Minimalstandard zur Verbesserung der IKT-Resilienz

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Wirtschaft, Bildung und Forschung WBF
Bundesamt für wirtschaftliche Landesversorgung BWL

Vorwort

Digitalisierung erfordert Schutzmassnahmen

Die zunehmende Vernetzung und Durchdringung praktisch aller Lebensbereiche mit Informatik eröffnet ökonomische wie gesellschaftliche Potenziale, auf die ein hochentwickeltes und industrialisiertes Land wie die Schweiz nicht verzichten kann. Gleichzeitig aber entstehen durch die zunehmende Digitalisierung neue Gefährdungslagen, auf die schnell und konsequent reagiert werden muss. Die besondere Gefahr gezielter Cyber-Angriffe auf die IT-Infrastruktur betrifft staatliche Stellen ebenso wie Betreiber von kritischen Infrastrukturen und andere Unternehmen oder Organisationen.

Die grundsätzliche Verantwortung zum Eigenschutz liegt bei den jeweiligen Unternehmen und Organisationen. Überall da jedoch, wo das Funktionieren von kritischen Infrastrukturen betroffen ist, besteht eine staatliche Verantwortung, basierend auf dem Auftrag der Bundesverfassung sowie dem Landesversorgungsgesetz. Dieser IKT-Minimalstandard ist Ausdruck der Schutzverantwortung des Staates gegenüber den Bürgerinnen und Bürgern, der Wirtschaft, den Institutionen und der öffentlichen Verwaltung.

Der IKT-Minimalstandard setzt dort an, wo sich eine moderne Gesellschaft Ausfälle am wenigsten leisten kann: bei den IKT-Systemen, welche für das Funktionieren der kritischen Infrastrukturen von Bedeutung sind. Betreibern von kritischen Infrastrukturen wird empfohlen, den vorliegenden IKT-Minimalstand oder vergleichbare Vorgaben (z. B. ISO, COBIT usw.) umzusetzen. Das vorliegende Dokument bietet jedoch grundsätzlich jedem interessierten Unternehmen oder jeder Organisation eine Hilfestellung und konkrete Handlungsanweisungen zur Verbesserung der eigenen IKT-Resilienz.

Management Summary

Der vorliegende IKT-Minimalstandard dient als Empfehlung und mögliche Richtschnur zur Verbesserung der IKT-Resilienz. Er richtet sich insbesondere an die Betreiber von kritischen Infrastrukturen, ist aber grundsätzlich für jedes Unternehmen oder jede Organisation anwendbar und frei verfügbar.

Der IKT-Minimalstandard richtet sich insbesondere an IKT-Verantwortliche und Geschäftsleitungsmitglieder von Betreibern kritischer Infrastrukturen.

Das Dokument gliedert sich in drei Teile:

1. Grundlagen: Dieser Teil dient als Nachschlagewerk und soll Hintergrundinformationen zur IKT-Sicherheit vermitteln.

2. Das Framework bietet den Anwendern, gegliedert nach den fünf Themenbereichen «Identifizieren», «Schützen», «Detektieren», «Reagieren» und «Wiederherstellen», ein Bündel konkreter Massnahmen zur Umsetzung an. Total handelt es sich um 106 Massnahmen.

3. Mit dem Self-Assessment und dem zugehörigen Bewertungstool (Excel) können die Organisationen und Unternehmen den Umsetzungsstand der Massnahmen beurteilen, respektive auch durch externe Firmen prüfen lassen (Audit). Die Ergebnisse können als Grundlage für ein organisationsübergreifendes Benchmarking verwendet werden.

Inhaltsverzeichnis

1 Teil 1 – Einführung

1.1 Übersicht

Der Teil 1 definiert die Grundlagen und Zielsetzung der IKT-Sicherheit, grenzt das umfassende Thema ein und erläutert den Einsatz des IKT-Minimalstandards.

1.2 Gesetzliche Grundlagen

Untenstehende Rechtsgrundlagen bilden die Basis für das Handeln der wirtschaftlichen Landesversorgung.[1]

- Bundesgesetz über die wirtschaftliche Landesversorgung (Landesversorgungsgesetz, LVG; SR 531)
- Verordnung über die Organisation der wirtschaftlichen Landesversorgung (Organisationsverordnung Landesversorgung; SR 531.11)
- Verordnung über die Vorbereitungsmassnahmen der wirtschaftlichen Landesversorgung (SR 531.12)

1.3 Ausgangslage und Zielsetzung

IKT-Sicherheit bedingt ein risikobasiertes Verhalten und den Einsatz sicherer Systeme im Verantwortungsbereich der jeweiligen Betreiber. Bereits durch die Umsetzung von bewährten Massnahmen, wie sie in vorliegendem IKT-Minimalstandard dargestellt werden, kann eine Vielzahl von IKT-Angriffen mit vertretbarem Aufwand abgewehrt werden. Der vorliegende Standard hat zum Ziel, Unternehmen und Organisationen ein vielseitig einsetzbares Hilfsmittel zur Hand zu geben, wodurch sie individuell die Resilienz ihrer IKT-Infrastruktur verbessern können. Durch den risikobasierten Ansatz ermöglicht der Standard die Umsetzung unterschiedlich strenger Schutzniveaus, angepasst an die Bedürfnisse der Organisation.

