Allianz für Cyber-Sicherheit

VDMA

ZVEI: Die Elektroindustrie

INTERNATIONAL DATA SPACES ASSOCIATION

Leitfaden Cyber-Sicherheits-Check OT

Ein Leitfaden zur Durchführung von Cyber-Sicherheits-Checks der operativen Technologie (CSC-OT) in der Industrie und Automatisierungstechnik

ISACA Germany Chapter

dpunkt.verlag

Herausgeber:
ISACA Germany Chapter e. V.
Storkower Straße 158
D-10407 Berlin

www.isaca.de
info@isaca.de

Autoren und Beteiligte:

- Martin Ennenbach
- Sebastian Fritsch
- Markus M. Lörsch
- Markus J Neuhaus
- Dirk Schugardt
- Christian Schwartz
- Andreas Teuscher
- Gregor Wittkowski
- Peter Böck
- Jordan Rahlwes
- Michael Krammel
- Mike Hofstetter
- Volker Reers
- Reinhard Erich Voglmaier
- Stefan Ahne
- Thomas Klir
- Markus Ruppel
- Detlef Hösterey
- Peter Loos
- Wolfgang Stadler
- Philipp Fath
- Erik Gremeyer
- Daniel Kastner
- Markus Müller
- Sven Super
- Alexander Junkermann
- Matthias Goeken

Die Inhalte dieses Leitfadens wurden von Mitgliedern des ISACA Germany Chapter e. V. in Kooperation mit dem BSI erarbeitet und sind sorgfältig recherchiert. Trotz größtmöglicher Sorgfalt erhebt die vorliegende Publikation keinen Anspruch auf Vollständigkeit. Sie spiegelt die Auffassung des ISACA Germany Chapter wider. ISACA Germany Chapter e. V. übernimmt keine Haftung für den Inhalt.

Stand: September 2021 (Final nach Review und Überarbeitung durch ISACA-Fachgruppe Cyber Security)

Leitfaden
CYBER-SICHERHEITS-CHECK OT

Ein Leitfaden zur Durchführung von Cyber-Sicherheits-Checks der operativen Technologie (CSC-OT) in der Industrie und Automatisierungstechnik

ISACA
Germany Chapter

Allianz für Cyber-Sicherheit

Mit der 2012 gegründeten Allianz für Cyber-Sicherheit (ACS) verfolgt das Bundesamt für Sicherheit in der Informationstechnik (BSI) das Ziel, die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyber-Angriffen zu stärken. Stand März 2021 gehören dieser Initiative 4772 Teilnehmer, 152 Partner und 100 Multiplikatoren an, die so ihren Beitrag für mehr Cyber-Sicherheit am Wirtschaftsstandort Deutschland leisten.

Das ISACA Germany Chapter e. V. (die Fachgruppe Cyber Security) hat mit dem im Februar 2020 veröffentlichten Leitfaden Cyber-Sicherheits-Check V2 einen Multiplikatoren-Beitrag zur Erhöhung der klassischen Office-IT erstellt. In Ergänzung dazu wurde der gemeinsam mit dem BSI entwickelte Zertifikatskurs »Cyber Security Practitioner« durch das ISACA Germany Chapter e. V. weiterentwickelt.

Bestätigt durch die positiven Anwendererfahrungen bei der Verwendung des Leitfadens Cyber-Sicherheits-Check V2 hat sich das ISACA Germany Chapter e. V. dazu entschlossen, einen Leitfaden Cyber-Sicherheits-Check für operative Technologie (CSC-OT) zu entwickeln. Der Leitfaden CSC-OT richtet sich an Verantwortliche und Prüfer, die über die sechsstufigen Vorgehensmodelle das operative Sicherheitsniveau der Produktions- und Prozessanlagen bestimmen können.

Vorwort

Zentralverband Elektrotechnik- und Elektroindustrie e. V. (ZVEI)

Die Bedrohung durch Cyber-Angriffe nimmt seit Jahren zu. Gleichzeitig richten sich Angriffe zunehmend nicht nur auf die klassische Informationstechnologie (IT), sondern auch die operative Technologie (OT) wird Opfer von Attacken und Ransomware.

Mit dem Leitfaden Cyber-Sicherheits-Check, der bereits in einer zweiten Version vorliegt, wurde schon ein sehr guter Einstieg geschaffen, sich mit der Cyber-Sicherheit der IT von Unternehmen und Behörden auseinanderzusetzen. Dieser bietet einen wichtigen Beitrag für das Thema und die Awareness-Steigerung.

Mit dem neuen Leitfaden »Cyber-Sicherheits-Check OT« wird in einem nächsten Schritt eine zugängliche Auseinandersetzung mit Security in der OT ermöglicht. Die voranschreitende Vernetzung zwischen IT und OT und die damit schwindende Abgrenzung zwischen den Bereichen erhöhen die Herausforderungen weiter. Für die Mitgliedsunternehmen des ZVEI nimmt Cyber-Sicherheit im Betrieb eine immer wichtiger werdende Bedeutung ein. Zunehmend bringen Angriffe auch die Abläufe auf dem Shop Floor in Gefahr, wo Störungen und Stillstände noch größere Auswirkungen haben und somit höhere Schadenssummen verursachen können. Hinzu kommt, dass sich eine Produktion häufig nicht schnell »neu aufsetzen« lässt und eine Behebung entsprechend aufwendiger ist.

Viele ZVEI-Mitglieder haben ihre Expertise in die Erstellung des neuen Leitfadens eingebracht, der insbesondere kleinen und mittleren Unternehmen einen erheblichen Mehrwert bietet. Nur durch einen stetigen Informations- und Erfahrungsaustausch mit Netzwerken, wie der Allianz für Cyber-Sicherheit (ACS), Behörden und Verbänden, wie dem ZVEI, kann das gemeinsame Ziel einer cyber-resilienten Industrie erreicht werden.

»Das Resilienz-Niveau muss sowohl in der IT als auch der OT an die steigende Bedrohungslage angepasst werden. Die Verantwortlichen müssen sich diesem Wettlauf stellen und ihre Kenntnisse kontinuierlich verbessern. Die ISACA-Leitfäden bieten hierfür einen sehr wichtigen Beitrag.«

Dr. Wolfgang Weber
Vorsitzender der Geschäftsführung
ZVEI – Zentralverband Elektrotechnik- und Elektronikindustrie e. V.

Verband Deutscher Maschinen- und Anlagenbau e. V. (VDMA)

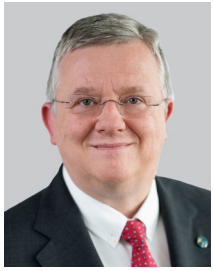
Die Abhängigkeiten in den globalen Lieferketten von funktionierenden IT/OT-Systemen sind eine der zentralen Herausforderungen für die vernetzte Wirtschaft und Gesellschaft. Erfolgreiche Cyber-Angriffe auf kritische Infrastrukturen und deren Zulieferer sind nicht mehr nur Einzelfälle. Die Zielgenauigkeit der Angreifer auf die mittelständische Industrie hat zugenommen, während das Risikobewusstsein und die Investitionsbereitschaft in Cyber-Abwehr oft nur unzureichend Schritt halten.

Insbesondere für den Maschinen- und Anlagenbau in seiner Rolle als Integrator vernetzter Systeme und Funktionen ist eine abgestimmte Vorgehensweise für eine dauerhaft zuverlässige Abwehr von Cyber-Angriffen notwendig. Nur in einer vertrauensvollen Zusammenarbeit zwischen Betreiber, Maschinenbauer, Komponentenlieferant und Dienstleister ist es möglich, Produktionssysteme und Industrieanlagen über den gesamten Investitionszeitraum zu schützen.

Für den Bereich der IT bietet der ISACA-Leitfaden Cyber-Sicherheits-Check mittelständischen Unternehmen bereits eine gute Grundlage. Die Risiken und deren Abwehr enden jedoch nicht an der Werkshalle. Daher begrüßt der VDMA die Erarbeitung einer abgestimmten Vorgehensweise für die Industrial Security.

Hierzu tauschen sich im VDMA-Netzwerk Fachleute aus Produktion, Softwareentwicklung und Cyber Security bereits seit knapp 10 Jahren regelmäßig zum Themenfeld OT/Industrial Security aus. Im Zentrum steht dabei die Frage, wie man mit dem Thema OT im eigenen Unternehmen startet, wo die Risiken liegen und welche Maßnahmen geeignet sind. Ziel muss sein, sich auf den Ernstfall angemessen vorzubereiten.

Wir bedanken uns im Namen des Maschinen- und Anlagenbaus bei den beteiligten Expertinnen und Experten für die Erstellung des Leitfadens, den interessierten Leserinnen und Lesern wünschen wir eine aufschlussreiche Lektüre.



»Cyber Security ist kein Sprint, es ist ein Marathon auf einer sich stetig wandelnden Strecke. Ein angemessener und dauerhafter Schutz von Produktionssystemen ist nur gemeinsam möglich, einen dafür geeigneten Einstieg für mittelständische Unternehmen stellen die Leitfäden der ISACA dar.«

Thilo Brodtmann
Hauptgeschäftsführer
Verband Deutscher Maschinen- und Anlagenbau e. V.

Bundesamt für Sicherheit in der Informationstechnik

Die Digitalisierung prägt uns Tag für Tag: Ein Büro ohne IT ist schon kaum mehr vorstellbar. Die weiter fortschreitende Automatisierung und Vernetzung macht auch vor Produktionshallen und den Maschinen und Anlagen nicht halt. Auch hier eröffnen sich neue Potenziale für Projekte, Produktionssysteme und Geschäftsmodelle von morgen – etwa durch die Entwicklungen um »Industrie 4.0«. Die technologische Entwicklung erlaubt keine Pause und verlangt Entscheidern, Administratoren, Entwicklern, Ingenieuren oder auch allen Mitarbeitern vieles ab. Getrieben von dieser rasanten Geschwindigkeit dürfen Sicherheitsüberlegungen aber nicht vernachlässigt werden, schließlich tragen die Steuerungssysteme an vielen Stellen einen erheblichen Anteil zu unser aller Leben bei – wie ein Blick auf die kritischen Infrastrukturen zeigt. Zukünftig wird diese Abhängigkeit durch die fortschreitende Digitalisierung weiter zunehmen.

Welche Tragweite Cyber-Angriffe haben können, zeigte sich in den letzten Jahren durch die Vielzahl an Produktionsunterbrechungen und -störungen in kleinen und großen Betrieben. Auch der BSI-Bericht »Die Lage der IT-Sicherheit in Deutschland 2020« stellt ein hohes Gefährdungspotenzial für Privatanwender, Unternehmen und Behörden fest. Diese Bedrohungen entstehen durch immer professionellere Täter. Die Liste der Betroffenen ist lang, in vielen Fällen kam es zu massiven Schäden – in manchen Fällen sogar zur Geschäftsaufgabe. Es ist davon auszugehen, dass auch Produktionssysteme zunehmend in den Fokus von Kriminellen rücken werden.

Vor diesem Hintergrund muss ein fundiertes Risikomanagement heute nicht nur zum Standardrepertoire der Unternehmensführung gehören, sondern auch Cyber-Bedrohungen und Sicherheitsmaßnamen umfassen. Dabei reicht ein alleiniger Fokus auf die IT nicht aus, sondern muss auch Steuerungs- und Automatisierungssysteme (OT) in ihrer Gesamtheit adressieren.

ISACA und das BSI, die Cyber-Sicherheitsbehörde des Bundes, arbeiten bereits seit 2014 in enger Kooperation, um das Bewusstsein für Cyber-Sicherheit bei den Verantwortlichen sowohl in der IT als auch in der OT zu schärfen und praxistaugliche Handreichungen zur Bestimmung des Status quo zu entwickeln. Denn Digitalisierung und Cyber-Sicherheit gehören untrennbar zusammen.

Mit dem Cyber-Sicherheits-Check der operativen Technologie (CSC-OT) tragen ISACA und BSI nun dem schnellen Wandel in der Cyber-Welt und den wachsenden Anforderungen zum Schutz der Produktionssysteme Rechnung. Gleichzeitig wurde der IT-Grundschutz wesentlich überarbeitet und ist in die Maßnahmenziele mit eingeflossen.

»Ich freue mich, dass Sie sich dieses Themas annehmen, und wünsche mir, dass wir Sie mit diesem Leitfaden bestmöglich bei der Optimierung Ihrer Cyber-Sicherheitsmaßnahmen unterstützen können.«

Arne Schönbohm
Präsident
Bundesamt für Sicherheit in der Informationstechnik (BSI)

International Data Spaces Association e. V. (IDSA)

In fünf Jahren wird die EU-Strategie für Daten vollständig umgesetzt sein und Einzelpersonen und Organisationen werden die Kontrolle über ihre Daten zurückgewonnen haben. Grundlage für diese Vision ist das Konzept der Datenräume (»Data Spaces«) – geschützte Umgebungen, in denen die Teilnehmer Daten frei austauschen können, indem sie sich an ein festes Regelwerk halten, das Datensouveränität ermöglicht und Transparenz und Fairness garantiert. Datenräume sind das »Level Playing Field« der europäischen Datenstrategie: Sie ermöglichen Interoperabilität und kombinieren alle Arten von Datenendpunkten – unzählige Quellen und Senken, bestehend aus smarten Objekten, Datenmarktplätzen, Cloud-Plattformen, Daten von Einzelpersonen, von offenen Datenquellen, von Datenbanken. Datenräume können »Data Sovereignty by Design« bieten – dies ist ein großer Wert an sich und der Wegbereiter für die Datenökonomie.

Datensouveränität setzt voraus, dass Daten auf jeder Stufe der Datenwertschöpfungskette mit klar definierten Nutzungsrechten versehen sind. Dies bedarf einer technischen Infrastruktur und schließt vertragliche Regelungen ein: Datenverknüpfung oder -analyse kann unterbunden oder ermöglicht werden, Dritten kann der Zugriff auf Daten verboten oder erlaubt sein. Um Datenräume gegen Angriffe aus dem Cyber-Raum angemessen zu schützen, sind technische und organisatorische Maßnahmen notwendig.

Die International Data Spaces Association (IDSA) als gemeinnützige Organisation mit über 130 Unternehmen aus 22 Ländern definiert dafür eine Referenzarchitektur und formale Spezifikationen, die in die Architektur von GAIA-X und in viele Datenräume europäischen Zuschnitts eingeflossen sind.

Insbesondere fundierte und pragmatisch zu nutzende Maßnahmen zur Cyber-Sicherheit, die in der Breite von Unternehmen angenommen werden, führen zu dem Entstehen von Datenräumen mit Tausenden von Teilnehmern als wesentlichem Bestandteil der nationalen Wirtschaft und des europäischen Binnenmarkts – und nur so lassen sich die großen Visionen der europäischen Datenstrategie als Zeitenwende in der Datenökonomie umsetzen.

»Wir brauchen das Engagement der gesamten Wirtschaft, belastbare Standards und unternehmerisches Denken allerorts, um Europa durch die smarte Nutzung von Industriedaten einen neuen Wettbewerbsvorsprung zu sichern.«

Lars Nagel
CEO
International Data Spaces Association

ISACA Germany Chapter e. V.

Das ISACA Germany Chapter e. V. ist der deutsche Zweig des weltweit führenden Berufsverbandes der IT-Revisoren, IT-Sicherheitsmanager und IT-Governance-Beauftragten. Der Verein wurde 1986 gegründet und ist mit über 3.200 Mitgliedern Teil des internationalen Verbandes ISACA, dem weltweit mehr als 140.000 Know-how-Träger in über 180 Ländern der Welt angehören. Zweck des Vereins ist es, durch Diskussion und Informationsaustausch zwischen den Mitgliedern und Interessenten das Verständnis der Probleme auf dem Gebiet der IT-Revision, IT-Sicherheit, Cyber Security sowie IT-Governance zu fördern und diese Erfahrungen durch Publikationen und Seminare allen Mitgliedern und Interessenten zur Kenntnis zu bringen.

