MPLS-TP)	Das MPLS-TP wurde speziell für Metro-, Aggregation- und Access-Netze optimiert. Die Ziele dabei: Vergleichbare Funktionalitäten wie TDM-basierte (Time Division Multiplexing) Technologien bereitstellen zu können und die Unterstützung von Point-to-Point- und Any-to-Any-Verbindungen mit einem ähnlich hohen Grad an Berechenbarkeit, Zuverlässigkeit und OAM-Funktionalitäten (Operations-, Administration-and-Management), wie sie die langjährig bewährten TDM-Netze bieten.
Multiprotocol Label Switching (MPLS)	Multiprotocol Label Switching ermöglicht die verbindungsorientierte Übertragung von Datenpaketen in einem verbindungslosen Netz entlang eines zuvor aufgebauten („signalisierten“) Pfads. Dieses Vermittlungsverfahren wird überwiegend von Betreibern grosser Transportnetze eingesetzt, die Sprach- und Datendienste auf Basis von IP anbieten. (Quelle Wikipedia)
Network access control (NAC)	Network access control oder Netzwerkszugangskontrolle ist eine Technik angewendet um sich gegen unautorisierte Netzwerkzugriffe zu schützen.
Network Address Translation (NAT)	Network Address Translation (NAT) bezeichnet ein Verfahren zum automatischen und transparenten Ersetzen von Adressinformationen in Datenpaketen. NAT-Verfahren kommen meist auf Routern und Sicherheits-Gateways zum Einsatz, vor allem, um den beschränkten IPv4-Adressraum möglichst effizient zu nutzen und um lokale IP-Adressen gegenüber öffentlichen Netzen zu verbergen. (Quelle BSI)
Netzleittechnik	Umfasst die Mess-, Steuerungs- und Regelungstechnik von Netzen wie zum Beispiel den Stromnetzen. Die Netzleittechnik ist ein Spezialgebiet der Prozessleittechnik; sie gehört zu den Angewandten Ingenieurwissenschaften.
Normalbetrieb	Anlagezustand innerhalb spezifischer Betriebsgrenzen und gemäss geltender Vorschriften (Quelle ENSI)
OEM	Original Equipment Manufacturer, übersetzt «Originalausrüstungshersteller». Darunter versteht man einen Hersteller von Komponenten oder Produkten, der diese in seinen eigenen Fabriken produziert, sie aber nicht selbst in den Einzelhandel bringt. OEM-Software kann sich von der sogenannten Vollversion (Retail) durch einen geringeren Lieferumfang oder eingeschränkte Funktionalität unterscheiden.
OT-Sicherheit	Unter «OT-Sicherheit» werden alle organisatorischen und technischen Massnahmen zum Schutz der Verfügbarkeit, Unversehrtheit (Integrität) und Vertraulichkeit von Informationen zur Überwachung und Steuerung der Anlagen zur Elektrizitätsverteilung (und -produktion) sowie der Schutz von Personen und Anlagen verstanden. Operational Technology (OT) meint dabei Technologien, welche direkt für die Bereitstellung oder Lieferung von Elektrizität notwendig sind (z.B. SCADA, PIA, Remote Access auf Installationen in Unterwerken, Rundsteuerung, Smart Meter).