1.4 Abgrenzungen

Der vorliegende IKT-Minimalstandard wurde durch die wirtschaftliche Landesversorgung in Zusammenarbeit mit externen Experten aus dem Bereich der IKT-Sicherheit erarbeitet.

Es existieren heute bereits mehrere international anerkannte Standards zur IKT-Sicherheit, die meist deutlich über das vorliegende Dokument hinausgehen (siehe Kapitel 1.4.1). Der vorliegende Minimalstandard versteht sich explizit nicht als Konkurrenz zu existierenden internationalen Standards, sondern ist mit diesen kompatibel, bei gleichzeitig reduziertem Umfang. Er soll einen einfacheren Einstieg in die Thematik ermöglichen und trotzdem ein hohes Schutzniveau gewährleisten.

Ergänzend zum vorliegenden IKT-Minimalstandard wurden durch die wirtschaftliche Landesversorgung weitere sektorspezifische Standards erarbeitet,[2] die einen höheren (technischen) Detaillierungsgrad aufweisen. Betreibern von kritischen Infrastrukturen wird empfohlen, sich zusätzlich zum Minimalstandard auch an den detaillierten sektorspezifischen Vorgaben zu orientieren, sobald diese vorliegen.

Gelten in einem Sektor bereits eigene Standards, oder werden internationale Standards wie ISO oder NIST verwendet, so können Unternehmen anhand der Checkliste in Kapitel «Teil 3 – Prüfungsauftrag» feststellen, ob sie den vorliegenden Minimalstandard bereits abgedeckt haben.

1.4.1 Grundlagendokumente und Standards

Weltweit existiert eine Vielzahl unterschiedlicher Standards und Informationsquellen zum Umgang mit IKT-Risiken. Einige davon sind von der Wirtschaft schon heute anerkannt und werden eingesetzt. Der vorliegende IKT-Minimalstandard basiert auf dem NIST Cybersecurity Framework Core.[3] Wo sinnvoll, wird er durch weitere international anerkannte Industriestandards ergänzt. Die wichtigsten davon sind:

1. NIST Guide to Industrial Control Systems (ICS) Security
   Dieser Guide wird ebenfalls vom National Institute of Standards and Technology erlassen und gepflegt und ergänzt das NIST Cybersecurity Core Framework um spezifische Vorgaben im Umgang mit industriellen Kontrollsystemen (ICS) im Speziellen, NIST Special Publication 800-82, Revision 2, Mai 2015.[4]

[1] Sämtliche Gesetzestexte lassen sich in der systematischen Sammlung des Bundesrechts nachlesen. Online sind die Gesetzestexte verfügbar unter: https://www.admin.ch/gov/de/start/bundesrecht/systematische-sammlung.html

[2] Aktuell für die Sektoren Stromversorgung und Lebensmittelversorgung. Weitere Sektoren sind in Arbeit und werden nach Fertigstellung veröffentlicht.

[3] https://www.nist.gov/cyberframework

[4] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

2. ISO 2700x
   Die International Organization for Standardization (ISO) veröffentlicht rund ein Dutzend sich gegenseitig ergänzende Standards zur Informatiksicherheit, welche als «2700x-Familie» bezeichnet wird. Der bekannteste Standard darunter ist der Standard ISO 27001. Er spezifiziert die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung des Kontexts einer Organisation.[5]

3. COBIT
   Control Objectives for Information and related Technology (COBIT)[6]

4. ENISA Good Practice Guide on National Cyber Security Strategies.[7]

5. Bundesamt für Sicherheit in der Informationstechnik (Deutschland), BSI 100-2.[8]

1.4.2 Grundsätze

1. Eigenverantwortung: Betreiber von kritischen Infrastrukturen sind grundsätzlich selbstverantwortlich für das Aufrechterhalten ihrer kritischen IKT-Prozesse.
2. Business Continuity Management: Alle Aspekte der IKT-Sicherheit sollen in ein übergeordnetes Business Continuity Management eingegliedert werden.
3. Risikomanagement: Es ist Aufgabe der Anwender dieses Standards, mögliche IKT-Risiken wie die Verletzung der Verfügbarkeit, Integrität und Vertraulichkeit laufend zu bewerten. Das Unternehmen muss beurteilen, welche Risiken gemildert werden sollen und welche es zu tragen bereit ist.

1.4.3 Massnahmen und Verweise in diesem Dokument

Wo immer möglich, wird auf das Duplizieren von Informationen verzichtet. Stattdessen wird auf andere IKT-Standards verwiesen. Den Anwendern dieses Standards wird geraten, bei Bedarf die angegebenen Quellen zu konsultieren.