Der Leitfaden Cyber-Sicherheits-Check für operative Technologie (CSC-OT) ist in Kooperation mit unseren Partnern und den Mitgliedern der Fachgruppe Cyber Security des ISACA Germany Chapter entstanden. Ich möchte mich ausdrücklich für die eingebrachte Expertise der operativen IT-Sicherheit bedanken, da diese Disziplin neben der Informationstechnologie weiteres Wissen im Bereich Produktions- und Prozessanlagen voraussetzt.

Der CSC-OT greift somit die Realität auf, dass die Automatisierung heute einen so hohen Grad der Vernetzung erreicht hat, dass Produktion und Steuerung ohne sie nicht mehr vorstellbar ist. Die bisherigen Mittel der Abschottung von sensitiven kritischen Infrastrukturen und die Kontrolle der Datenströme stößt jedoch immer mehr an ihre Grenzen. Die künftigen Herausforderungen im Hinblick auf die neuen Anforderungen in einer noch höher vernetzten Industrie-4.0-Umgebung setzen eine vertrauensvolle Zusammenarbeit voraus.

»Die Sicherheit der Informations- und Kommunikationssysteme ist ein integraler Bestandteil moderner Produktion, denn ohne Sicherheit keine Industrie 4.0 und auch kein Vertrauen von Kunden.«

Andreas Teuscher
Leiter der Fachgruppe Cyber Security
ISACA Germany Chapter e. V.

Inhaltsverzeichnis

1 Einleitung

Im aktuellen Berichtszeitraum (2020) setzte sich der Trend zu gezielten Angriffen auf komplette Netzwerke von Unternehmen oder anderen Institutionen fort.

So wurden Automobilhersteller und ihre Zulieferer, verschiedene Flughäfen oder Fluggesellschaften, aber auch weniger bekannte Unternehmen mit hohen Umsätzen angegriffen. Auch kleinere Betriebe wurden angegriffen, die sich durch Alleinstellungsmerkmale, wie zum Beispiel die Produktion spezieller Komponenten im Maschinenbau, auszeichnen oder schlechte Schutzmechanismen aufwiesen.[1]

1.1 Motivation und Hintergrund

Cyber-Sicherheit ist heutzutage auch im Zuge von Digitalisierung und Industrie 4.0 in aller Munde.

Das Allianz Risk Barometer 2020[2] nennt Cyber-Vorfälle als wichtigstes Geschäftsrisiko für Unternehmen weltweit, auf Platz zwei folgen Betriebsunterbrechungen, z. B. durch Ausfälle in digitalen Lieferketten. Das Weltwirtschaftsforum stuft Cyber-Vorfälle ebenfalls als eines der größten globalen Risiken ein. Trotzdem scheinen viele Organisationen noch verhältnismäßig arglos zu sein.

Jedoch darf die Verneinung der Frage: »Bin ich überhaupt ein Angriffsziel?« auf keinen Fall zum Anlass genommen werden, sich nicht zu schützen. Vorfälle ereignen sich häufig als Kollateralschaden einer ungerichteten Malwareattacke (Petya, WannaCry, die Hacker-Gruppe »REvil«). Über 230.000 Computer in über 150 Ländern waren infiziert (bei Petya bzw. WannaCry). Deutsche Unternehmen wie Beiersdorf und die Deutsche Bahn, die dänische Reederei Maersk, der russische Ölproduzent ROSNEFT, der amerikanische Pharmakonzern Merck Sharp & Dohme und viele weitere waren davon betroffen.

1. Die Lage der IT-Sicherheit in Deutschland 2020 | Gefährdungslage, *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.html*.
2. *https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2020-de.html*

Häufig wird dabei vor allem an Technik und insbesondere an Informationstechnologie (IT) gedacht. Ein sehr wichtiges Feld der Cyber-Sicherheit sind jedoch auch Produktions- und Prozessanlagen, die von industriellen Steuerungssystemen kontrolliert werden, der sogenannten operativen Technologie (OT, engl. Operational Technology).

Zu zweifelhaftem Ruhm brachte es im Jahr 2010 der Computerwurm Stuxnet, der speziell zum Angriff auf SCADA-Systeme des Herstellers Siemens entwickelt wurde. Dabei erfolgte eine Manipulation von Frequenzumrichtern, die beispielsweise zur Steuerung der Geschwindigkeit von Motoren dienen. Mutmaßlich war Stuxnet zur Sabotage des iranischen Atomprogramms gedacht, bei dem er die entsprechenden Leittechniken infizierte und störte. Obwohl dieser Angriff mutmaßlich auf staatliche Stellen zurückzuführen war, zeigt er jedoch drastisch die technischen Eingriffsmöglichkeiten in die Steuerungssysteme von Industrieanlagen. Weitere Schadsoftware von Industroyer (2016) über Triton (2017) hat die permanente Gefährdung von OT-Systemen/Industrial Control-Systemen (ICS) sichtbar unter Beweis gestellt. Sicherheitsvorfälle in ICS-Umgebungen sind häufiger geworden (siehe [SANS-Survey]) und die Angriffsvektoren haben sich in dieser relativ kurzen Zeit rasant weiterentwickelt. Doch trotz prominenter Sicherheitsvorfälle und eines verbesserten Informationsaustauschs existieren noch Barrieren zwischen den OT-Experten und den Fachleuten für Cyber-Sicherheit in der traditionellen Office-IT. Dieser Leitfaden soll eine Brücke bilden und somit Hindernisse für die Fortentwicklung der Cyber-Sicherheit von OT-Systemen, vor allem in Industrie-4.0-Umgebungen, abbauen.

Aufgrund der technologischen Entwicklung, der Risikolage und der gesetzlichen Anforderungen sind Betreiber von Prozessanlagen unmittelbar mit dem Thema Cyber-Sicherheit konfrontiert und müssen ihre Cyber-Sicherheitsrisiken kennen. Bei den gesetzlichen Anforderungen spielt z. B. das IT-Sicherheitsgesetz eine wesentliche Rolle. Hier sind Betreiber von Anlagen in der Pflicht, ihren Sicherheitsstatus nachzuweisen. Die Anforderungen und die daraus resultierenden Pflichten an Betreiber kritischer Infrastrukturen sollen dafür sorgen, dass deren IT-Systeme höchsten Sicherheitsstandards genügen, da ein Ausfall oder eine Beeinträchtigung der Versorgungsdienstleistungen dramatische Folgen für Wirtschaft, Staat und Gesellschaft in Deutschland hätten. Dieser Leit-

faden dient nicht der Erfüllung der Anforderungen an Betreiber kritischer Infrastrukturen, kann aber ein Grundverständnis schaffen, diese dort, wo notwendig, beim Definieren von IT-Sicherheitsmaßnahmen mit zu betrachten.

1.2 Ziele des Leitfadens

Der Cyber-Sicherheits-Check OT richtet sich an alle Unternehmen, die Automatisierungssysteme einsetzen, zum Beispiel in der Fertigung, Chemie, Arzneimittelherstellung, Wasserversorgung, in Transport und Verkehr sowie dem Gesundheitswesen und der technischen Gebäudeausstattung.

Adressaten sind alle Personen, die für die Sicherheit von Prozess- und Produktionsanlagen verantwortlich oder zuständig sind. Das umfasst Geschäftsführer, Werksleiter, Fertigungs- und Schichtleiter sowie Automatisierungsverantwortliche. Durch eine praxisnahe Sprache und kompakte Darstellung sollen auch Personen angesprochen werden, die keine Experten für Cyber-Sicherheit sind.

Der Begriff Cyber-Sicherheit (engl. Cyber Security) wird in diesem Leitfaden verwendet, um den Schutz vor Gefahren zu beschreiben, die aus dem Internet auf daran angeschlossene Systeme oder Prozesse wirken. Der Begriff klingt technisch und suggeriert eine technische Lösung der Sicherheitsfrage an der Nahtstelle zum Cyber-Raum. In der gelebten Praxis stehen oftmals tatsächlich technische Aspekte im Fokus von Mitarbeitern und Management. Es ist aber wichtig, darauf hinzuweisen, dass es immer eines Zusammenspiels von Technik, Mensch und Organisationen für die Cyber-Sicherheit bedarf.

Mithilfe des Cyber-Sicherheits-Checks OT (CSC-OT) können Unternehmen das aktuelle Niveau der Cyber-Sicherheit ihrer industriellen Steuerungssysteme bestimmen. Das Ziel ist es, Transparenz zu schaffen bezüglich der umgesetzten technischen und organisatorischen Maßnahmen zur Gewährleistung der Cyber-Sicherheit der betrachteten Systeme. Hierbei werden die besonderen Gegebenheiten von industriellen Produktions- und Prozessanlagen berücksichtigt.

Der hier vorgestellte CSC-OT ermöglicht eine Analyse, die den Umsetzungsgrad in Bezug auf die Maßnahmenziele ermittelt (siehe Kapitel 7). Aus dieser lassen sich direkt erste technische und organisatorische Maß-

nahmen identifizieren, um das Cyber-Sicherheitsniveau der OT-Anlagen zu erhöhen. Sie kann aber auch als Startpunkt für eine tiefergehende Analyse dienen, um weitere relevante Branchenstandards, Best Practices und Normen einzubeziehen. Die zugrunde liegenden Maßnahmenziele für die Beurteilung wurden so konzipiert, dass sie bei effektiver Umsetzung die Cyber-Risiken reduzieren.

Die in diesem Leitfaden beschriebene Vorgehensweise setzt voraus, dass alle Beteiligten über Grundkenntnisse zum Thema IT, Netzwerk und Besonderheiten im ICS-Umfeld verfügen. Für Prüfer sind Vorkenntnisse der Standardfamilie IEC 62443 ([IEC 62443-1-1], [IEC 62443-3-3]), der ISO/IEC-27000-Serie (primär [ISO 27001]) oder im IT-Grundschutz [IT-Grundschutz-Kompendium] zwingende Voraussetzung.

2 Cyber-Sicherheit für die operative Technologie (OT)

2.1 OT und industrielle Steuerungssysteme

Operational Technology (OT) als Oberbegriff ist Hardware und Software, die durch direkte Überwachung und/oder Steuerung von Industrieanlagen, Anlagen, Prozessen und Ereignissen Änderungen erkennt oder verursacht[3]. OT-Systeme beinhalten somit alle Formen industrieller Prozesstechnik und ihrer Automatisierungssysteme. Die verwendete Technologie von OT und IT ist zwar vergleichbar, jedoch sind Einsatzbereich und Verwendung unterschiedlich.

Industrielle Steuerungssysteme (Industrial Control Systems) bilden einen Schwerpunkt der OT. Sie automatisieren die Steuerung von Maschinen und Systemen. Hierzu werden Betriebsparameter über Sensoren (z. B. Temperatur, Füllstände, Gewicht) aufgenommen und in der Steuerung zu Befehlen an die Aktorik verarbeitet (Schalter, Stellglieder für z. B. Pumpen, Ventile, Klappen).

OT findet sich auch in Bereichen wie Energie- und Wasserversorgung, Verkehrsleitsysteme und Überwachung, Medizintechnik, Gebäudetechnik bis hin zur privaten Haustechnik (Smart Home). Auch der Bereich »Internet of Things« (IoT) wird von OT beeinflusst. Digitalisierung und Industrie 4.0 sind die aktuellen Schlagwörter, die vor allem auf die zunehmende Verzahnung von IT und OT fokussieren.

Industrielle Steuerungssysteme basieren klassisch auf sogenannten SPS (speicherprogrammierte Steuerungen), die entsprechende Schnittstellen zur Anbindung besitzen und über die die Prozesssignale (Eingaben und Ausgaben) übertragen werden. Als Übertragungstechnologien werden unterschiedliche Varianten genutzt. Während in der Vergangenheit verstärkt serielle Verbindungen oder Bussysteme (z. B. Feldbus) zum Einsatz kamen, sind IP-basierte Netzwerkprotokolle und -verbindungen mittlerweile Standard. Dabei kommen sowohl kabelgebundene Tech-

3. *https://www.gartner.com/en/information-technology/glossary/operational-technology-ot*

nologien zum Einsatz (z. B. Ethernet) als auch kabellose Systeme (z. B. WLAN, Bluetooth, Mobilfunk).

In Prozessanlagen treffen zwei unterschiedliche Informationswelten mit verschiedenen Sichtweisen aufeinander. Neben den beschriebenen Steuerungssystemen kommen ebenso IT-Systeme aus dem Office-Bereich, beispielsweise zur anlagenübergeordneten oder betriebswirtschaftlichen Steuerung, zum Einsatz. Dazu gehören unter anderem ERP-Systeme (Enterprise Resource Planning).

Zwischen diesen unterschiedlichen Informationswelten besteht der Bedarf, Informationen auszutauschen. Die ISA-95-Pyramide (Hierarchien) stellt diese Zusammenhänge in Ebenen strukturiert dar (siehe Abbildung 2–1). Sie besteht aus Modellen und Terminologie, mit denen bestimmt werden kann, welche Informationen zwischen Systemen für Vertrieb, Finanzen und Logistik und Systemen für Produktion, Wartung und Qualität ausgetauscht werden müssen. Die Ebenen 0-2 bilden dabei die Steuerungs- und Leitsysteme ab, die Ebene 3 umfasst die Prozessführung. Zu diesen gehören z. B. Bedienerterminals, Beobachtungs- und Anzeigekomponenten, Programmiergeräte, Entwicklungsarbeitsstationen (Engineering Station oder Engineering Workstation) oder die Datenbanken zur Aufzeichnung der Produktions- und Prozessdaten (Data Historian). Die Ebene 4 repräsentiert die Informationswelt der übergeordneten Betriebsführung mit Schnittstelle zur Automatisierungstechnik.

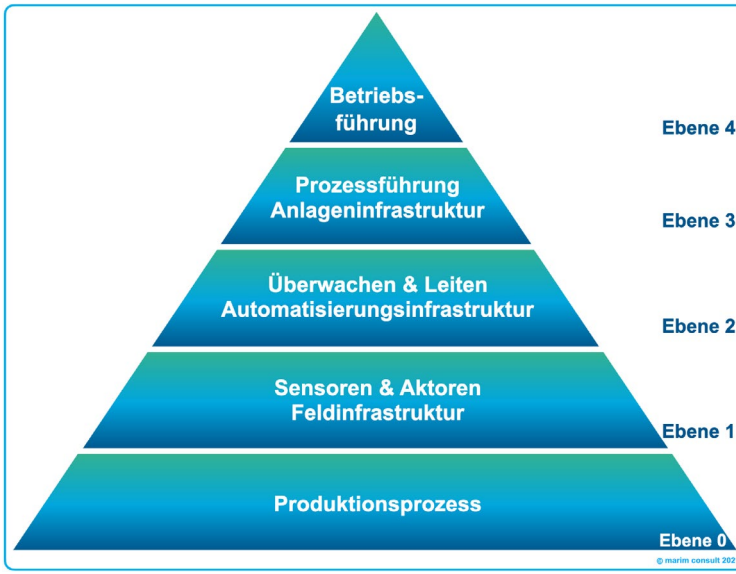


Abb. 2–1 Automatisierungspyramide (Quelle abgeleitet von der ISA-95)

Das Thema Cloud Computing ist nicht in der klassischen Pyramide enthalten, gewinnt aber zunehmend an Bedeutung. Cloud Computing beschreibt die Bereitstellung von IT-Infrastruktur und IT-Leistungen, wie beispielsweise Speicherplatz, Rechenleistung oder Anwendungssoftware, als Service über das Internet.