Begriffe	Definition
Partner Informations Austausch (PIA)	Partner Informationssystem. Schweizerische geschlossene Plattform mit dem Ziel, Daten zwischen den Leitstellen austauschen. Diese Informationen werden primär für die Netzführung und Netzsteuerung genutzt.
Penetration Test	Unter «Penetration Test» wird ein umfassender Sicherheitstest einzelner Systeme oder Netzwerke verstanden. Es geht um die Prüfung der technischen Umsetzung der Cyber-Sicherheitsmassnahmen. Penetration Tests sind ein Bestandteil eines Sicherheitsaudits.
Plesiochrone Digitale Hierarchie (PDH)	Die Plesiochrone Digitale ist eine international standardisierte Technik zum Multiplexen digitaler Datenströme, die über Weitverkehrsstrecken übertragen werden. Die Datenströme müssen annähernd synchron sein. Heute wird diese Technik fast nur noch bei Datenübertragungsraten bis zu 45 Mbit/s verwendet.
Primärtechnik	Ausser den zur Umspannung notwendigen Transformatoren sind im Umspannwerk auch Schaltanlagen für die ober- und unterspannungsseitig abgehenden Leitungen vorhanden. Die technischen Einrichtungen (Transformatoren, Sammelschienen etc.) sowie die Leitungen sind in der Regel redundant ausgelegt, so dass bei Ausfall eines Betriebsmittels die Versorgung weiterhin gewährleistet ist.
Programmable logical control (PLC)	Siehe Speicherprogrammierbare Steuerung
Prozesskoppelsystem	Das Prozesskoppelsystem stellt das Verbindungselement zwischen der Prozessebene und der Leitebene dar.
Prozessleittechnik	Als Prozessleittechnik bezeichnet man Mittel und Verfahren, die dem Steuern, Regeln und Sichern verfahrenstechnischer Anlagen dienen. Zentrales Mittel sind dabei das Prozessleitsystem und die Speicherprogrammierbare Steuerung.
Remote Terminal Unit (RTU)	Als Remote Terminal Unit (RTU, deutsch Fernbedienungsterminal) wird ein regeltechnisches bzw. steuerungstechnisches Instrument zur Fernsteuerung bezeichnet.
Risiko	Risiko ist die häufig auf Berechnungen beruhende Vorhersage eines möglichen Schadens im negativen Fall (Gefahr) oder eines möglichen Nutzens im positiven Fall (Chance). Was als Schaden oder Nutzen aufgefasst wird, hängt von Wertvorstellungen ab. Risiko wird auch häufig definiert als die Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmass dieses Schadens. (Quelle BSI)
Router	Router sind Netzwerkgeräte, die Netzwerkpakete zwischen mehreren Rechnernetzen weiterleiten können
Sandbox	Eine Sandbox ist ein isolierter Bereich innerhalb einer Anwendung oder eines Betriebssystems. Sie verhindert, dass unerwünschte Aktionen ausserhalb des kontrollierten Umfelds ausgeführt werden können. Dadurch werden die Gefahren und Auswirkungen von Schadprogrammen abgewehrt. (Quelle BSI)
Schadsoftware	Siehe Malware

Begriffe	Definition
Schutzobjekt	Schutzobjekte sind Infrastrukturen, Services, Systeme, Anwendungen, Netzwerke, Datensammlungen, etc., die zur Erfüllung des Unternehmensauftrags eingesetzt und somit geschützt werden müssen.
Schutzsysteme	Sicherungssystem bestehend aus Sensoren, Logik und Steuerelementen, um einen Prozess in einen sicheren Zustand zurückzuführen, wenn vordefinierte Konditionen verletzt wurden.
Schutzziel	Schutzziele beschrieben Schutzobjekte die mit den entsprechenden Massnahmen geschützt werden.
Sekundärtechnik	Unter den Begriff Sekundärtechnik fallen die Einrichtungen eines Umspannwerks, die an der Umspannung in direktem Sinn nicht beteiligt sind. Darunter versteht man z.B. lokale Steuerung, Spannungsregelung, Netzschutz, Energiezählung, Fernsteuerung, usw.
Sicherheitsaudit	Unter «Sicherheitsaudit» wird eine umfassende Prüfung der organisatorischen und technischen Cyber-Sicherheitsmassnahmen verstanden. Es geht um die Analyse von Schwachstellen der Cyber-Sicherheit im Bereich der Konzeption/Architektur, Implementierung, Betrieb, menschliches Fehlverhalten und Standortsicherheit sowie die Sicherheit der einzelnen Systemkomponenten.
Sicherheitskultur	Sicherheitskultur umfasst von den Mitgliedern der Organisation des Betreibers einer Kernanlage geteilte Werte, Weltbilder, verbales und nonverbales Verhalten sowie Merkmale der vom Menschen geschaffenen physischen Umgebung. Zur Sicherheitskultur gehören jene Werte, jene Weltbilder, jenes Verhalten und jene Umgebungsmerkmale, die bestimmen oder zeigen, wie die Mitglieder der Organisation mit nuklearer Sicherheit umgehen (Quelle ENSI)
Security Information and Event Management (SIEM)	SIEM Systeme werden eingesetzt um sicherheitsrelevante Ereignisse zu identifizieren, zu bewerten und den Administrator daraufhin zu alarmieren.
SIS Protection	Siehe Schutzsysteme
Smart metering	Intelligente Messsysteme, die über eine bidirektionale Kommunikation ihre Messdaten übertragen und Steueraufgaben übernehmen können.
Speicherprogrammierbare Steuerung (SPS)	Eine speicherprogrammierbare Steuerung ist ein Gerät, das zur Steuerung oder Regelung einer Maschine oder Anlage eingesetzt und auf digitaler Basis programmiert wird. (Quelle Wikipedia)
Stationsbus	Bussystem in einem Unterwerk (UW) zwischen der UW-Leitstelle und den Sensoren im Stromfeld.
Stationsleittechnik	Gesamtsteuerung in einem Unterwerk bestehend aus Leitstelle, Sensoren und Aktionen. Ist das Bindeglied zwischen dem Prozess und der Netzleitebene.
Stromzähler	Stromzähler für die Messung der elektrischen Arbeit (Summierung von Wirkleistung).