[5] *https://www.iso.org/standard/66435.html*

[6] *http://www.isaca.org/COBIT/Pages/default.aspx*

[7] *https://www.enisa.europa.eu/topics/national-cyber-security-strategies*

[8] *https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/cyber-sicherheit_node.html*

1.5 Einführung in den IKT-Minimalstandard

In diesem Abschnitt werden die für den IKT-Minimalstandard zentralen Themenfelder vorgestellt.

1.5.1 IKT-Sicherheitsgrundsätze

Bevor IKT-Sicherheit operativ umgesetzt werden kann, muss ein Unternehmen seine IKT-Grundsätze festlegen. Dazu gehört insbesondere die Beantwortung der folgenden Fragen:

- was wird getan?
- wie wird es getan?
- wer ist dafür verantwortlich?
- wie wird es gemessen?

Die IKT-Sicherheitsgrundsätze definieren die Regeln, Prozesse, Metriken und organisatorischen Strukturen, welche für eine effektive Planung und Steuerung erforderlich sind.

1.5.2 Organisation und Verantwortlichkeiten

Als Grundlage für die IKT-Sicherheit muss eine generelle Sicherheitsorganisation im Unternehmen etabliert werden, welche klare Aufgaben, Verantwortungen und Kompetenzen definiert. In diesem Rahmen soll auch die Definition und Umsetzung der Defense-in-Depth-Strategie vorgenommen werden. IKT-Risiken sollen Teil des globalen Risikomanagements sein. Dies ist Voraussetzung, um mögliche IKT-Bedrohungen zu erkennen und entsprechende Massnahmen zu definieren. Die Sicherheitsorganisation muss die Geschäftsleitung befähigen, über die dazu notwendigen Ressourcen zu entscheiden. Die Sicherheitsorganisation ist durch die Geschäftsleitung mit adäquaten Kompetenzen auszustatten, sodass sie ihre Kernaufgaben uneingeschränkt in enger Zusammenarbeit mit den Unternehmensbereichen umsetzen kann.

1.5.3 Politik, Weisungen und Richtlinien

Bevor eine IKT-Sicherheitsstrategie (z. B. Defense-in-Depth-Strategie) umgesetzt werden kann, ist es notwendig, die Richtlinien, Prozesse und Arbeitsanweisungen einer Organisation zu identifizieren oder allenfalls zu definieren.

Die Businessanforderungen der verschiedenen Unternehmenseinheiten müssen den Verantwortlichen für die Cybersecurity gegenüber bekanntgemacht und dokumentiert werden. Es kann sich hierbei bspw. um juristische, finanzielle, strategische oder operative Anforderungen handeln.

1.5.4 Risikomanagement

Voraussetzung für die Verbesserung der IKT-Resilienz durch die Implementierung einer Defense-in-Depth-Strategie ist ein aktives Risikomanagement. Dieses soll den Risikoappetit des Unternehmens berücksichtigen. Daher ist es wichtig, dass die Organisationseinheit, welche für den Betrieb und die Wartung der IKT-Systeme verantwortlich ist, die Methoden und Prozesse des Risikomanagements der Organisation kennt und diese hinsichtlich der IKT-Risiken anwenden kann. Der IKT-Risikoprozess hat zum Ziel, mögliche Bedrohungen für die zu schützenden IKT-Systeme, Applikationen und Daten zu identifizieren, zu bewerten und den Umgang mit den identifizierten Risiken zu definieren. Der Risikoprozess gliedert sich in die drei Teilprozesse Risikoanalyse, Risikobewertung sowie die Risikobewältigung durch Umsetzung entsprechender Massnahmen. Um die Wirksamkeit der Massnahmen zu überprüfen, werden Risiken fortlaufend neu beurteilt und allfällige Veränderungen ausgewiesen. Bei Bedarf werden anschliessend die Massnahmen allenfalls angepasst.

Eine absolute Sicherheit wird es nie geben. Deshalb muss die Unternehmensführung den Risikoappetit festlegen.