In der OT setzen sich mittlerweile Komponenten aus der klassischen Office-IT immer mehr durch und finden dort Anwendung. Dies durchzieht fast alle Ebenen der Pyramide. Obwohl die OT und Büro-IT immer stärker zusammenrücken, gibt es jedoch erhebliche Unterschiede. Im Kern geschuldet sind die Unterschiede dem Wesen der OT, das heißt, intelligente Systeme steuern hier physikalische Prozesse. Ein Aspekt ist die Notwendigkeit, dass Teilprozesse in Echtzeit ablaufen müssen. Davon sind insbesondere die Ebenen 1-3 betroffen. Weiterhin ist die Verfügbarkeit bei OT-Systemen die herausragende Anforderung. Dies hat zum Beispiel Einfluss auf die Wartbarkeit (Patchmanagement) dieser Systeme. Wartungsfenster stellen oft ein Problem dar. In der OT ist außer-

dem der Aspekt der Betriebssicherheit (Safety) von zentraler Bedeutung. Hier geht es um den Schutz von Menschen und Umwelt vor physischem Schaden. Dies ist in der Büro-IT weitestgehend ohne Bedeutung. Ein weiterer Unterschied sind die differenzierten Lebenszyklen von OT-Anlagen und IT-Systemen und Komponenten. Während in der Büro-IT die durchschnittliche Nutzungsdauer zwischen drei und fünf Jahren liegt, sind in der OT Lebenszyklen von 20 bis 30 Jahren (geschuldet den zugehörigen Produktionsanlagen) keine Seltenheit.

Dennoch gibt es auch Gemeinsamkeiten zwischen Büro-IT und OT. Auch bei der OT kann man die Cyber-Sicherheit nicht nur durch Technik herstellen, sondern muss organisatorische und personenbezogene Maßnahmen (z. B. bei der Awareness) berücksichtigen. Viele Maßnahmen für Cyber-Sicherheit sind für Büro-IT und OT vom Prinzip her gleich. Sie unterscheiden sich jedoch oft in ihrer inhaltlichen Ausgestaltung und müssen entsprechend angepasst sein.

Hier gibt es entsprechende Leitfäden und Standards, die dazu wichtige Handlungsempfehlungen darstellen und die als Referenzen bei den jeweiligen Maßnahmenzielen mit angegeben sind. Hierzu gehören die IEC 62443 ([IEC 62443-1-1], [IEC62443-3-3]), das ICS-Security-Kompendium des BSI [ICS-Kompendium] und die ISO/IEC 27001 [ISO 27001], die auch in der IT eine zentrale Bedeutung hat, sowie weitere branchenspezifische Empfehlungen und Vorgaben.

2.2 Technische Entwicklung und Industrie 4.0

Betrachtet man die historische Entwicklung der OT, insbesondere im Bereich der industriellen Steuerungssysteme, handelte es sich hierbei ursprünglich um geschlossene Systeme mit proprietärer Technologie. In Verbindung mit dem sehr niedrigen Vernetzungsgrad gab es somit kaum Angriffsvektoren aus dem Cyber-Raum. Aus diesem Grund spielte das Thema Cyber-Sicherheit in der OT keine wesentliche Rolle, sofern die Verfügbarkeit nicht betroffen war. Einfachste Sicherheitsmechanismen, wie man sie in der Büro-IT kennt (zum Beispiel Verschlüsselung, Authentisierung), waren technologisch nicht oder nur rudimentär implementiert.

Die zunehmende Vernetzung und die verstärkte Nutzung von Standardkomponenten und -protokollen (Ethernet und IP anstelle von proprietären BUS-Systemen) führten zu einer Konvergenz von OT- und IT-

Netzen. Standardkomponenten der Office-IT wurden Bestandteil von OT-Netzwerken, die ihrerseits mit der Office-IT Daten austauschen. Hinzu kommt, dass Office-IT-Netzwerke standardmäßig mit dem Internet verbunden sind und OT-Netzwerke zunehmend verbunden werden. Damit sind die noch schwach geschützten OT-Systeme den Bedrohungen aus der Office-IT und dem Cyber-Raum ausgesetzt.

Industrie 4.0 bezeichnet diese Bestrebung zur Digitalisierung im Produktionsumfeld durch Vernetzung von Maschinen und Abläufen in der Industrie mithilfe von Informations- und Kommunikationstechnologie.

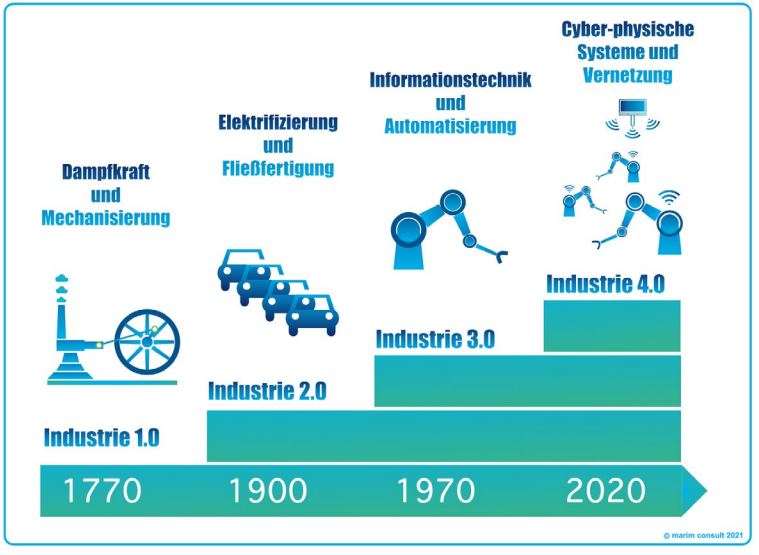


Abb. 2–2 Wandel der Industrietechnologie (Quelle: ISACA-Fachgruppe Cyber Security)

2.3 Risiken und Cyber-Bedrohungen in der OT

Während die Angriffe auf die herkömmliche IT in erster Linie finanzielle und operative Schäden erzeugen, liegt das Risiko beim Angriff auf Prozessanlagen auch in der Safety, d. h. im Bereich des Personen-, Anlagen- und Umweltschutzes. Angreifer, die Zugriff auf das Leitsystem einer Prozessanlage erlangen, können diese zerstören, die Umwelt verunreini-

gen sowie Menschen einen Schaden an Leib und Leben zufügen. Bei der Betrachtung von Cyber-Sicherheit in der OT sind deshalb Safety-Aspekte zu berücksichtigen.

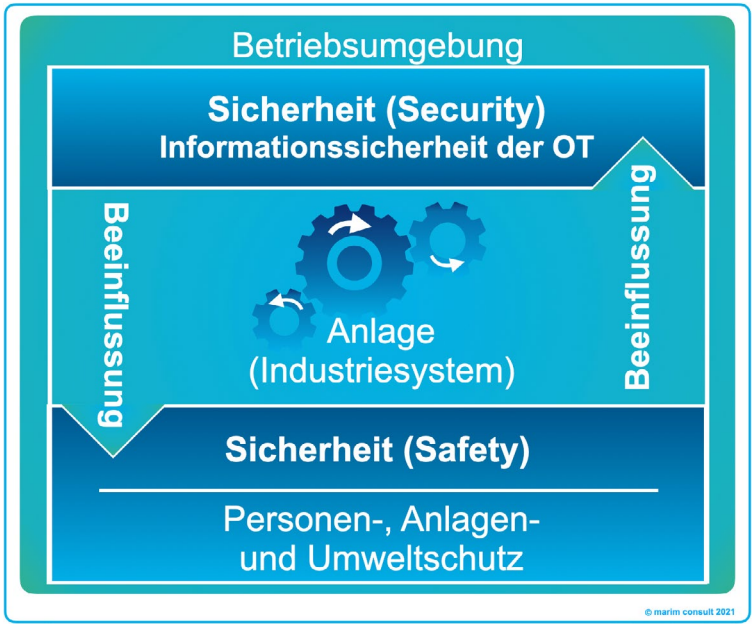


Abb. 2–3 Safety und Security (Quelle: ISACA-Fachgruppe Cyber Security)

Cyber-Sicherheit, Cyber-Angriff, Cyber-Kriminalität und Cyber-Spionage sind längst bekannte Schlagwörter in der Presse und öffentlichen Diskussion. Der Begriff »Cyber« im Kontext der Informationssicherheit erfordert jedoch eine zusätzliche Erklärung, da er oft missverstanden oder zu sehr verallgemeinert wird. Er bezieht sich auf den »Cyber-Raum« als offenen Raum, in dem informationsverarbeitende Systeme aufgestellt und miteinander verbunden sind. Im Hinblick auf diesen Leitfaden umfasst Cyber-Sicherheit die Absicherung der Schnittstellen gegen Bedrohungen aus dem Cyber-Raum zu den informationsverarbeitenden Systemen einer

Institution, insbesondere der »Nahtstelle« zwischen öffentlichem Cyber-Raum und kontrollierten Unternehmensumgebungen.

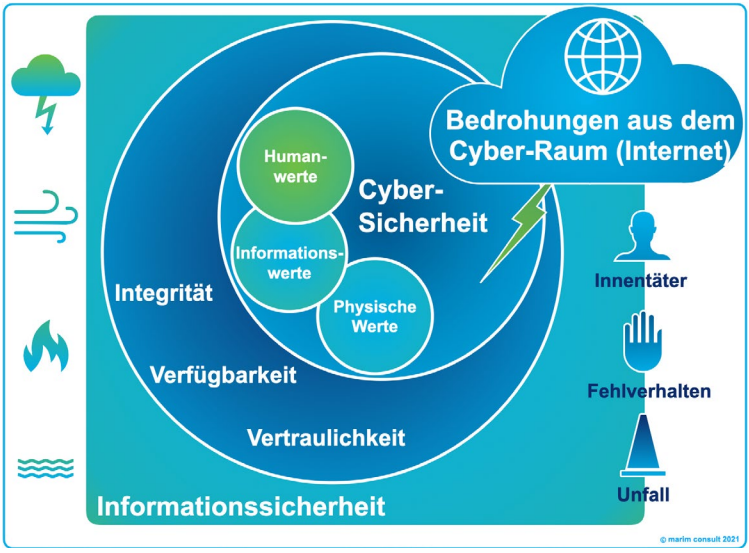


Abb. 2–4 Cyber-Raum und Informationssicherheit (Quelle: ISACA-Fachgruppe Cyber Security)

Bedrohungen aus dem Cyber-Raum (siehe Abbildung 2-4) stellen ein erhebliches Risiko für eine Industrie dar. Die Schäden können immens sein und Unternehmen in ihrer Existenz bedrohen:

- Schaden für die Sicherheit von Personen, Umwelt und Anlagen
- Produktionsausfall oder Fehlproduktion
- Verlust oder Offenlegung von Informationen und geistigem Eigentum (Patente, Konstruktionsdaten etc.)
- Finanzieller Schaden
- Reputationsschaden
- Haftungsansprüche
- Strafen (z. B. wegen Nichtbeachtung gesetzlicher Anforderungen)

Bedrohungen gehen nicht allein von vorsätzlichen oder gezielten Angriffen aus. Erhebliche Schäden treten auch bei Opfern nicht zielgerichteter Angriffe auf, z. B. durch Schadcodes, die per E-Mail übertragen und durch Unwissenheit oder Unachtsamkeit von Mitarbeitern aktiviert werden (Wannacry, Petya, NotPetya etc.).

Prinzipiell unterliegen OT-Anlagen und ihre Steuerungen den gleichen Bedrohungen wie IT-Systeme. Jedoch sind die Risiken und Gegenmaßnahmen aufgrund der Anforderungen einer Industrieumgebung sowie der unterschiedlichen Schadensauswirkungen und Kritikalität anders zu bewerten. Im industriellen Umfeld haben daher viele Cyber-Bedrohungen ein anderes Gewicht. Bestehende Sicherheitsstrukturen der Office-IT ohne Anpassungen zu übernehmen, funktioniert aufgrund der unterschiedlichen Strukturen und Anforderungen nicht.

Das BSI veröffentlicht regelmäßig die Top-10-Bedrohungen und Gegenmaßnahmen für Industrial Control System Security [ACS2]. Die letzte Version wurde im Jahre 2019 veröffentlicht, alle zwei Jahre ist eine Aktualisierung geplant. Zu den zehn identifizierten Bedrohungen werden erstens Problembeschreibung und Ursachen, zweitens mögliche Bedrohungsszenarien und drittens Gegenmaßnahmen aufgezeigt. Diese können, um ein Gefühl für eine Bewertung zu bekommen, unterstützend herangezogen werden. Die Top 10 verstehen sich als Bedrohungsübersicht und erheben keinen Anspruch auf Vollständigkeit.

Top 10 Bedrohungen	Trend seit 2016
Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware	
Infektion mit Schadsoftware über Internet und Intranet	
Menschliches Fehlverhalten und Sabotage	
Kompromittierung von Extranet und Cloud-Komponenten	
Social Engineering und Phishing	
(D)DoS Angriffe	
Internet-verbundene Steuerungskomponenten	
Einbruch über Fernwartungszugänge	
Technisches Fehlverhalten und höhere Gewalt	
Kompromittierung von Smartphones im Produktionsumfeld	

Abb. 2–5 Top-10-Bedrohungen [ACS2]

In der Praxis zeigen sich weitere Bereiche, die zu besonderen Risiken im Bereich von OT und Prozessanlagen führen:

- Teilweise »blindes« Vertrauen in und ungenügende Steuerung von Lieferanten und Dienstleistern
- Fokussierung auf die Hauptleittechnik und Vernachlässigung essenzieller Nebensysteme
- Fehlendes Bewusstsein für Cyber-Sicherheit
- Unzureichende oder veraltete Dokumentation der Anlagen
- Fehlende Rollen und Verantwortlichkeiten
- Fehlende regelmäßige unabhängige Prüfungen
- Fortbetrieb von vernetzten Altsystemen ohne Sicherheitsmaßnahmen
- Fehlende Netzwerküberwachung
- Unsichere Fernwartungszugänge
- Mangelhaftes Test- und Änderungsmanagement

Die Maßnahmenziele in Kapitel 7 beschreiben ganzheitliche Ansätze, um den genannten Bedrohungen entgegenzuwirken.

2.4 Cyber-Sicherheitskonzepte der OT

Wie bereits erläutert, sind die Ansätze und Konzepte zur Cyber-Sicherheit von IT und OT in vielerlei Hinsicht gleich. Die konkrete Ausgestaltung im OT-Umfeld kann sich jedoch erheblich von der IT unterscheiden und erfordert die Berücksichtigung anderer Aspekte.

Diese Besonderheiten adressiert unter anderem besonders gut die international anerkannte und angewandte Normenfamilie IEC 62443. Sie hebt beispielsweise die Bedeutung der Einbeziehung aller Beteiligten beim Neubau, Umbau und Betrieb von Prozessanlagen hervor. Das Zusammenspiel und Rollenverständnis von Hersteller, Integrator und Betreiber ist eine grundlegende Voraussetzung für eine sichere OT-Umgebung.