Begriffe	Definition
Supervisory Control and Data Acquisition (SCADA)	Unter Supervisory Control and Data Acquisition versteht man das Überwachen und Steuern technischer Prozesse mittels eines Computer-Systems. Synonym: ICS-System (Industrial Control System)
Switch	In Computer-Netzwerken wird als Switch ein Kopplungselement, das Netzwerksegmente miteinander verbindet.
Synchrone Digitale Hierarchie (SDH)	Die Synchrone Digitale Hierarchie ist eine der Multiplextechniken im Bereich der Telekommunikation, die das Zusammenfassen von niederratigen Datenströmen zu einem hochratigen Datenstrom erlaubt. Das gesamte Netz ist dabei synchron.
Tunneling	Tunnel bzw. Tunneling bezeichnet in einem Netzwerk die Konvertierung und Übertragung eines Kommunikationsprotokolls, das für den Transport in ein anderes Kommunikationsprotokoll eingebettet wird.
Utility	Energieversorgungsunternehmen
Verfügbarkeit	Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können. (Quelle BSI)
Verschlüsselung	Verschlüsselung (auch Chiffrierung) ist die von einem Schlüssel abhängige Umwandlung von „Klartext“ genannten Daten in einen „Geheimtext“ (auch „Chiffrat“), so dass der Klartext aus dem Geheimtext nur unter Verwendung eines geheimen Schlüssels wiedergewonnen werden kann.
Vertraulichkeit	Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschliesslich Befugten in der zulässigen Weise zugänglich sein. (Quelle BSI)
Virtual LANs (VLAN)	Virtuelle lokale Netze werden zur logischen Strukturierung von Netzen verwendet. Dabei wird innerhalb eines physikalischen Netzes eine logische Netzstruktur abgebildet, indem funktionell zusammengehörende Arbeitsstationen und Server zu einem virtuellen Netz verbunden werden.
Virtual Private Network (VPN)	Virtual Private Network ist ein virtuelles privates (in sich geschlossenes) Kommunikationsnetz, das ein bestehendes Kommunikationsnetz als Transportmedium verwendet.
Werktelefonie	Nottelefon zur Kommunikation zwischen Leitstellen, Kraftwerken und Stationen. Wird insbesondere bei ausgefallenem Leitsystem und Mobil- und Bürotelefonie genutzt.
Wide Area Network (WAN)	Wide Area Network ist ein Rechnernetz, das sich im Unterschied zu einem LAN über einen sehr grossen geografischen Bereich erstreckt.
Zähler	Siehe Stromzähler

Tabelle 40 Glossar

6.3 Abkürzungen

Abkürzung	Beschreibung
DMZ	Demilitarized Zone
HMI	Human Maschine Interface
ICS	Industrial Control Systems
ICT	Information and communication technology
ICT	Information Communications Technology
IDS	Intrusion Detection System
IED	Intelligent Electronic Device
IKT	Informations- und Kommunikationstechnik
IPS	Intrusion Prevention System
ISMS	Information Security Management System
IT	Information technology
KVM	Keyboard, Video und Maus
LAN	Local Area Network
MAC Address	Media Access Control Address
MMI	Man Maschine Interface
MMS	Mensch-Maschine-Schnittstelle
MPLS	Multiprotokoll Label Switching
MPLS-TP	Multiprotokoll Label Switching - Transport Profile
NAC	Network Access Control
NAT	Network Address Translation
OT	Operational Technology
PDH	Plesiochronous Digital Hierarchy
PIA	Partner Informations Austausch
PLC	Programmable logic control
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
SDH	Synchronous Digital Hierarchy
SIEM	Security information and event management
SLA	Service Level Agreement, Dienstleistungsvereinbarung
SPS	Speicherprogrammierbare Steuerung
UFLS	Unterfrequenzabhängiger Lastabwurf
VLAN	Virtual LANs
VPN	Virtual Private Network
WAN	Wide Area Network

Tabelle 41 Abkürzungsverzeichnis