1.6 Elemente einer Defense-in-Depth-Strategie

1.6.1 Übersicht Defense-in-Depth

Die IKT-Sicherheitsstrategie eines Unternehmens ist darauf auszurichten, die für die Geschäftsprozesse notwendigen kritischen IKT-Betriebsmittel zu schützen. Dazu braucht es einen mehrschichtigen Ansatz, welcher international als «Defense-in-Depth» bekannt ist. Darunter versteht man einen koordinierten Einsatz mehrerer Sicherheitsmassnahmen, um die IKT-Betriebsmittel in einem Unternehmen zu schützen. Die Strategie basiert auf dem militärischen Prinzip, dass es für einen Feind schwieriger ist, ein komplexes und mehrschichtiges Abwehrsystem zu überwinden als eine einzige Barriere. Gleichzeitig werden die Methoden und Vorgehensweisen der potenziellen Angreifer beobachtet, um darauf basierend entsprechende Abwehrdispositive vorzubereiten. Im IKT-Sicherheitsumfeld zielt ein Defense-in-Depth-Konzept darauf ab, Verletzungen der IKT-Sicherheit zu erkennen, darauf zu reagieren, sowie die Konsequenzen der Sicherheitsverletzung zu minimieren, bzw. zu mildern. Defense-in-Depth verfolgt einen holistischen Ansatz, welcher alle (IKT-)Betriebsmittel gegen beliebige Risiken zu schützen versucht. Die Ressourcen des Unternehmens sollen so eingesetzt werden, dass ein effektiver Schutz vor bekannten Risiken sowie eine umfassende Überwachung potenzieller zukünftiger Risiken gewährleistet ist. Die entsprechenden Massnahmen müssen die Gesamtheit der IKT-Systeme schützen. Dazu gehören Personen, Prozesse, Objekte, Daten und Geräte. Ein Angreifer stellt erst dann eine Bedrohung für ein IKT-System dar, wenn es ihm gelingt, eine existierende Schwachstelle in einem dieser Elemente auszunutzen. Organisationen und Unternehmen sind gehalten, die Massnahmen laufend zu überwachen und, wo nötig, an neue Bedrohungen anzupassen.

1.6.2 Industrielle Kontrollsysteme (Industrial Control Systems, ICS)

Aufgrund der komplexen Architektur von ICS können Verwundbarkeiten schlimmstenfalls sehr lange unentdeckt bleiben und entsprechende Exploits eine Bedrohung darstellen (engl. Advanced Persistent Threat, APT). Der Einsatz des oben beschriebenen Defense-in-Depth-Konzeptes bietet angemessenen Schutz gegenüber diesen Bedrohungen.

Nachfolgend werden einige für ICS typische Angriffsmethoden aufgeführt:

- Angriffe aus dem Internet auf ein online erreichbares ICS, mit dem Ziel, einen dauerhaften Fernzugriff zu etablieren.
- Fernzugriffe auf das ICS unter Ausnutzung gestohlener Zugangsdaten.
- Angriffe auf das ICS durch Ausnutzen von Schwachstellen des Webinterfaces.
- Einschleusen von Malware in das ICS über kompromittierte Datenträger (z. B. USB-Sticks, Smartphones etc.).
- Angriffe auf die Büroautomation (z. B. mittels Phishing-Mails, Drive-by-Infektionen etc.), mit dem Ziel, über allfällige Schnittstellen ins ICS vorzudringen.

Grundsätzlich gilt, dass bezüglich der Implementierung von Defense-in-Depth-Konzepten wichtige Unterschiede zwischen der Büroautomation und einem ICS bestehen. Tabelle 1 zeigt sicherheitsrelevante Themenfelder und ihre unterschiedliche Bedeutung für IKT und ICS.