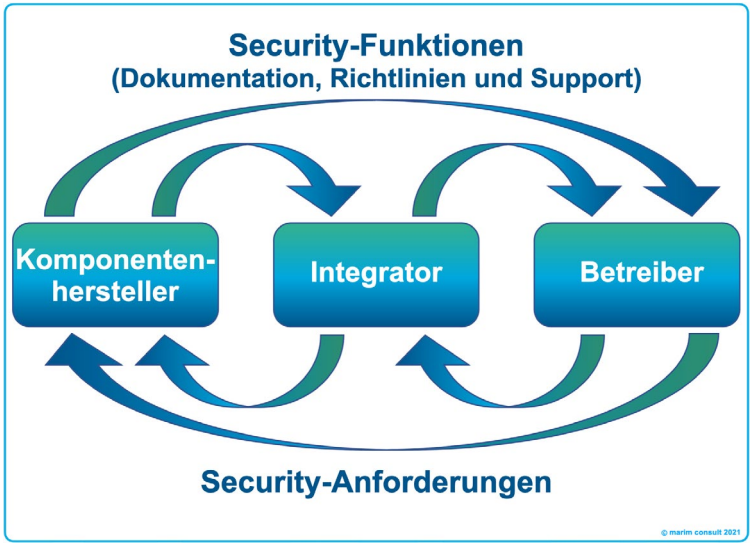


Abb. 2–6 Zusammenspiel der Beteiligten gem. IEC 62443
(Quelle: ISACA-Fachgruppe Cyber Security)

Dabei beschreiben Einzelnormen der IEC 62443 die Security-Anforderungen an die Beteiligten, die in den unterschiedlichen Phasen des Anlagenlebenszyklus, von der Konzepterstellung bis zur Außerbetriebnahme, Anwendung finden.

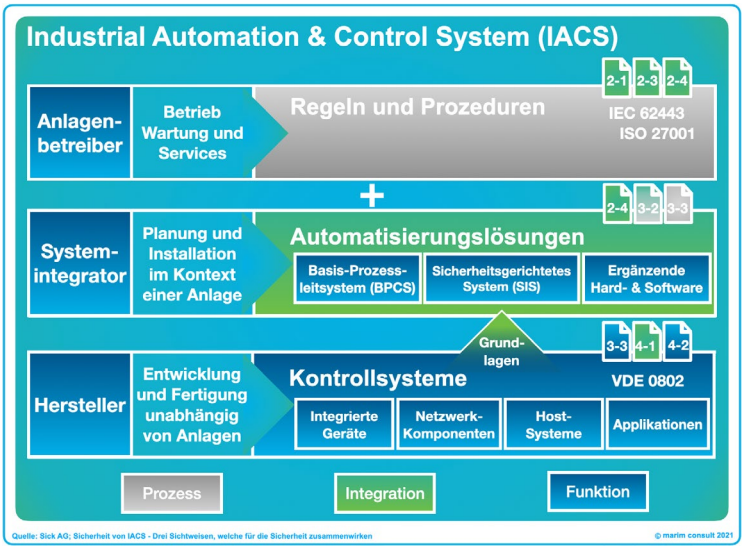


Abb. 2–7 Übersicht der Verantwortlichkeiten gem. IEC 62443 (Quelle: SICK AG, A. Teuscher)[4]

Dieser Leitfaden richtet sich an Betreiber. Anforderungen an Integratoren und Hersteller werden nur indirekt aus Betreibersicht adressiert (Anforderungen an Lieferanten). Direkte Anforderungen an Hersteller werden im Leitfaden nicht betrachtet. Dennoch sollte der Betreiber bei der Auswahl seiner Hersteller deren Konformität zu den Normanforderungen berücksichtigen bzw. einfordern.

Dem Integrator kommt ebenfalls eine besondere Rolle zu, die auch im Leitfaden mitberücksichtigt ist. Dieser plant, implementiert und konfiguriert die Gesamtanlage, indem er die Komponenten der Hersteller

4. Die in Abbildung 2–7 verwendeten Farben gliedern sich wie folgt auf. Grau steht für die Verantwortung der Betriebsprozesse beim Anlagenbetreiber. Grün steht für die Verantwortlichkeiten von Komponenten, Systemen und die Integration in einen sicheren Betrieb. Blau steht für die Funktion, die auch die industrielle Cyber Security beinhalten muss. Dabei ist die Verantwortung und das Zusammenwirken von Hersteller, Systemintegrator und Anlagenbetreiber hervorzuheben.

nach den Vorgaben des Betreibers errichtet. Mit der Qualität seiner Ausführung legt der Integrator auch im Hinblick auf Cyber-Sicherheit einen äußerst wichtigen Grundstein für den sicheren Betrieb der Anlage. Neben guter Implementierung sind dabei insbesondere auch alle Maßnahmen zu bedenken, mit denen der Integrator den Betreiber zu diesem sicheren Betrieb befähigt (z. B. Dokumentation, Training, Patchmanagement und Wartungsvereinbarungen). Hier sind die Betreiber gefordert, durch geeignete Cyber-Sicherheitsspezifikationen und gut gemanagte Qualitätsprüfungen in der Implementierung und Abnahme den Integrator in die Pflicht zu nehmen.

Weiterhin übernimmt der Integrator während der Inbetriebnahme oft die Rolle eines »Quasi-Betreibers«. In manchen Fällen führt er die Anlagen auch in der Produktion. In der Regel ist er aber in der Rolle des Gewährleistenden und oftmals langfristigen Servicepartners mit Durchführung der Wartung der Anlage betraut. Hier entsteht oftmals beim Betreiber der falsche Eindruck, dass damit auch die Verantwortung beim Servicepartner liegt.

Hieraus hervorgehend ist auch das Konzept der gestaffelten Verteidigung über die Wertschöpfungskette für OT-Anlagen grundlegend. Es beruht auf mehreren aufeinander abgestimmten Sicherheitsmaßnahmen der Hersteller, Integratoren und Betreiber. Diese werden durch mehrere Schichten umgesetzt. Der Angreifer muss deshalb mehrere Verteidigungslinien überwinden, um erfolgreich zu sein. Für bestmöglichen Schutz sollten daher zwischen den Beteiligten abgestimmte Maßnahmen in den Bereichen Komponentensicherheit, Planung und Prozesse umgesetzt sein.

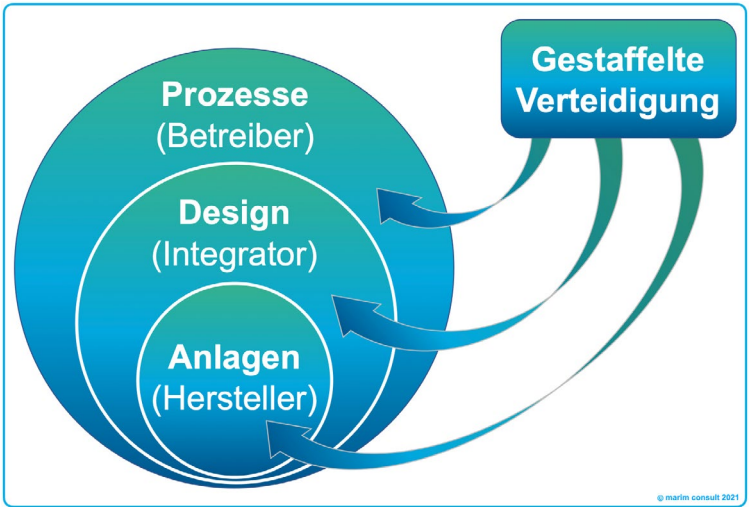


Abb. 2–8 Verantwortungsbereiche der Beteiligten (Quelle: ISACA-Fachgruppe Cyber Security)

Zusammengefasst ist die primäre Aufgabe der Hersteller die Entwicklung und Bereitstellung sicherer Komponenten (Security by Design, vgl. Kap. 7, Maßnahmenziele C und D). Durch die sichere Entwicklung wird bereits ein wesentlicher Grundstein gelegt. In der Planungsphase besteht die Herausforderung darin, durch die Auswahl sicherer Komponenten ein sicheres System zu entwickeln. Der Betreiber muss seine Prozesse so ausrichten, dass eine ganzheitliche Umsetzung der Sicherheitsanforderungen gewährleistet wird. Eine gute Basis dafür bilden die »Grundlegenden Anforderungen (Foundational Requirements)« der IEC 62443.

Besonders hervorzuheben ist für die OT eine sinnvolle, den Anforderungen und Risiken Rechnung tragende Unterteilung von Systemen, die die IEC 62443 durch das Konzept der »Zones & Conduits« aufzeigt.

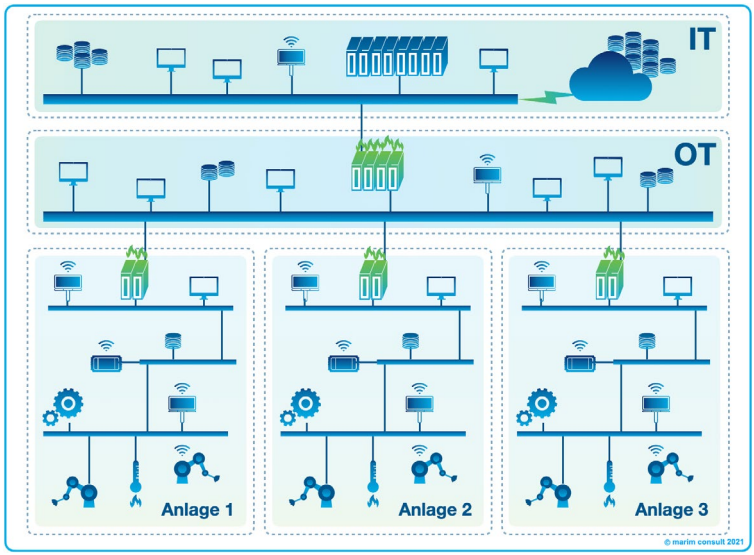


Abb. 2–9 Zones & Conduits: das Zellschutzkonzept (Quelle: ISACA-Fachgruppe Cyber Security)

Das Zellschutzkonzept ist mit dem Konzept der Segmentierung Teil der tiefengestaffelten Verteidigung. Durch geeignete Segmentierung der Netzwerkinfrastruktur sind die verschiedenen Ebenen (Feldebene bis zur Produktionsführung) voneinander getrennt angeordnet und durch geeignete Schutzmechanismen (Firewalls, Übergänge, Conduits) abgesichert (vgl. Maßnahmenziele A). Eine potenzielle Cyber-Attacke aus dem Internet müsste ggf. mehrere Zonen überwinden und Conduits missbräuchlich nutzen, um kritische Bereiche zu erreichen. Darüber hinaus können die einzelnen Zonen getrennte Sicherheitsbereiche darstellen, sodass potenzielle Angriffe auf eine Zone sich nicht ungehindert auf andere ausbreiten können (vergleichbar zu Brandabschnitten in einem Brandschutzkonzept). Die Planung und der Aufbau eines geeigneten Zellschutzkonzepts innerhalb der Anlage ist wesentliche Aufgabe in der Designphase und liegt somit im Zuständigkeitsbereich des Integrators. Zwischen den Anlagen und in der OT ist es Aufgabe des Betreibers und der Integratoren. Die

Maßnahmenziele sind mit einer Referenzangabe zu den grundlegenden Anforderungen der IEC 62443 versehen. Weitere Maßnahmen referenzieren auf die ISO/IEC 27001 als Standardwerk zur Beschreibung eines Informationssicherheitsmanagementsystems (ISMS) und auf das BSI IT-Grundschutz-Kompendium. Ein ISMS beschreibt einen systematischen ganzheitlichen und auf Risikomanagement beruhenden Ansatz zur Organisation und Benennung der Kernmaßnahmen (Anhang A) zur Informationssicherheit. Die ISO/IEC 27001 ist somit gleichermaßen im IT- wie im OT-Bereich einsetzbar und empfehlenswert, wobei sich die Ausgestaltung der konkreten Maßnahmen unterscheidet.

3 Grundsätze des Cyber-Sicherheits-Checks OT

Um Vertrauen in eine objektive Beurteilung zu schaffen, müssen folgende Voraussetzungen sowohl durch Einzelpersonen als auch durch Unternehmen, die Dienstleistungen im Bereich der Cyber-Sicherheit erbringen, eingehalten werden:

- Eine formale Beauftragung des CSC-OT durch die Institution (siehe dazu ISACA IT-Prüfungsstandard 1001 – Audit Charter [ISACA1])
- Unabhängigkeit (siehe dazu ISACA IT-Prüfungsstandard 1002 – Organisatorische Unabhängigkeit und 1004 – Persönliche Unabhängigkeit [ISACA1])
- Rechtschaffenheit und Vertraulichkeit (siehe dazu ISACA IT-Prüfungsstandard 1005 – Berufsübliche Sorgfalt [ISACA1])
- Fachkompetenz (siehe dazu ISACA IT-Prüfungsstandard 1006 – Expertise [ISACA1])
- Nachweise und Nachvollziehbarkeit (siehe dazu ISACA IT-Prüfungsstandard 1205 – Nachweise [ISACA1])
- Objektivität und Sorgfalt (siehe dazu ISACA IT-Prüfungsstandards 1207 – Unregelmäßigkeiten und gesetzeswidrige Handlungen und 1204 – Wesentlichkeit [ISACA1])
- Sachliche Darstellung (siehe dazu ISACA IT-Prüfungsstandard 1401 – Berichterstattung [ISACA1])

Bei der Planung und Durchführung von Assessments im Bereich OT und industrieller Anlagen ist besonders darauf zu achten, dass die Durchführenden neben den erforderlichen Fachkenntnissen in der IT-Sicherheit auch über fundierte praktische Erfahrungen mit industriellen Steuerungssystemen (ICS), Anlagen sowie den technischen und organisatorischen Prozessen verfügen.

Grundvoraussetzung für jede Beurteilung im Rahmen des CSC-OT ist ein uneingeschränktes Informations- und Einsichtnahmerecht. Dies bedeutet, dass dem Beurteiler keine Informationen vorenthalten werden dürfen. Hierzu gehört auch die Einsichtnahme in sensible oder geheim gehaltene Informationen, die den Betrieb der OT-Anlagen, das Informationssicherheitsmanagement sowie den IT-Betrieb betreffen, sofern der Beurteiler ein entsprechend berechtigtes Interesse glaubhaft machen kann. Durch eine Vertraulichkeitserklärung zwischen dem Beurteiler und der Institution sollte hierzu formale Klarheit geschaffen werden.

Die Maßnahmen des CSC-OT wurden auf der Grundlage verschiedener Cyber-Sicherheitsstandards und Kompendien erstellt. Die Maßnahmenübersicht (siehe Kapitel 7) enthält für jede Maßnahme Querverweise auf diese Unterlagen, sodass vertiefende Betrachtungen möglich sind.

Falls zu einzelnen Teilen in diesem Dokument des Beurteilungsgegenstands keine Aussagen getroffen werden, sind andere einschlägige Vorschriften, Gesetze, Standards oder Vorgaben von Herstellern oder Berufsverbänden wie dem VDMA oder dem ZVEI zu verwenden. Die Nutzung dieser Regelwerke ist im Beurteilungsbericht zu dokumentieren und zu begründen.

Die Vor-Ort-Beurteilung kann sowohl von einem Beurteiler allein als auch in einem Team von mehreren Personen durchgeführt werden. Hier ist darauf zu achten, dass ausreichend Fachwissen vorhanden ist, um die spezifischen Cyber-Sicherheitsanforderungen der OT-Anlage sowie ggf. deren Komponenten ausreichend beurteilen zu können.

Grundsätzlich sollte bereits bei der Planung eines CSC-OT beachtet werden, dass der laufende Betrieb in der Institution durch die Beurteilung nicht wesentlich gestört wird. Der Beurteiler greift niemals selbst aktiv in Systeme ein und erteilt auch keine Handlungsanweisungen zu Änderungen an IT-Systemen, Infrastrukturen, Dokumenten oder organisatorischen Abläufen. Er benötigt, sofern notwendig, jeweils ausschließlich lesenden Zugriff.

4 Durchführung des Cyber-Sicherheits-Checks OT

4.1 Beurteilungsgegenstand

Gegenstand eines CSC-OT ist grundsätzlich der gesamte Betriebsbereich. Der CSC-OT legt seinen Fokus auf die Systeme der Level 0 bis 3 (Prozessführung und seine Netzwerke inklusive Feldbusse und Ein-/Ausgabebaugruppen). Dies umfasst die eigentlichen OT-Anlagen, aber auch maschinennahe Systeme (z. B. MES) sowie deren Anbindungen an die Office-IT, Direktanbindungen an externe Netze sowie an das Internet.

Darüber hinaus sind alle Systeme und Dienste mit physischen, logischen oder funktionalen Schnittstellen im Hinblick auf ihre Bedeutung für den sicheren Anlagenbetrieb zu analysieren. Insofern sind auch Hilfs- und Nebensysteme zu betrachten, auch wenn sie nur mittelbar den sicheren Anlagenbetrieb beeinflussen. Eine Auswahl relevanter Systeme umfasst:

- Heizung/Klima/Lüftung
- Stationsautomatisierung und elektrische Schutztechnik (elektrische Energieversorgung)
- Autarke Steuerungen von Nebenanlagen (z. B. Tanklager, Ver- und Entsorgung)
- Gebäudeautomatisierung
- Online-Überwachungs- und Diagnosesysteme, Prozessdaten-Management und Archivierung
- Engineering und Anlagendokumentation
- Verbundene Systeme (Brandmeldesystem, Videoüberwachung etc.)
- Safety-Systeme
- Externe Services wie Cloud

Sofern wesentliche Systeme, Anlagenteile sowie technische, organisatorische Prozesse von der Beurteilung ausgenommen werden, ist dies als Abgrenzung des Beurteilungsgegenstands im Beurteilungsbericht zu dokumentieren und zu begründen.

4.2 Vorgehensweise

Die Vorgehensweise zur Durchführung eines CSC-OT wird im Folgenden schrittweise erläutert.

4.2.1 Schritt 1 – Auftragserteilung

Anfrage und Beurteilungsgegenstands

Bei der Durchführung eines CSC im Umfeld der OT sind der Umfang und die Komplexität des Beurteilungsgegenstands (nachfolgend Scope genannt) entscheidend für den Aufwand. Um den Aufwand beziffern zu können, muss der Scope herausgearbeitet werden.

Hierzu sind Vertreter verschiedener Parteien zusammenzubringen, beispielsweise:

- Geschäftsführung
- Betriebsleitung
- Werksleitung
- Produktionsleitung
- Leittechnikverantwortliche
- IT-Leitung
- IT-Dienstleister

Es ist festzulegen, welche OT-Komponenten und Netzwerke als Gegenstand des CSC analysiert werden sollen. Hierbei ist darauf zu achten, ein gemeinsames Verständnis zu schaffen, was zu den Komponenten zählt. Der Scope ist zu dokumentieren und durch die Leitungsebene (Geschäftsführung, Werksleitung, Auftraggeber) unter Berücksichtigung der Teilnehmer freizugeben.

So kann das Scoping bereits Bestandteil des Auftrags sein und der zeitliche Rahmen bereits feststehen. Hierbei kann es vorkommen, dass nicht alle zu überprüfenden Bereiche analysiert werden können. Bei sehr komplexen und umfangreichen Umgebungen bietet es sich an, das Scoping im Vorfeld zusätzlich zu beauftragen und durchzuführen.

Auftragserteilung

Um eine umfangreiche und wirksame Beurteilung sicherzustellen, sollte der Auftrag zur Durchführung eines CSC-OT durch die Betriebsleitung oder das Management der betreffenden Organisation erfolgen. Eine rangniedrigere oder gleichgestellte Leitungsebene kann keine Beauftragung für einen gleichgestellten oder übergeordneten Bereich erteilen. Mit der Beauftragung des CSC-OT sollte auch der Beurteilungsgegenstand definiert sein.

Es ist möglich, einen CSC-OT in jedem Stadium des Sicherheitsprozesses einer Organisation zu initiieren. Es müssen daher weder Dokumente zur OT-Sicherheitsorganisation oder zur Organisation existieren, noch muss ein bestimmter Umsetzungsstand von OT-Sicherheitsmaßnahmen erreicht sein.

4.2.2 Schritt 2 – Risikoeinschätzung

Zur Bestimmung des Risikos für die zu beurteilende Institution und den jeweiligen Scope muss vor der Vor-Ort-Beurteilung eine Risikoeinschätzung durchgeführt werden. Hierbei wird mittels Schadenshöhe und Eintrittswahrscheinlichkeit eine Risikokennzahl ermittelt. Darauf basierend können der zu erwartende Zeitaufwand, die Beurteilungstiefe sowie die Wahl der Stichproben bei der Durchführung des CSC risikoorientiert bestimmt werden.

Wurde die Risikoeinschätzung **bereits von der Institution durchgeführt**, kann der Beurteiler diese ohne weitere eigene Aktivitäten übernehmen (soweit Schadenshöhe und Eintrittswahrscheinlichkeit bestimmt worden sind), wenn ihm diese nachvollziehbar und angemessen erscheint.

Sofern die Risikoeinschätzung für die betreffende Institution noch **nicht durchgeführt** wurde, sollte diese erstmalig durch die Institution oder in Kooperation mit dem Beurteiler nach dem nachfolgenden Schema erfolgen.

Startpunkt der Risikoeinschätzung ist die Bestimmung der Schadenshöhe für jedes Schutzziel (Verfügbarkeit, Integrität und Vertraulichkeit) anhand der nachfolgenden Tabelle 4–1.

	Verfügbarkeit	Integrität	Vertraulichkeit
Wert der Daten und Prozesse[5]	gering 0 normal 1 hoch 2 sehr hoch 3	gering 0 normal 1 hoch 2 sehr hoch 3	gering 0 normal 1 hoch 2 sehr hoch 3
Schadenshöhe = Wert je Schutzziel			

Tab. 4–1 Bestimmung der Schadenshöhe

Als Nächstes erfolgt die Bestimmung der Eintrittswahrscheinlichkeit anhand der Tabelle 4–2.

5. Die Schwellenwerte gering, normal, hoch, sehr hoch sind von der Institution selbst nach dem zugrunde liegenden Risiko-Appetit festzulegen.

	Verfügbarkeit	**Integrität**	**Vertraulichkeit**
Abhängigkeit von der OT, IT und Grad der Vernetzung (Attraktivität für Angreifer)	lokal[6] 1 teilweise vernetzt[7] 2 voll vernetzt[8] 3	lokal 1 teilweise vernetzt 2 voll vernetzt 3	lokal 1 teilweise vernetzt 2 voll vernetzt 3
	Verfügbarkeit	**Integrität**	**Vertraulichkeit**
Kompetenz (Wissen) der Angreifer	allgemein[9] 1 moderat[10] 2 fachspezifisch[11] 3	allgemein 1 moderat 2 fachspezifisch 3	allgemein 1 moderat 2 fachspezifisch 3
	Verfügbarkeit	**Integrität**	**Vertraulichkeit**
Angriffe in der Vergangenheit	abgewehrt 1 unbekannt/ erfolgreich 3	abgewehrt 1 unbekannt/ erfolgreich 3	abgewehrt 1 unbekannt/ erfolgreich 3
Eintrittswahrscheinlichkeit = Addition der Werte je Schutzziel			

Tab. 4–2 Bestimmung der Eintrittswahrscheinlichkeit

6. Prozesse IT-gestützt, aber auch manuell durchführbar, nachweislich in einem geschlossenen Netz ohne Internetanbindung.
7. Prozesse IT-gestützt, zeitlich begrenzt, manuell durchführbar, separierte Netze mit kontrolliertem Datenaustausch (Fernwartung) und begrenzter Internetnutzung.
8. Prozesse vollständig IT-gestützt, separierte Netze mit kontrolliertem Datenaustausch (Fernwartung) und Internetnutzung (z. B. E-Mail, Internetrecherche, Einsatz von Cloud-Services, mobile Anwendungen).
9. Der Angreifer verfügt über einfaches Wissen, Ressourcen und Werkzeuge, um unautorisiert auf Daten und Prozesse zuzugreifen und diese ggf. zu verändern oder zu löschen.
10. Der Angreifer verfügt über Wissen in Bezug auf die Organisation, besitzt geeignete Ressourcen und Werkzeuge, um unautorisiert auf Daten und Prozesse zuzugreifen und diese ggf. zu verändern oder zu löschen.
11. Der Angreifer verfügt über spezifisches Wissen in Bezug auf die Organisation, besitzt umfangreiche Ressourcen und zielgerichtete Werkzeuge, um unautorisiert auf Daten und Prozesse zuzugreifen und diese ggf. zu verändern oder zu löschen.

Die Risikokennzahl wird nun pro Schutzziel durch Multiplikation der Schadenshöhe mit der Eintrittswahrscheinlichkeit (Summe der Einzelwerte je Schutzziel) ermittelt.

Formel je Schutzziel (VVI):
(Abhängigkeit + Kompetenz + Angriffe) × Schadenshöhe = Risikokennzahl

Im CSC-OT wird für die Risikoeinschätzung und die weitere Bearbeitung der Maximalwert aus den drei Risikokennzahlen genutzt.

Hieraus ergeben sich die nachfolgenden Risikoeinschätzungen:

normal = 0 – 9
hoch = 10 – 18
sehr hoch = 19 – 27

Die Risikoeinschätzung (normal, hoch, sehr hoch) wird bei der Durchführung des CSC-OT für die Beurteilung der Angemessenheit von zu bewertenden Maßnahmen innerhalb der Vor-Ort-Beurteilung (Schritt 5) und der Berichterstellung (Schritt 6) genutzt.

4.2.3 Schritt 3 – Informationssichtung

Die Informationssichtung dient dem Beurteiler dazu, einen Überblick über die Aufgaben, die Organisation und die Infrastrukturen der OT zu gewinnen. Die Informationssichtung beinhaltet lediglich eine grobe Sichtung der zur Verfügung gestellten Dokumente. Hierbei werden (soweit vorliegend) die Rahmenkonzepte für OT und IT, die Liste der kritischen Prozesse der OT, die Sicherheitsleitlinien für OT und IT, die Sicherheitskonzepte (inklusive Netzplan) für OT und IT sowie die Safety-Konzepte beurteilt.

Idealerweise werden im Vorfeld nachfolgende Informationen zur Verfügung gestellt, um die Vor-Ort-Beurteilung vorzubereiten:

- **Organisation, Prozesse, Personal und Verantwortlichkeiten**
  - Vorgaben zu OT und zur Informationssicherheit (Leitlinie, Standards, Richtlinien)
  - Organigramm und OT sowie Informationssicherheitsorganisation

- **Technische Dokumentation**
  - Struktur des Netzes als physischer und logischer Netzplan (inkl. IP-Netzadressen und Netzmasken, IP-Adressen aller angeschlossenen Netzinterfaces, MAC-Adressen, Computername und Funktionalität der Systeme, (falls vorhanden) DNS-Name, Zonen)
  - Inventar aller in der Anlage beteiligten programmierbaren Komponenten (inkl. Abgrenzung und Schnittstellen zu anderen Systemen)
  - Prozessübersichtsdiagramm (übergeordneter Gesamtprozess, ggf. Teilprozesse)
  - Safety-Konzepte für die Operational Technology

- **Frühere Auditberichte und Risikoanalysen**

Sind keine ausreichenden Informationen vorhanden, wird die Informationssichtung durch Gespräche ergänzt, in denen sich der Beurteiler den erforderlichen Überblick verschaffen kann. Auf Basis der gewonnenen Erkenntnisse bestimmt der Beurteiler risikoorientiert die Stichproben und Schwerpunkte der Beurteilung.

4.2.4 Schritt 4 – Vorbereitung der Vor-Ort-Beurteilung

Zur Vorbereitung der Vor-Ort-Beurteilung sollte ein Ablaufplan unter Einbeziehung der Cyber-Sicherheitsrisikoeinschätzung erstellt werden. Dieser gibt an, welche Inhalte wann beurteilt werden sollen und welche Ansprechpartner (Rollen/Funktionen) hierzu erforderlich sind. Der Ablaufplan ist der betreffenden Institution vorab zu übersenden.

4.2.5 Schritt 5 – Vor-Ort-Beurteilung

Hintergrund aller Bewertungen sind die Maßnahmenziele in Kapitel 7. Die Vor-Ort-Beurteilung selbst beginnt immer mit einem kurzen Eröffnungsgespräch und endet mit einem Abschlussgespräch. Im Eröffnungsgespräch wird den Beteiligten (z. B. Produktionsverantwortliche, Werksleitung) die Vorgehensweise und Zielrichtung des CSC-OT erläutert. Außerdem werden organisatorische Punkte geklärt, wie z. B. Zutrittskontrolle, Besprechungsraum oder etwaige Änderungen zum Ablauf.

Im Rahmen der Vor-Ort-Beurteilung werden Interviews geführt, die Umgebung der OT, insbesondere die Produktions- und IT-Systeme, in Augenschein genommen und evtl. weitere Dokumente gesichtet. Bei der Durchführung der Vor-Ort-Beurteilung sollten die für die jeweiligen Themen zu befragenden Ansprechpartner zur Verfügung stehen. Die zu beurteilenden Stichproben (z. B. Dokumente, Produktions- und IT-Systeme) und die festgestellten Sachverhalte sollten vom Beurteiler ausreichend detailliert dokumentiert werden, um diese Informationen später für die Erstellung des Berichts angemessen verwenden zu können.

Im Abschlussgespräch, an dem auch die Leitungsebene der Institution teilnehmen sollte, wird eine erste allgemeine Einschätzung zum Niveau der Cyber-Sicherheit in der OT-Umgebung der Institution gegeben. Darüber hinaus eröffnet der Beurteiler schwerwiegende Sicherheitsmängel, die die Cyber-Sicherheit der Institution unmittelbar stark gefährden und deshalb zeitnah behandelt werden sollten.

4.2.6 Schritt 6 – Nachbereitung/Berichterstellung

Der CSC-OT wird mit einem Beurteilungsbericht abgeschlossen. Der Bericht gibt einen Überblick zur Cyber-Sicherheit der OT-Umgebung der Institution und enthält neben der Darlegung der Cyber-Sicherheitsrisikoeinschätzung eine Liste der festgestellten Mängel. Zu jedem Maßnahmenziel (siehe Kapitel 7) ist das jeweilige Beurteilungsergebnis zu dokumentieren. Im Bericht werden allgemeine Empfehlungen zur Behandlung der festgestellten Mängel aufgezeigt. Hieraus kann die beurteilte Institution entnehmen, in welchen Bereichen vermehrt Aktivitäten erforderlich sind, um das Cyber-Sicherheitsniveau der OT-Umgebung zu erhöhen. Nähere Informationen zur Erstellung des Berichts finden sich in Abschnitt 4.7 »Erstellung des Beurteilungsberichts«.

4.3 Qualität der Durchführung/Personenzertifikat

Einen CSC-OT kann eine Institution sowohl durch qualifiziertes eigenes Personal als auch durch einen kompetenten Dienstleister durchführen lassen. In beiden Fällen ist jedoch sicherzustellen, dass die Analysten über ausreichendes Fachwissen verfügen (Mindestanforderung Cyber Security Practitioner OT, Cyber Security Practitioner IT oder äquivalente Qualifikation sowie Grundwissen zu OT- und IT-Umgebungen) und die in diesem Leitfaden vorgegebene Herangehensweise genutzt wird.