Sicherheitsthema	IKT (z. B. Büroinformatik)	ICS (z. B. AKW-Steuerung)
Antivirus	Weit verbreitet. Einfach zu verteilen und zu aktualisieren. Anwender haben die Möglichkeit zur Personalisierung. Antiviren-Schutz kann auf Geräte oder Unternehmensebene konfiguriert werden.	Der Speicherbedarf und die Verzögerung des Datenaustauschs durch den Scanvorgang der Antiviren-Software kann ein ICS-System negativ beeinflussen. Organisationen können ihre älteren ICS-Elemente meist nur mit Produkten aus dem Sekundärmarkt schützen. Antivirenlösungen verlangen zudem im ICS-Umfeld oft nach «Ausnahme»-Ordnern, um zu verhindern, dass geschäftskritische Dateien unter Quarantäne gestellt werden.
Sicherheits-aktualisierungen (Update Management)	Klar definiert, unternehmensweit ausgeführt, automatisiert über Fernzugriff.	Lange Vorlauf- und Planungszeit bis zur erfolgreichen Patch-Installation; immer herstellerspezifisch; kann das ICS (temporär) zum Erliegen bringen. Notwendigkeit, das diesbezüglich akzeptable Risiko zu definieren.
Technologie-lebenszyklus (Technology Support Lifecycle)	2–3 Jahre, mehrere Anbieter, laufende Weiterentwicklung und Upgrades.	10–20 Jahre, typischerweise derselbe Lieferant/Dienstleister über den gesamten Lebenszyklus, Ende des Lebenszyklus verursacht neue Sicherheitsgefährdungen.
Methoden zum Testen und Auditieren (Testing and Audit Methods)	Einsatz von zeitgemässen (ev. automatisierten) Methoden. Die Systeme sind üblicherweise resilient und zuverlässig genug, um Assessments im laufenden Betrieb zu ermöglichen.	Z. B. aufgrund des grossen Grades an Individualentwicklungen sind automatisierte Assessmentmethoden möglicherweise nicht geeignet. Es besteht eine höhere Wahrscheinlichkeit für Fehleranfälligkeit während eines Assessments. Assessments im laufenden Betrieb sind deswegen tendenziell schwieriger.
Change Management	Regulär und in regelmässigem Rhythmus geplant. Abgestimmt auf die Vorgaben der Organisation, zur minimalen/maximalen Einsatzdauer.	Komplexer Prozess mit potenziellen Auswirkungen auf die Geschäftstätigkeit der Organisation. Strategische, individuelle Planung notwendig.
Asset Klassifikation (Asset Classification)	Üblich und jährlich ausgeführt. Ausgaben/Investitionen werden gemäss den Ergebnissen geplant.	Wird nur durchgeführt, wenn notwendig/vorgeschrieben. Ohne Inventar sind Gegenmassnahmen oftmals nicht der Bedeutung des Systemelements angemessen.
Vorfallreaktion/-analyse (Incident Response and Forensics)	Einfach zu entwickeln und umzusetzen. U.U. regulatorische Vorschriften (Datenschutz) zu beachten.	Fokussiert primär auf die Wiederaufnahme des Systems. Forensikprozesse wenig entwickelt.
Physische Sicherheit (Physical Security)	Variiert zwischen schwach (Büro-IT) bis stark (gehärtete Rechenzentren).	Typischerweise sehr gute physische Sicherheit.
Sichere System-entwicklung (Secure Software Development)	Integraler Teil des Entwicklungsprozesses.	ICS wurden historisch meist als physisch isolierte Systeme konzipiert. Sicherheit als integraler Teil der Systementwicklung war entsprechend wenig verbreitet. Anbieter von ICS haben diesbezüglich Fortschritte gemacht, jedoch langsamer als in der IKT- Welt. Kernelemente von ICS lassen oft keine nachträglichen Sicherheitslösungen zu, bzw. diese sind nicht verfügbar.
Sicherheitsvorgaben	Allgemeine regulatorische Vorgaben, abhängig vom Sektor (nicht alle Sektoren).	Spezifische regulatorische Richtlinien, abhängig vom Sektor (nicht alle Sektoren).

Tabelle 1: Unterschiede zwischen IT und ICS

Folgende Faktoren sind bei Anwendung eines Defense-in-Depth-Konzeptes in einem ICS zu berücksichtigen:

- Die Kosten, um alte Systeme nach zeitgemässen Bedürfnissen abzusichern
- Der wachsende Trend, ICS mit Geschäftsnetzwerken zu verbinden
- Die Möglichkeit, Fernzugriffe für Anwender zu ermöglichen, sowohl im IKT- als auch im ICS-Umfeld
- Notwendigkeit, der eigenen Zulieferkette (engl. Supply Chain) vertrauen zu müssen
- Zeitgemässe Möglichkeiten, ICS-spezifische Protokolle zu überwachen und zu schützen
- Die Möglichkeit, das Fachwissen über sich neu entwickelnde Bedrohungen gegenüber ICS stets aktuell zu halten

Der Defense-in-Depth-Ansatz erschwert direkte Angriffe auf IKT-Systeme und erhöht die Wahrscheinlichkeit, auffälliges oder unübliches Verhalten innerhalb des Systems frühzeitig zu entdecken. Dieser Ansatz ermöglicht auch die Schaffung von gesonderten Zonen für die Implementierung von Technologien, die ein Eindringen ins System erkennen können (Intrusion-Detection-Technology). Typische Elemente einer Defense-in-Depth-Strategie finden sich in Tabelle 2.

Elemente einer Defense-in-Depth-Strategie	
Risk Management Programm	• Identifizierung von Sicherheitsrisiken • Risikoprofil • Akkurate Bestandsverwaltung der IKT-Betriebsmittel
Cybersecurity-Architektur	• Standards/Empfehlungen • Richtlinien • Vorgehensweise
Physische Sicherheit	• Schutz von Endgeräten • Kontrollzentrum, Zugangskontrollen • Videoüberwachung, Zugangskontrollen & Barrieren
Netzwerk-Architektur	• Typische Sicherheitszonen • Demilitarized Zones (DMZ) • Virtual LANs
Netzwerk Perimeter Security	• Firewalls • Fernzugriff & Authentifizierung • Jump Servers/Hosts
Host Security	• Patch- & Schwachstellen-Management • Endgeräte • Virtuelle Geräte
Security Überwachung	• Intrusion Detection Systems • Sicherheits-Audit-Logging • Sicherheitsvorfall und Event-Überwachung
Vendor Management	• Lieferketten Überwachung & Management • Managed Services & Outsourcing • Nutzung von Cloud-Diensten
Das Element Mensch	• Richtlinien • Vorgehensweisen • Training und Wahrnehmung