4.4 Beurteilungsmethoden

Unter »Beurteilungsmethoden« werden alle für die Ermittlung eines Sachverhaltes verwendeten Handlungen verstanden. Während eines CSC-OT können vom Beurteiler u. a. folgende Beurteilungsmethoden genutzt werden:

- Mündliche Befragung (Interview)
- Inaugenscheinnahme von IT-Systemen, Orten, Räumlichkeiten und Gegenständen
- Beobachtung (Wahrnehmungen im Rahmen der Vor-Ort-Beurteilung)
- Dokumentenanalyse (hierzu gehören auch elektronische Daten oder statistische Auswertungen)
- Datenanalyse (z. B. Konfigurationsdateien, Logfiles, Auswertung von Datenbanken etc.)
- Schriftliche Befragung (z. B. Fragebogen)
- Prüfberichte und Zertifizierungen Dritter

Welche dieser Methoden angewendet werden, hängt vom konkreten Sachverhalt ab und ist durch den Beurteiler festzulegen. Dieser hat weiterhin zu beachten, dass in jedem Fall der Grundsatz der Verhältnismäßigkeit eingehalten wird. Für die Ermittlung eines Sachverhaltes können auch mehrere Beurteilungsmethoden kombiniert zur Anwendung kommen. Beachtet werden muss, dass keinesfalls selbst Zugriff auf den Prüfungsgegenstand genommen werden darf.

4.5 Verbindliche Maßnahmenziele

Durch die Etablierung verbindlicher Maßnahmenziele soll sowohl eine gleichbleibend hohe Qualität des CSC-OT als auch eine Vergleichbarkeit der Tätigkeit unterschiedlicher Beurteiler gewährleistet werden.

Die verbindlichen Maßnahmenziele für einen CSC-OT basieren auf den konkret festgestellten kritischsten Sicherheitsmängeln im Umfeld der OT sowie auf den Referenzen zu den »Basismaßnahmen der OT-Cyber-Sicherheit« (siehe Referenztabelle im Anhang).

Die Beurteilungstiefe (Intensität) wird vom Beurteiler je nach Höhe der Cyber-Sicherheitsrisikoeinschätzung risikoorientiert angepasst.

4.6 Bewertungsschema

Werden im Rahmen eines CSC-OT Sicherheitsmängel festgestellt, so hat der Beurteiler spätestens bei der Berichterstellung festzulegen, wie die betreffenden Mängel in ihrer Kritikalität zu bewerten sind.

Sicherheitsmängel sind wie folgt einzuordnen:

»Kein Sicherheitsmangel«

Zum Zeitpunkt der Beurteilung konnte kein Sicherheitsmangel festgestellt werden. Es gibt keine ergänzenden Hinweise.

»Sicherheitsempfehlung«

Auch eine voll umgesetzte Sicherheitsmaßnahme kann um eine Sicherheitsempfehlung ergänzt werden. Durch die Umsetzung der im Sachverhalt beschriebenen Maßnahmenempfehlungen kann die Sicherheit erhöht werden. Verbesserungsvorschläge für die Umsetzung von Maßnahmen, ergänzende Maßnahmen, die sich in der Praxis bewährt haben, oder Kommentare hinsichtlich der Angemessenheit von Maßnahmen können ebenfalls als Sicherheitsempfehlung aufgeführt werden.

»Sicherheitsmangel«

Bei einem »Sicherheitsmangel« liegt eine Sicherheitslücke vor, die mittelfristig behoben werden sollte. Insbesondere die Verfügbarkeit und Integrität, aber auch die Vertraulichkeit der OT- und IT-Systeme wie auch der Informationen kann beeinträchtigt sein.

»Schwerwiegender Sicherheitsmangel«

Ein »schwerwiegender Sicherheitsmangel« ist eine Sicherheitslücke, die umgehend geschlossen werden sollte, da die Verfügbarkeit und/oder die Integrität wie auch die Vertraulichkeit der OT- und IT-Systeme sowie der Informationen stark gefährdet sind und ein erheblicher Schaden zu erwarten ist.

Alle Arten von Sicherheitsmängeln und -empfehlungen sind im Beurteilungsbericht in der Art zu dokumentieren, dass die Bewertung für einen sachkundigen Dritten nachvollziehbar ist.

4.7 Erstellung des Beurteilungsberichts

Der Beurteilungsbericht eines CSC-OT ist dem Produktionsverantwortlichen, der Leitungsebene bzw. dem Auftraggeber schriftlich bekannt zu geben. Eine Entwurfsversion des Berichts sollte vorab übermittelt werden, um zu verifizieren, ob die festgestellten Sachverhalte (nur festgestellte Sachverhalte – ohne Bewertungen und Empfehlungen) sachlich richtig aufgenommen wurden.

Der Beurteilungsbericht umfasst mindestens die folgenden drei Teile:

- Die Rahmendaten, inklusive detaillierter Beschreibung des Beurteilungsgegenstands
- Eine Zusammenfassung für die Leitungsebene (einschließlich Cyber-Sicherheitsrisikoeinschätzung)
- Die Detailbeurteilung (ausführliche Darstellung der festgestellten Mängel, deren Bewertung sowie die abgeleiteten Maßnahmenziele zur Abstellung der Mängel)

Der Beurteilungsbericht ist als Mängelbericht ohne Würdigung positiver Aspekte zu erstellen.

Teil I – Rahmendaten

Dieser Teil enthält die organisatorischen Informationen:

- Beurteilungsgegenstand (Scope)
- Abgrenzung des Beurteilungsgegenstands
- Beurteiler
- Ansprechpartner
- Beurteilungsgrundlagen
- Zeitlicher Ablauf
- Verteiler für den Beurteilungsbericht
- Rahmendaten des Beurteilungsdokuments bzw. der Dokumentenlenkung
  - Dateiname
  - Druckdatum
  - Dokumentenstatus

Teil II – Zusammenfassung für die Leitungsebene

Dieser Teil enthält eine Zusammenfassung für die Leitungsebene. In knapper, verständlicher Form sollten die wesentlichen Mängel und daraus hervorgehende Empfehlungen zusammengefasst werden:

- Zusammenfassung
- Cyber-Sicherheitsrisikoeinschätzung
- Übersicht der Beurteilungsergebnisse für alle Maßnahmenziele

Teil III – Detailbeurteilung

Dieser Teil des Berichts beinhaltet die ausführliche Darstellung der beurteilten Themenfelder, die festgestellten Mängel, deren Bewertung sowie die abgeleiteten Maßnahmenziele zur Behebung der Mängel. Bei der Bewertung der festgestellten Mängel ist das in Abschnitt 4.6 dargestellte Bewertungsschema zu verwenden:

- Maßnahmenziel (siehe Kapitel 7)
- Ergebnis einschließlich Bewertung
- Stichprobe(n)
- Beschreibung festgestellter Mängel inkl. Maßnahmenempfehlung(en)

Formale Aspekte zum Beurteilungsbericht

Bei der Erstellung des Beurteilungsberichts sind folgende formalen Aspekte zu berücksichtigen:

- Die Seitenkennzeichnung muss so gestaltet sein, dass jede Seite eindeutig identifiziert werden kann (z. B. mit Seitennummer sowie Versionsnummer, Bezeichnung und Datum des Berichts).
- Verwendete Fachbegriffe oder Abkürzungen, die nicht allgemein gebräuchlich sind, müssen in einem Glossar bzw. Abkürzungsverzeichnis zusammengefasst werden.
- Der Bericht muss die geprüften Organisationseinheiten und die Empfänger des Berichts eindeutig bezeichnen sowie etwaige Verwendungsbeschränkungen vermerken.
- Der Bericht ist durch den Beurteiler zu unterschreiben.
- Form und Inhalt eines Berichts können je nach Art der in Auftrag gegebenen Beurteilungsarbeiten unterschiedlich sein, jedoch sind für den CSC-OT die Mindestanforderungen an den Beurteilungsbericht[12] sowie der ISACA IT-Prüfungsstandard 1401 (siehe [ISACA1]) einzuhalten.

12. Ein Muster-Bericht für einen CSC-OT findet sich auf der Webseite des ISACA Germany Chapter e. V. (siehe Kap. 7).

5 Glossar und Begriffsdefinition

Die folgenden Begrifflichkeiten werden in diesem Dokument verwendet:

Aktor oder **Aktuator** ist ein technisches Bauteil, das ein elektrisches Signal in eine physikalische Größe (elektrisches Signal in mechanische Bewegungen etc.) umsetzt und damit der Prozesssteuerung dient.

APT (Advanced Persistent Threat) bezeichnet einen sehr komplexen, zielgerichteten, aufwendig vorbereiteten und durchgeführten Cyber-Angriff. Aufgrund der hohen technischen Komplexität, der genauen Abstimmung auf das Ziel und der dafür erforderlichen fachlichen Expertise gelten APTs als äußerst aufwendig und die negativen Auswirkungen für die betroffene Stelle oft als erheblich.

Asset/Inventar bezeichnet im Allgemeinen einen Vermögenswert (Asset) von materiellem oder immateriellem Wert, der es wert ist, geschützt zu werden, einschließlich Menschen, Informationen, Infrastrukturen (Hardware, Software etc.), Finanzen oder Ansehen (ISACA CSX Nexus).

Assetregister/Inventarregister (Vermögenswert, Anlagegut[13]) ist eine Aufstellung/Liste von Hardware (z. B. Server und Switches), Software (z. B. geschäftskritische Anwendungen und Unterstützungssysteme) und vertraulichen Informationen in einer informationstechnischen Umgebung. Sie sind integrale Bestandteile der Systeme und der Netzwerkinfrastruktur des Unternehmens. Bei der Informationssicherheit, der Computersicherheit und der Netzwerksicherheit handelt es sich bei einem IT-Asset um Daten, Geräte oder andere Komponenten der Umgebung, die informationsbezogene Aktivitäten unterstützen.

CPPS (»**Cyber-physisches Produktionssystem**«) ist ein in einer industriellen Produktionsumgebung genutztes *CPS*.

CPS (»**Cyber-physisches System**«) meint eine komplexe Struktur, in der IT-Komponenten mit mechanischen/elektronischen Komponenten permanent vernetzt sind. Die Strukturen können dabei sehr umfassend werden, wie z. B. bei einem intelligenten Stromnetz.

13. Definition aus dem BSI Compendium für Betreiber, VDI 2182.

CPS-Plattform ist die Basis für Aufbau und Integration eines *CPS*.

Cyber-Kriminalität sind kriminelle Aktivitäten, die den *Cyber-Raum* als Quelle, Ziel und/oder Werkzeug nutzen.

Cyber-Raum umfasst alle durch das Internet über territoriale Grenzen hinweg weltweit erreichbaren Informationsinfrastrukturen.

Cyber-Sicherheit verfolgt im *OT*-Umfeld den Schutz der Verfügbarkeit, Integrität und Vertraulichkeit von OT-Anlagen und Informationen gegen Bedrohungen aus dem *Cyber-Raum*.

Data Historian (auch Process Historian, Operational Historian) bezeichnet ein Programm, das Zeitserien von Produktions- oder Prozessdaten entgegennimmt und aufzeichnet. Die Daten werden unter anderem zum Statuscheck, zur Qualitätssicherung oder zur Kosten- und Performanzkontrolle herangezogen.

DCS (Distributed Control System) ist ein verteiltes, typischerweise hierarchisches System von Kontrolleinheiten, die über ein Netzwerk verbunden sind. Solche Systeme werden für komplexe Gesamtsysteme (Werke, Prozessketten) eingesetzt.

Embedded System ist ein in ein anderes System – typischerweise eine Maschine – »eingebettetes System«, wobei mit letzterem ein Computer gemeint ist, der eine bestimmte Überwachungs- oder Steuerungsfunktion im Gesamtkontext übernimmt. Das eingebettete System ist dabei für den Benutzer meist nicht als solches zu erkennen. Die Variation reicht von hochspezialisierten Modulen bis zu »embedded PCs«.

Firmware ist in elektronische Geräte mehr oder weniger fest eingebettete (embedded) Software. Heutzutage geschieht dies meist in einem *Flash-Speicher* oder *EEPROM* und damit ist sie grundsätzlich auch ohne Austausch von Hardware änderbar, ggf. ist sie aber auch fest in *ROM* oder *EPROM*. Firmware und Hardware bilden eine nur gemeinsam funktionierende Einheit. Sie liegt damit ggf. noch unterhalb des Betriebssystems.

Flash-Speicher ist eigentlich ein Flash-*EEPROM*, kann aber – beispielsweise in Form eines USB-Sticks oder von SSD-Festplatten – auch für das Wiederbeschreiben durch Anwender gedacht sein. Er trägt aber auch häufig die *Firmware* einer Komponente. Die Informationen wer-

den als ortsfeste Ladungen gespeichert, die nicht abfließen können (sodass die Information persistent gespeichert ist), weil eine Leitung in die Speicherschicht nur über einen Isolator hinweg mit hohen Spannungen und durch den quantenmechanischen Tunneleffekt ermöglicht wird.

HMI bezeichnet die »Human-Machine-Interaction«, also die Wechselwirkung zwischen Menschen und Maschinen. HMI ist auch die Abkürzung für Human-Machine-Interface (Mensch-Maschine-Schnittstelle), ein Gerät oder eine Software, die dem Benutzer die Kommunikation mit Maschinen oder Produktionsanlagen ermöglicht.

ICS (Industrial Control System) bezeichnet Steuerungssysteme für industrielle Anlagen von einzelnen Anzeigetafeln bis hin zu weit verteilten Systemen mit mehreren Tausend Feldanschlüssen.

Industrie 4.0 bezeichnet den Übergang hin zur »vernetzten« Fabrik, nachdem in den Stufen davor der Übergang von »Industrie 0.0« (keine Industrie) über Industrie 1.0 (Fabrik durch Mechanisierung), 2.0 (Elektrifizierung) zu 3.0 (Elektronifizierung) erfolgte. Die Besonderheit beim 4.0-Übergang besteht darin, dass die nun in einem Netz hängenden Produktionswerkzeuge sich »gegenseitig kennenlernen« und damit eine übergreifende Selbstoptimierung möglich wird. Die Grenzen der Fabrik beginnen dabei zu zerfließen, weil sie nicht mehr nur physisch zu definieren sind. Mehrere Fabriken können durch Vernetzung ebenso zu einer »Meta-Fabrik« werden, wie Herstellung und Logistik zusammenwachsen (Teile der Endproduktion werden durch den Logistiker übernommen) und sogar der Verbraucher kann zum Teil der Fabrik werden, weil er direkt in das Produkt-Customizing eingreift (z. B. per »car configurator« oder Poster-/T-Shirt-Druck mit individuellen Motiven via Internet u. a.).

Integration, horizontale ist das Zusammenführen von Komponenten über Systemgrenzen hinweg innerhalb einer funktionalen oder organisatorischen Hierarchieebene.

Integration, vertikale ist das Zusammenführen von Komponenten innerhalb eines Systems über funktionale oder organisatorische Hierarchieebenen hinweg.

Intelligente Fabrik (engl. »smart factory«) bezeichnet eine Umgebung, in der auf Basis von *CPS* Fertigung und Logistik selbstorganisierend integriert sind, bis hin zu einem mit der Produktionsanlage kommunizierenden Produkt (*intelligentes Produkt*).

Intelligente Produktion (engl. »smart production«) ist der Herstellungsvorgang in einer *intelligenten Fabrik*, der ggf. eine Kommunikation zwischen dieser und den *intelligenten Produkten* einschließt.

Intelligentes Produkt (engl. »smart product«) bezeichnet ein Werkstück, das mit seiner Fertigungsanlage und in der Logistikkette mit den *CPS* oder anderen Produkten kommuniziert.

IoT, Internet of Things (dt. **Internet der Dinge**), ist ein Sammelbegriff für Technologien einer globalen Infrastruktur der Informationsgesellschaften, die es ermöglicht, physische und virtuelle Gegenstände zu vernetzen und sie durch Informations- und Kommunikationstechniken zusammenarbeiten zu lassen.

KRITIS (kritische Infrastrukturen) sind Organisationen oder Einrichtungen mit wesentlicher Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

Legacy System (dt. »Altsystem«) bezeichnet in der Informatik eine etablierte, historisch gewachsene Anwendung im Bereich Unternehmenssoftware. Legacy ist hierbei das englische Wort für Vermächtnis, Hinterlassenschaft, Erbschaft oder auch Altlast.