Tabelle 2: Elemente einer Defense-in-Depth-Strategie

1.6.3 Risikomanagement

1.6.3.1 Risikomanagementprogramm

Voraussetzung zur Implementierung einer Defense-in-Depth-Strategie ist das Verständnis der Geschäftsrisiken einer Organisation, welche im Zusammenhang mit IKT-Bedrohungen stehen. Diese Risiken müssen in Abstimmung mit dem unternehmensweiten Risikoappetit bewirtschaftet werden. Die Verantwortlichen für Betrieb und Unterhalt von IKT-Systemen müssen Cyberrisiken erkennen, bewerten und adressieren können. Dazu müssen sie verstehen, wie diese Methoden auf ihre jeweilige Systemlandschaft angewendet werden müssen. Dafür braucht es ein klares Verständnis der Bedrohungsszenarien, der operativen und technischen Prozesse sowie der eingesetzten Technologien. Erst dann kann eine Defense-in-Depth-Strategie in das normale Tagesgeschäft integriert werden. Es ist Aufgabe des Managements, «Security» als Voraussetzung aller computerbasierten Aktivitäten in der Organisation zu etablieren.

Die obenstehenden Grundsätze im Umgang mit Risiken gelten generell. Verschiedene IKT-Anwendungen sind aufgrund ihrer Kritikalität aber von spezieller Bedeutung. Dazu gehören insbesondere industrielle Kontrollsysteme (engl. Industrial Control Systems, ICS). Das Design einer wirkungsvollen ICS-Sicherheits-Architektur setzt voraus, dass die Unternehmensrisiken in Relation zu den funktionalen (operativen) Anforderungen an das ICS gestellt werden. Das kann auch die physische Welt betreffen (z. B. Perimeterschutz um Rechenzentren). Entscheidungsträger auf allen Ebenen der Organisation müssen die Bedeutung von Cyberrisiken kennen und sich aktiv in den Riskomanagementprozess einbringen. Regelmässige Risikoanalysen für ausgewählte Systeme, Applikationen und Prozesse, inklusive der zugehörigen Netzwerke, sind unabdingbar. Führen Sie diese Analysen nach strengen Vorgaben durch und verwenden Sie dabei einen strukturierten, systematischen Ansatz.

1.6.3.2 Risikomanagementframework

IKT-Risikoanalysen sollen in ein Risikomanagementframework eingebettet sein und regelmässig für klar definierte Untersuchungsobjekte durchgeführt werden, wie beispielsweise für geschäftskritische Anlagen, Prozesse und Applikationen (auch im Entwicklungsstadium) sowie deren Abhängigkeiten von weiteren Systemen, Netzen und Diensten.

Das Ziel des Risikomanagementframeworks ist es, den identifizierten Risiken verantwortliche Personen/Rollen zuzuweisen, welche die Risiken überwachen (Monitoring), beurteilen und adäquate Massnahmen umsetzen, um die Risiken innerhalb der vorgängig definierten akzeptablen Grenzen zu halten (= Risikoappetit).

1.6.3.3 Risikoanalyse

Der Untersuchungsbereich der IKT-Risikoanalyse soll klar definiert sein. Die betroffenen Geschäftsprozesse und die betreffenden technischen Elemente sowie mögliche externe Faktoren müssen beschrieben werden und ihre Gewichtung in der Analyse definiert sein. Damit werden auch die Inhalte und Grenzen der Analyse definiert.

1.6.4 Business Impact Analyse

Im Rahmen einer Business Impact Analyse sollen die potenziell realistische und die potenziell schlimmste Auswirkung (auf die Geschäftstätigkeit) der Kompromittierung einer IKT-Komponente (inkl. Personen, Daten, Prozessen, Diensten, Netzen) für unterschiedliche Kategorien erhoben werden (z. B. finanziell, operativ, rechtlich, reputabel, gesundheitlich).

Schlussendlich muss festgelegt werden, welche Auswirkungen auf die Geschäftstätigkeit das Unternehmen zu tragen bereit ist, falls die dafür notwendigen IKT-Ressourcen nicht wie vorgesehen verfügbar sind. Entsprechend sind die Anforderungen und Schutzniveaus zu definieren, welche notwendig sind, um die Verfügbarkeit, Integrität und Vertraulichkeit der identifizierten IKT-Ressourcen gemäss dem tragbaren Risiko zu gewährleisten.

1.6.5 Massnahmen

Die Massnahmen zu den in der Business Impact Analyse beschriebenen Risiken sollen identifiziert, überprüft und freigegeben werden. Diese sollen zusammen mit den Plänen zum exakten Vorgehen durch die Geschäftsleitung freigegeben werden.

Dabei soll berücksichtigt werden, dass das Restrisiko für alle Betriebsmittel im relevanten Umfeld ermittelt und in geeigneter Weise (z. B. gemildert, vermieden, übertragen oder akzeptiert) gemäss dem Risikoappetit behandelt wird.

Für jedes einzelne individuelle Betriebsmittel (engl. asset) soll so das maximal zulässige Risiko bestimmt werden, so dass die (kumulierten) IKT-Risiken kalkuliert werden können.