Leitung/Management wird als Begriff für Vorstand, Geschäftsführer, Behördenleitung verwendet.

Maßnahmenziele (engl. »control objectives«) sind Vorgaben für die mit den Maßnahmen zu erreichenden Aspekte, mit denen also der Erfolg der Maßnahmen beurteilt werden kann. Hierzu gehören Themen des Sicherheitsmanagements genauso wie technische Aspekte.

MTU ist eine »Master Terminal Unit«, von der aus in einem *SCADA*-Kontext Kommandos an *RTU*s abgesetzt werden und Informationen von den RTUs abgefragt werden, wobei die MTU die Verbindung aufbaut. An der MTU im Kontrollzentrum werden die Informationen

zusammengeführt und aufbereitet, sodass Kontrollentscheidungen getroffen werden können.

Office-IT bezeichnet in Abgrenzung zu *Produktions-IT* (siehe dort) im Kontext dieses Leitfadens alle IT-Komponenten außerhalb der Fertigung und damit die klassische Büro-IT ebenso wie die IT-Komponenten im Rechenzentrum.

Orchestrierung kann sich u. a. auf Services oder Systeme beziehen und meint das flexible Zusammenführen verschiedener Einzelkomponenten zu einem wohldefinierten Zweck.

OT ist die Abkürzung für operative Technologie (engl. Operational Technology) und steht als eine allgemeine Bezeichnung für jede Art von Kontrollsystem in der industriellen Produktion. OT umfasst damit ICS, SCADA, DCS und PLC-Systeme und leitet aus Sensor-Daten (automatisch oder via Operateur) Entscheidungen ab, mittels derer Aktoren angesteuert werden.

PLC (Programmable Logic Controller) ist eine programmierbare Kontrolleinheit, die digitale oder analoge Inputs mittels *Sensoren* aufnehmen, verarbeiten und digitale oder analoge Outputs mittels *Aktoren* erzeugen kann. Es handelt sich also um einen I/O-optimierten und typischerweise für industrielle Bedingungen »gehärteten« Computer mit einem Real-Time Operating System.

PNK ist eine »prozessnahe Komponente« (engl. »Field Control Station« (FCS)) und damit in einem Steuerungssystem eine mit *Sensor* oder *Aktor* direkt verbundene Komponente wie ein *PLC*.

Produktions-IT bezeichnet in Abgrenzung zu *Office-IT* (siehe dort) alle IT-Komponenten, die in einer Fertigungsanlage eingesetzt werden, wie Anlagensteuerung, *Sensoren, Aktoren* und Robotik. Nicht zu verwechseln ist der Begriff mit der ähnlichen bis gleichen Bezeichnung für eine »Staging-Ebene« in der IT im Sinne einer Entwicklungs-, Test- und Produktionsumgebung bei der »Produktivsetzung« neuer Komponenten.

ROM, EPROM, EEPROM sind Formen von »Read Only Memory« oder »Festwertspeicher« und damit eine Speicherform, auf die durch den Anwender nur lesend, aber nicht schreibend bzw. ändernd zugegriffen werden kann. Das einmalige, initiale Beschreiben eines ROM wird als Programmierung bezeichnet und ist methodisch sehr verschieden von einem Schreibzugriff auf einen Schreib-Lese-Speicher (RAM). Formen des ROM sind das einmalig programmierbare »Programmable ROM« (PROM), das mit UV-Licht löschbare »Erasable Programmable ROM« (EPROM) und das elektrisch löschbare »Electrically EPROM« (EEPROM). Heutzutage wird statt eines ROM häufig ein *Flash-Speicher* benutzt.

RTU ist eine »Remote Terminal Unit«, also ein Fernbedienungs- bzw. Fernwartungs-Terminal.

SCADA steht für »Supervisory Control and Data Acquisition« und damit für das Überwachen und Steuern technischer Prozesse mit einem IT-System.

Sensor ist ein technisches Bauteil, das physikalische oder chemische Messgrößen quantitativ erfassen und in ein elektrisches Signal umwandeln kann und damit der Prozessüberwachung dient.

VDE ist der »Verband der Elektrotechnik Elektronik Informationstechnik e. V.«, der unter anderem Regeln für die (Elektro-)Technik für die Normierung, Prüfung und Zertifizierung erarbeitet.

VDMA ist der »Verband Deutscher Maschinen- und Anlagenbau«, der die Interessen seiner vorrangig mittelständischen Mitgliedsunternehmen der Investitionsgüterindustrie vertritt.

VVI beschreibt die Schutzziele in der Operational Technology, welche die Verfügbarkeit, die Vertraulichkeit und die Integrität sind.

ZVEI ist der »Zentralverband Elektrotechnik- und Elektronikindustrie«, der die Interessen seiner vorrangig mittelständischen Mitgliedsunternehmen der Elektroindustrie vertritt.

6 Literaturverzeichnis

[ACS1] Allianz für Cyber-Sicherheit, Webauftritt, *www.allianz-fuer-Cyber-Sicherheit.de*

[ACS2] TOP-10-Cyberbedrohungen ICS-Anlagen, *https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005.html*

[ICS-Kompendium] ICS-Security-Kompendium für Hersteller und Integratoren, BSI, 2014

[IEC 62264-3] IEC 62264-3:2016-12 Enterprise-control system integration – Part 3: Activity models of manufacturing operations management

[IEC 62443-1-1] IEC TS 62443-1-1:2009 Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models

[IEC 62443-3-3] IEC 62443-3-3:2013 Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels

[ISACA1] ISACA, IT-Prüfungsstandards, 2013, *www.isaca.org/Knowledge-Center/Standards/Pages/Standards-forIS-Audit-and-Assurance-German.aspx*

[ISO 27001] DIN EN ISO/IEC 27001:2017-06 Informationstechnik -Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Anforderungen

[IT-Grundschutz-Kompendium] IT-Grundschutz-Kompendium, BSI, 2020

[SANS-Survey] SANS 2019 State of OT/ICS Cybersecurity Survey, Seite 7, Figure 4: Comparison of OT/Control System Incidents 2017 vs. 2019

7 Maßnahmenziele

Die nachfolgend aufgeführten Maßnahmenziele A bis N sind bei der Durchführung eines Industrie-Cyber-Sicherheits-Checks verbindlich zu beurteilen. Die Reihenfolge der Maßnahmenziele ist dabei nicht als Priorisierung oder zwingende Abfolge bei der Beurteilung anzusehen, sondern dient lediglich der Strukturierung. Zur Beurteilung eines Maßnahmenziels sind die zu dem jeweiligen Maßnahmenziel zugehörigen Basismaßnahmen heranzuziehen. Die Stichproben für die Vor-Ort-Beurteilung sind nach einem risikoorientierten Ansatz zu prüfen. Dabei ist neben der Bedrohungslage und der damit verbundenen Schadenseintrittswahrscheinlichkeit insbesondere die Kritikalität der Auswirkungen auf die Produktionsprozesse mit einzubeziehen.

Ziffer	Maßnahmenblock
A	Segmentierung und Zonierung des Netzwerks und Absicherung der Netzwerkübergänge
B	Abwehr von Schadprogrammen und Sicherheitsgateways
C	Beschaffung und Inventarisierung von Systemen
D	Vermeidung von Sicherheitslücken, Systemhärtung und Änderungsmanagement
E	Sichere Interaktion mit Bereichen außerhalb der Automatisierungsnetze und Fernwartung
F	Logdatenerfassung, -auswertung und Systemüberwachung
G	Sicherstellung eines aktuellen Informationsstands
H	Bewältigung von Sicherheitsvorfällen
I	Sichere Identifizierung und Authentifizierung, insbesondere von menschlichen Nutzern
J	Gewährleistung der Verfügbarkeit von Ressourcen, Cyber-Sicherheitsorganisation
K	Durchführung nutzerorientierter Maßnahmen, Sensibilisierung und Weiterbildung
L	Sichere Nutzung sozialer Netzwerke
M	Analyse von Schwachstellen und Konfigurationsüberprüfung
N	Sicherer Umgang mit Cloud-Diensten

Maßnahmenziele		Basismaßnahmen	Referenzen
A	**Segmentierung und Zonierung des Netzwerks und Absicherung der Netzwerkübergänge** Die Produktionsnetze sind in Sicherheitszonen unterteilt und durch geeignete Gateways voneinander getrennt. Es soll durch die Zonierung der Netze verhindert werden, dass ein Internet-Angriff ungehindert bis in die Automatisierungsebene durchschlägt. Idealerweise bildet jede Anlage einen eigenen Sicherheitsbereich, übergeordnete Bereiche, wie Level 2, Level 3, IT, Cloud, Fernzugriff, sind wie Zwiebelschalen kaskadiert und bilden somit ein geeignetes Defense-in-Depth-Konzept.	– Alle Produktionsnetze sind in Segmente unterteilt und von den IT-Netzen getrennt. Alle Übergänge sind identifiziert und dokumentiert und durch geeignete Gateways geschützt. – Der Datenverkehr zu und von den Produktionsnetzen ist durch eine DMZ zu leiten und zu kontrollieren. Dies gilt insbesondere für Verbindungen aus nicht vertrauenswürdigen Netzen. – Drahtlos- und Funkverbindungen sind besonders abzusichern (Verschlüsselung und Zugangskontrolle). – Netzwerkzugriff erhalten nur zugelassene mobile Endgeräte, die keine weitere Netzwerkverbindung aktiv haben dürfen (Brücke ins IT-Netz oder Internet durch zweite Netzwerkschnittstelle).	**ISO/IEC 27001:2013** A.6.2.1, A.9.1.2, A.12.1.4, A.13.1.1, A.13.1.2, A.13.1.3, A.14.1.2, A.14.1.3 IEC 62443-1-1 IEC 62443-3-3 FR 5: SR 5.1, SR 5.2, SR 5.3 **BSI IT-Grundschutz 2021:** IND.1.A5, IND.1.A16, IND.1.A20, IND.1.A21, IND.2.1.A1, IND.2.1.A2, IND.2.1.A6, IND.2.1.A11, IND.2.1.A16, IND.2.1.A17, IND.2.2.A3, IND.2.3.A3, IND.2.4.A1, IND.2.7.A7, IND.2.7.A9, DER.1.A8, CON.1, NET.1.1, NET.1.2, NET.2.1, NET.2.2, NET.3.1, NET.3.2, NET.3.3, OPS.3.1.A11, OPR.4.A16, SYS.3.2.2.A10

→

Maßnahmenziele		Basismaßnahmen	Referenzen
A		– Komponenten aus den Ebenen 0-2 sollten nur externen Netzzugang erhalten, wenn dies für die Funktionalität zwingend notwendig ist. – Die Netzwerksegmentierung ist geeignet, DoS-Angriffe abzuwehren, speziell im Bereich der Echtzeitkommunikation.	

Maßnahmenziele		Basismaßnahmen	Referenzen
B	**Abwehr von Schadprogrammen und Sicherheitsgateways** Im Sinne einer gestaffelten Verteidigung gegen Angriffe durch Schadprogramme müssen mehrere Sicherheitsgateways hintereinander zum Einsatz kommen, die die Ausbreitung von Schadcode erkennen und verhindern. Ziel ist es, die letzte Verteidigungslinie möglichst nahe an die Anlage heranzubringen bzw. dort abzubilden.	– Firewalls oder Application Layer Gateways (ALGs), die zwischen Zonengrenzen zum Einsatz kommen, sollten Funktionalitäten zur Erkennung und Abwehr von Schadprogrammen besitzen. – Es sollten dabei unterschiedliche Technologien, wie signaturbasierte Erkennung, Heuristik, »Machine based Learning« etc., zum Einsatz kommen. Server- und Bediener-systeme sind mit einem geeigneten Virenschutz ausgestattet. Systeme ohne entsprechenden Schutz sind isoliert. – Neben den vorher genannten technischen Maßnahmen sollten organisatorische Vorgaben zum Schutz vor Schadsoftware und Missbrauch u. a. zur Nutzung von externen Wartungsnotebooks und Wechseldatenträgern etabliert sein.	**ISO/IEC 27001:2013** A.12.2.1 IEC 62443-3-3 FR 3: SR 3.2, SR 3.3, SR 3.4, FR 7: SR 7.1 **BSI IT-Grundschutz 2021:** IND.1.A3, IND.1.A10, IND.2.1.A8, DER.1, DER.2.1, DER.2.2, OPS.1.1.4

Maßnahmenziele		Basismaßnahmen	Referenzen
C	**Beschaffung und Inventarisierung von Systemen** Zur Identifikation von Risiken und Planung von Abwehrmaßnahmen auf den eingesetzten Systemen ist eine vollständige Inventarisierung erforderlich. Bereits bei der Beschaffung ist eine geeignete Klassifizierung vorzunehmen, sodass die Geräte entsprechend ihrem Einsatzzweck ausgewählt und abgesichert werden können. Bei der Auswahl der Geräte sind Hersteller und Produkte zu bevorzugen, die über entsprechende Sicherheitszertifizierungen verfügen.	– Alle Systeme (inkl. Hardware und Software) sind vollständig inventarisiert und hinsichtlich ihrer Kritikalität klassifiziert, abgeleitet von auf den Systemen verarbeiteten Daten. – Versionen und Patchstände sind bekannt und werden bei Veränderungen erfasst. Es kommen Tools zur automatisierten Inventarisierung zum Einsatz. – Bei der Beschaffung von neuen Systemen erfolgt im Vorfeld eine Klassifizierung hinsichtlich des geplanten Einsatzzweckes. – Neue Komponenten werden vor der Inbetriebnahme inventarisiert, soll heißen, wir gehen von einem digitalen Zwilling aus, dessen Asset-Inventarisierung die Software, die Konfiguration, inkl. der Sicherheitseinstellungen, und die cyber-sicherheitsrelevante Dokumentation enthalten muss.	**ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.8.1.3, A.8.2.1, A.8.2.3 IEC 62443-2-1 IEC 62443-3-3 FR 7: SR 7.8 **BSI IT-Grundschutz 2021:** IND.1.A11, IND.1.A23, IND.2.1.A13, OPS.1.1.3.A1, ORP.4.A3, IND.1.A12, IND.1.A3, DER.4.A14, ER.1.A9, ORP.1.A2, ORP.3.A3, ORP.1.A7

Maßnahmenziele		Basismaßnahmen	Referenzen
D	**Vermeidung von Sicherheitslücken, Systemhärtung und Änderungsmanagement** Um das Risiko erfolgreicher Cyber-Angriffe zu minimieren, müssen ausnutzbare Sicherheitslücken konsequent vermieden werden.	– Ein wirksamer Change-Management-Prozess sollte etabliert werden. – Bei der Planung und Beschaffung von Komponenten werden die Sicherheitsfunktionalitäten und entsprechende Zertifizierungen berücksichtigt. – Kommunikationsschnittstellen sollten deaktiviert werden, sofern diese nicht benötigt werden. Aktive Schnittstellen sollten möglichst gehärtet betrieben werden, d. h., nicht genutzte Dienste sollten deaktiviert werden. – Die Patch- und Updatefähigkeit der eingesetzten Komponenten ist für den geplanten Lifecycle sichergestellt. – Bekannte Sicherheitslücken werden durch Workarounds und bereitgestellte Sicherheitsaktualisierungen geschlossen.	**ISO 27001:2013** A.12.1.2, A.12.5.1, A.12.6.1, A.14.1.1, A.14.2.2, A.14.2.3, A.14.2.4 IEC 62443-4-1 Practice 7 – Security-Update-Management **BSI IT-Grundschutz 2021:** IND.1.A3, IND.1.A6, IND.1.A12, IND.1.A17, IND.2.1.A4, IND.2.1.A13, IND.2.7.A2, IND.2.7.A3, CON.1.A1, CON.1.A3, CON.1.A4, CON.1.A5, CON.1.A15, CON.5.A1, CON.5.A3, CON.5.A4, CON.5.A6, CON.5.A9, OPS.1.1.3, OPS.1.1.4.A1, OPS.1.1.4.A6, OPS.1.1.3.A1, OPS.1.1.3.A15, ORP.4.A3, IND.1.A12, IND.1.A3, DER.4.A14, DER.1.A9

→

Maßnahmenziele		Basismaßnahmen	Referenzen
D		– Betriebssysteme, Serverdienste und Anwendungen werden vor Inbetriebnahme gehärtet. – Ein Prozess zur sicheren Softwareentwicklung ist etabliert. – Es muss ein effektives Schwachstellen- und Updatemanagement eingeführt sein.	