1.6.6 Cybersecurity-Architektur

Die Cybersecurity-Architektur umfasst die spezifischen Massnahmen und ihre strategische Platzierung innerhalb des Netzwerks zur Etablierung einer Sicherheitsschicht im Sinne der Defense-in-Depth-Strategie. Sie soll zudem Informationen zum Datenfluss zwischen allen Systemen und deren Verbindungen ermöglichen. Ebenso soll die Cybersecurity-Architektur mit dem

physischen Inventar der Anlagen und IKT-Betriebsmittel abgestimmt sein, um ein ganzheitliches Verständnis der Informationsflüsse innerhalb der Organisation sicherzustellen.

Die Cybersecurity-Architektur soll im Einklang mit dem NIST Framework Core sein. Die Cybersecurity-Architektur berücksichtigt den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Daten, Diensten und Systemen. Zur Umsetzung soll ein Implementierungsplan erstellt werden, welcher sich an der Unternehmenskultur und den strategischen Zielen orientiert, gleichzeitig aber dem Sicherheitsbedürfnis angemessen Rechnung trägt und den diesbezüglichen Ressourcenbedarf ausweist. In der Regel wird die Cybersecurity-Architektur durch einen integrierten Aufgabenplan ergänzt, der erwartete Ergebnisse (Indikationen und Auslöser für die weitere Überprüfung und Ausrichtung) identifiziert, Projektzeitpläne festlegt, Ressourcenbedarfsabschätzungen liefert und wesentliche Projektabhängigkeiten identifiziert.

1.6.7 Physische Sicherheit

Physische Sicherheitsmassnahmen reduzieren das Risiko von versehentlichen oder vorsätzlichen Verlusten oder Schäden an IKT-Betriebsmitteln der Organisation oder deren Umfeld. Zu den zu schützenden Betriebsmitteln gehören unter anderem physische Vermögenswerte wie Werkzeuge und Anlagen, die Umwelt, das erweiterte Umfeld sowie das geistige Eigentum, einschliesslich proprietärer Daten wie Prozesseinstellungen und Kundeninformationen. Physische Sicherheitskontrollen müssen häufig spezifische Umwelt-, Sicherheits-, Regulierungs-, Rechts- und sonstige Anforderungen erfüllen. Organisationen sollen physische Sicherheitskontrollen wie technische Kontrollen dem Schutzbedarf anpassen. Um einen umfassenden Schutz zu gewährleisten, beinhaltet der physische Schutz auch den Schutz von IKT-Komponenten (= Security) und Daten aus dem Umfeld, welche mit der IKT verbunden sind. Die Sicherheit an vielen IKT-Infrastrukturen ist eng mit der Anlagensicherheit (= Safety) verbunden. Dies, um Mitarbeitende aus gefährlichen Situationen herauszuhalten, ohne dass sie in ihrer Arbeit oder in Notfallverfahren behindert werden. Physische Sicherheitskontrollen sind aktive oder passive Massnahmen, die den physischen Zugriff auf alle Bestandteile der IKT-Infrastruktur begrenzen. Diese Schutzmassnahmen sollen u.a. folgende Fälle verhindern:

- Unbefugter physischer Zutritt zu sensiblen Orten
- Physische Veränderung, Manipulation, Diebstahl oder sonstige Entfernung oder Zerstörung bestehender Systeme, Infrastruktur, Kommunikationsschnittstellen oder physischer Standorte
- Unbefugte Beobachtung von sensiblen Anlagen durch visuelle Betrachtung, Fotografien oder jede andere Art von Aufzeichnungen
- Die unerlaubte Einführung/Installation von neuen Systemen, Infrastruktur, Kommunikationsschnittstellen oder anderer Hardware
- Die unerlaubte Einführung von Geräten (USB-Stick, Wireless Access Point, Bluetooth- oder Mobilgeräten), die dazu dienen, Manipulationen an Hardware vorzunehmen, die Kommunikation abzuhören oder andere schädliche Auswirkungen haben

Um den Anforderungen an die Informationssicherheit zu genügen, sind physische Betriebsmittel, einschliesslich Systemen und Netzwerkausrüstung, Bürogeräten (z.B. Netzwerkdruckern und Multifunktionsgeräten) und Spezialausrüstung (z.B. industriellen Steuerungssysteme) über ihren gesamten Lebenszyklus vom Erwerb (z.B. Kauf oder Leasing) über die Wartung bis zur Entsorgung zu schützen.

Auch mobile Geräte (einschliesslich Laptops, Tablets und Smartphones) und ihre Daten sind gegen unbefugten Zugriff, Verlust und Diebstahl zu schützen, indem Sie die Sicherheitseinstellungen konfigurieren, den Zugang beschränken, Sicherheitssoftware installieren und die Geräte zentral verwalten.