Maßnahmenziele		Basismaßnahmen	Referenzen
E	**Sichere Interaktion mit Bereichen außerhalb der Automatisierungsnetze und Fernwartung** Kommunikationsvorgänge zwischen den Automatisierungsnetzen und Bereichen außerhalb dieser Netze (wie Level 2 und 3, Cloud, IT-Bereich, Remote- und Fernwartungszugänge) sind mit geeigneten Maßnahmen abzusichern, um Angriffe zu verhindern. Diesen sollte eine entsprechende Risikoanalyse zugrunde liegen. Insbesondere ist in Betracht zu ziehen, dass Angreifer Systeme als Zwischenstation nutzen können, um darüber Angriffe gegen andere Ziele zu führen.	– Die Kommunikation mit Bereichen außerhalb der Automatisierungstechnik ist eingeschränkt. Die Zahl der Übergänge ist minimal gehalten. – Durch eine Default-Regel DENY-ANY ist die transparente IP-Kommunikation unterbunden. Erlaubt ist nur, was explizit freigegeben wird. – Persönliche Kommunikation, IT-Dienste, wie Internet, E-Mail, Chat, sind unterbunden. – Unsichere Protokolle, für die bekannte Schwachstellen oder viele Angriffsvektoren existieren, werden vermieden. – Idealerweise kommen Protokolle zum Einsatz, die über Application Layer Gateways zuverlässig eingeschränkt und geschützt werden können. Verbindungen sollten soweit möglich von innen nach außen aufgebaut werden. – Es existiert ein belastbares Konzept zur sicheren Bereitstellung von Remotezugängen und Fernwartungen.	**ISO/IEC 27001:2013** A.13.2.1, A.13.2.2, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3, A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 IEC 62443-3-3 FR 5: SR 5.1, SR 5.2, SR 5.3 **BSI IT-Grundschutz 2021:** IND.1.A21, IND.2.1.A16, IND.2.4.A1, IND.2.7.A9, ORP.1.A12

Maßnahmenziele		Basismaßnahmen	Referenzen
F	**Logdatenerfassung, -auswertung und Systemüberwachung** Um Angriffe erkennen zu können und nachgelagert Analysen durchzuführen, ist es notwendig, auf Logdaten zuzugreifen. Diese müssen gegen Manipulation gesichert werden. Oftmals bleiben Sicherheitsvorfälle unerkannt, weil kurzfristig kein sichtbarer oder offensichtlicher Schaden eintritt. Mithilfe eines gut getarnten und hinreichend vorsichtigen Vorgehens ist es Angreifern aber u. U. möglich, über längere Zeiträume die Kontrolle über Zielsysteme zu übernehmen, ohne dass diese Angriffe unmittelbar aufgrund singulärer Ereignisse detektiert werden. Daher ist es notwendig, ebenfalls Verfahren zur Aufdeckung von	– Relevante Logdaten werden vollständig erfasst und regelmäßig ausgewertet. – Die Nutzung privilegierter Konten, administrativer, insbesondere schreibender Zugriffe wird fortlaufend überwacht. – Logdaten sind angemessen vor Manipulation und Zerstörung geschützt. – Änderungen an Konfigurationen sind, wenn möglich, automatisiert zu überwachen und Alarmierungen bei relevanten Ereignissen durchzuführen. – Es ist sicherzustellen, dass Datum und Zeitsynchronisation im gesamten Netz einheitlich zur Verfügung gestellt werden.	**ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4 IEC 62443-3-3 FR 2: SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 FR 3: SR3.3, SR 3.4 **BSI IT-Grundschutz 2021:** IND.1.A10, DER.1, DER.2.1.A2, PS.1.1.5, ORP.5.A3

→

Maßnahmenziele		Basismaßnahmen	Referenzen
F	nicht offensichtlichen Sicherheitsvorfällen und langfristig angelegten Angriffen zu entwickeln. Hierbei sind auch Konfigurationsdateien zu überwachen, um Änderungen, insbesondere ungewollte Änderungen, nachvollziehen zu können und zeitnah darauf reagieren zu können.		

Maßnahmenziele		Basismaßnahmen	Referenzen
G	**Sicherstellung eines aktuellen Informationsstands** Die Fähigkeit zur Planung wirksamer Cyber-Sicherheitsmaßnahmen wird im Wesentlichen durch die Qualität und den Umfang des eigenen Informationsstands bestimmt. Daher muss die Versorgung mit aktuellen und fachlich verlässlichen Informationen zur Cyber-Sicherheit, insbesondere zu den Aspekten von OT-Anlagen, sichergestellt werden.	– Aktuelle Informationen zur Cyber-Sicherheit werden fortlaufend aus verlässlichen Quellen bezogen und ausgewertet. – Cyber-Sicherheitsmaßnahmen werden regelmäßig auf der Basis vorhandener Informationen hinsichtlich ihrer Effektivität überprüft und angepasst.	**ISO/IEC 27001:2013** A.6.1.4, A.16.1.3 **BSI IT-Grundschutz 2021:** IND.1.A12, IND.2.7.A4, DER.1.A12, DER.2.1.A2, DER.2.1.A9, OPS.1.1.3.A1

Maßnahmenziele		Basismaßnahmen	Referenzen
H	**Bewältigung von Sicherheitsvorfällen** Geeignete Prozesse und Verfahren zur Bewältigung von Sicherheitsvorfällen sind zu etablieren und zu üben, um eine schnelle und angemessene Bewältigung von Sicherheitsvorfällen und damit die Aufrechterhaltung des Geschäftsbetriebs sicherzustellen.	– Es existieren etablierte Prozesse und Verfahren zur schnellen und angemessenen Bewältigung von Sicherheitsvorfällen (Notfallmanagement). – Es müssen regelmäßige Datensicherungen durchgeführt werden. – Die Bewältigung von Sicherheitsvorfällen wird regelmäßig geübt (Wiederherstellungstest). Dabei wird insbesondere geprüft, ob die vorgesehenen Notfallmaßnahmen wirksam sind. – Abgeschlossene Sicherheitsvorfälle werden hinsichtlich der Ursachen und möglicher Konsequenzen ausgewertet. – Sicherheitsvorfälle werden zur Strafverfolgung und Lagebilderstellung an die zuständigen Behörden gemeldet.	**ISO/IEC 27001:2013** A.12.3.1, A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.17.1.1, A.17.1.2, A.17.1.3, A.17.2.1 IEC 62443-3-3 FR 6 **BSI IT-Grundschutz 2021:** IND.2.1.A7, IND.2.1.A18, IND.2.7.A5, CON.3, DER.2.1, DER.2.2, DER.2.3, DER.4

Maßnahmenziele		Basismaßnahmen	Referenzen
I	**Sichere Identifizierung und Authentifizierung, insbesondere von menschlichen Nutzern** Die Authentisierung ist notwendig, um unberechtigte Zugriffe von Benutzern zu verhindern sowie Aktivitäten nachzuvollziehen und zuordnen zu können.	– Es muss gewährleistet werden, dass nur identifizierte und berechtigte Personen Zugang zur Anlage erhalten. – In kritischen Bereichen werden besonders sichere Passwörter oder Multi-Faktor-Authentisierungs-(MFA-)Verfahren eingesetzt. – Die Zugangskennungen und damit verbundene Berechtigungen werden an zentraler Stelle verwaltet, regelmäßig überprüft und bei Bedarf angepasst oder entzogen. – Sitzungen werden beim Verlassen des Bedienerplatzes gesperrt. Erfolglose Anmeldeversuche werden protokolliert und ausgewertet. – Authentisierungsdaten für Bereiche unterschiedlichen Schutzbedarfs sollten voneinander getrennt werden.	**ISO/IEC 27001:2013** A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.4.2, A.9.4.4 IEC 62443-3-3 FR 2: SR 2.1, SR 2.2, SR 2.3, SR 2.5, SR 2.6, SR 2.7 **BSI IT-Grundschutz 2021:** IND.1.A8, IND.1.A14, IND.1.A15, IND.2.2.A2, APP.2.1, APP.2.2, ORP.4, NET.1.2, NET.2.1, NET.2.2, NET.3.1, NET.3.2, NET.3.3, OPS.1.1.2, OPS.1.2.5.A3, OPS.1.2.5.A7, OPS.1.2.5.A17, ORP.1, ORP.4, SYS.1.1, SYS.2.1, SYS.3.2.1

Maßnahmenziele		Basismaßnahmen	Referenzen
J	**Gewährleistung der Verfügbarkeit von Ressourcen, Cyber-Sicherheits-organisation** Zur wirksamen Abwehr von Bedrohungen der Cyber-Sicherheit sind ausreichend eigene finanzielle und personelle Ressourcen bereitzustellen.	– Es existiert eine Cyber-Sicherheitsorganisation mit einem Informationssicherheitsbeauftragten für die Automatisierungstechnik (ISB-OT). – Es müssen finanzielle und personelle Ressourcen zur Abwehr von Bedrohungen der Cyber-Sicherheit ausreichend zur Verfügung stehen. – Bei Bedarf werden qualifizierte und zuverlässige externe Dienstleister eingebunden. – Unter Ressourcen sind auch Test- und Entwicklungsumgebungen vorzusehen.	**ISO/IEC 27001:2013** A.6.1.1, A.6.1.2, A.12.1.1, A.12.1.4, A.12.3.1 IEC 62443-2-1 ORG 1.1, ORG 1.3 **BSI IT-Grundschutz 2021:** IND.1.A1, ISMS.1, PS.1.1.2, ORP.1

Maßnahmenziele		Basismaßnahmen	Referenzen
K	**Durchführung nutzerorientierter Maßnahmen, Sensibilisierung und Weiterbildung** Auch das eigene Personal muss in den Mittelpunkt einer Cyber-Sicherheitsstrategie gerückt werden. Sämtliche technischen Vorkehrungen können durch menschliche Fehler oder bewusste Fehlhandlungen unwirksam werden.	– Bediener, Instandhaltung und OT-Personal werden zielgruppenorientiert regelmäßig für die Gefahren eines Cyber-Angriffs sensibilisiert und hinsichtlich des korrekten Verhaltens geschult. – Standard-Sicherheitsprinzipien werden umgesetzt, z. B. die Kenntnis von Passwörtern und Systemdetails werden nur erforderlichen Personen zugänglich gemacht. – Personal und Management sind mit ihren Rollen und Verantwortlichkeiten vertraut. – Es ist eine klare Rollentrennung vorhanden. Eine Konzentration zu vieler Zuständigkeiten in einer Rolle wird vermieden.	**ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A8.1.2 **BSI IT-Grundschutz 2021:** ORP.3

Maßnahmenziele		Basismaßnahmen	Referenzen
L	**Sichere Nutzung sozialer Netzwerke** Mitarbeiter sind zu sensibilisieren, dass keine vertraulichen Informationen (Bilder, Projekte, Anlagendokumente etc.) in sozialen Medien veröffentlicht werden.	– Es existieren verbindliche Vorgaben (Social Media Guidelines) hinsichtlich des sicheren und seriösen Auftritts der Organisation sowie der beruflichen Profile der Beschäftigten in sozialen Netzwerken. – Mitarbeiter werden regelmäßig hinsichtlich der Risiken und des korrekten Verhaltens in sozialen Netzwerken sensibilisiert. – Direkte Schnittstellen zwischen sozialen Netzwerken und Betriebsinfrastruktur dürfen nicht hergestellt werden.	**ISO/IEC 27001:2013:** A.7.2.2, A.8.1.3, A.8.2.3, A.13.2.1, A.13.2.2, A.13.2.3 **BSI IT-Grundschutz 2021:** APP.1.4.A2, CON.9.A1, CON.9.A2, CON.9.A3, CON.9.A4

Maßnahmenziele		Basismaßnahmen	Referenzen
M	**Analyse von Schwachstellen und Konfigurationsüberprüfung** Es sollten regelmäßige Schwachstellen- und Konfigurationsüberprüfungen von qualifizierten und erfahrenen Personen, die nicht an der Planung oder Implementierung der zu beurteilenden Systeme beteiligt waren, durchgeführt werden, um Fehlerquellen frühzeitig zu erkennen.	– Die Systeme werden regelmäßig von unabhängigen, qualifizierten Personen auf sichere Konfiguration, Härtung und Schwachstellen überprüft. Neuentwicklungen sollten vor der Inbetriebnahme auf Schwachstellen überprüft werden. – Umfang und Intensität der Überprüfungen sind der Cyber-Sicherheits-Risikoeinschätzung angemessen. – Die Ergebnisse der Überprüfungen werden konsequent zur Reduzierung von Risiken genutzt.	**ISO/IEC 27001:2013:** A.14.2.8, A.18.2.1, A.18.2.3 **BSI IT-Grundschutz 2021:** IND.1.A12, IND.1.A17, IND.2.1.A19, OPS.1.1.6.A14

Maßnahmenziele		Basismaßnahmen	Referenzen
N	**Sicherer Umgang mit Cloud-Diensten** Die Verwendung von Cloud-Diensten sollte regelmäßig überprüft werden. Insbesondere sollten Abhängigkeiten zwischen der Prozesssteuerung und Cloud-Diensten bekannt sein und bezüglich Risiken bewertet werden, um einen unautorisierten Datenabfluss zu verhindern.	– Es existieren verbindliche Vorgaben hinsichtlich der Speicherung, Verwendung und Verarbeitung von Daten in Cloud-Diensten. – Cloud-Provider sind in Bezug auf die bestmögliche Erfüllung der Sicherheitsanforderungen unter Berücksichtigung kommerzieller Aspekte auszuwählen. – Bei der Auswahl sind Aspekte eines Wechsels des Cloud-Anbieters zu berücksichtigen. – Der angemessene Umgang mit Cyber-Risiken einer Cloud-Lösung muss über ein Risiko-Assessment bestimmt werden. – Cloud-Dienste werden fachgerecht provisioniert, administriert und überwacht. Die Nutzung von Cloud-Diensten sollte einem Freigabeprozess unterliegen.	**ISO/IEC 27001:2013:** A.14.2.8, A.15.1.1, A15.1.2, A15.1.3, A15.2.1, A15.2.2, A.18.2.1, A.18.2.3 **BSI IT-Grundschutz 2021:** IND.2.1.A1, IND.2.1.A4, IND.1.A21, IND.2.1.A16, ISMS.1, ORP.4.A23, OPS.1.1.6, OPS.2.2,

→

Maßnahmenziele		Basismaßnahmen	Referenzen
N		– Mitarbeiter werden regelmäßig hinsichtlich der Risiken und des korrekten Umgangs mit Cloud-Diensten sensibilisiert. – Sofern vorhanden, werden direkte Schnittstellen zwischen Cloud-Diensten und der eigenen OT (und IT) angemessen abgesichert. – Nicht zulässige Cloud-Dienste sollten gesperrt, erlaubte durch geeignete Sicherheitsmaßnahmen geschützt werden.	

ISACA Germany Chapter e. V.
Storkower Straße 158
D-10407 Berlin

www.isaca.de
info@isaca.de