1.6.8 Hardware Lifecycle Management

Die Beschaffung (Kauf oder Leasing) von widerstandsfähiger, zuverlässiger Hardware soll immer den Sicherheitsanforderungen entsprechen. Mögliche Schwachstellen in der Hardware sollen immer identifiziert werden.

Das Ziel ist es, sicherzustellen, dass die Hardware die erforderliche Funktionalität bietet und die Sicherheit kritischer oder sensibler Informationen und Systeme über den gesamten Lifecycle hinweg nicht beeinträchtigt.

1.6.9 Mobile Device Konfiguration

Um Daten vor unbefugtem Zugriff, Verlust und Diebstahl zu schützen, sollen mobile Geräte (einschliesslich Laptops, Tablets und Smartphones) immer über eine Standardkonfiguration verfügen, welche den Sicherheitsanforderungen entspricht.

Ziel der Standardkonfiguration ist es, auch bei Verlust oder Diebstahl die Informationssicherheit von gespeicherten oder übermittelten Daten auf dem mobilen Gerät zu gewährleisten.

1.6.10 Industrielle Kontrollsysteme

Industrielle Kontrollsysteme (engl: «Industrial Control Systems», ICS) müssen ihrem Schutzbedarf entsprechend überwacht und kontrolliert werden. Insbesondere zur Sicherstellung von versorgungsrelevanten Prozessen müssen diese Systeme technisch und physisch besonders geschützt werden.

1.6.11 ICS-Netzwerk-Architektur

Beim Entwerfen einer Netzwerkarchitektur empfiehlt es sich in der Regel, ICS-Netzwerke vom Firmennetzwerk zu trennen. Die Art des Datenverkehrs auf diesen beiden Netzwerken ist unterschiedlich: Internet-Zugang, FTP, E-Mail und Remote-Zugriff werden in der Regel im Firmennetzwerk erlaubt, hingegen im ICS-Netzwerk nicht. Wenn ICS-Daten auf dem Firmennetzwerk übertragen werden, könnten diese abgefangen oder DDoS- oder Man-in-the-Middle-Attacken ausgesetzt werden. Durch die getrennte oder stark eingeschränkte Konnektivität zwischen dem Firmennetzwerk und dem ICS-Netzwerk können Sicherheits- und Leistungsprobleme im ICS-Netzwerk minimiert werden.

1.6.12 ICS-Netzwerk-Perimeter-Security

Die Kosten einer ICS-Installation und die Aufrechterhaltung einer homogenen Netzwerkinfrastruktur bedeuten oft, dass eine Verbindung zwischen dem ICS- und dem Firmennetzwerk erforderlich ist. Diese Verbindung stellt ein erhebliches Sicherheitsrisiko dar und sollte technisch geschützt werden. Wenn die Netzwerke verbunden werden müssen, wird dringend empfohlen, dass nur minimale (wenn möglich einzelne) Verbindungen erlaubt werden, und dass die Verbindung über eine Firewall und eine DMZ (separates Netzwerksegment) erfolgt. ICS-Server, welche Daten aus dem Firmennetzwerk enthalten, müssen in eine DMZ gestellt werden. Externe Verbindungen müssen bekannt sein und auf einen minimalen Zugriff über die Firewall beschränkt werden. Der Datenaustausch kann zusätzlich durch Systeme, welche Anomalien zu erkennen vermögen, überwacht und plausibilisiert werden.

1.6.13 Host Security

Auf Host- resp. Workstation-Ebene muss eine weitere Sicherheitsschicht implementiert werden. Firewalls schützen die meisten Geräte gegen das Eindringen von aussen. Allerdings erfordert ein gutes Sicherheitsmodell mehrstufige Verteidigungsschichten. Zur vollständigen Sicherung des Netzwerks gehört auch die Sicherung aller Hosts. Eine solche Schicht für die Host-Sicherheit soll einem Benutzer ermöglichen, verschiedene Betriebssysteme und Anwendungen zu nutzen, während sie einen adäquaten Schutz der Geräte sicherstellt.

Es müssen ein Konzept zu Passwortrichtlinien für alle Benutzer auf einem System erstellt werden sowie die bekannten Accounts (wie z. B. «Administrator») umbenannt werden. Restriktive Passwortrichtlinien werden von den Anwendern möglicherweise unterlaufen, indem die Passwörter unsicher aufbewahrt werden (z. B. auf Notizzetteln), oder die Anwender immer wieder ähnliche Passwörter verwenden. Die Komplexität der Passwortbestimmungen soll der Berechtigungsstufe der Anwender angemessen sein. Optional können Zyklen zum Wechsel der Passwörter definiert werden.

Die folgenden allgemeinen Empfehlungen sollen durch die Organisationen für jeden ICS-Host und jedes Gerät, das Zugriff auf das Unternehmensnetzwerk hat, umgesetzt werden (unabhängig vom Betriebssystem):

- Installation und Konfiguration einer Host-basierten Firewall
- Bildschirmschoner mit kurzen Intervallen und Aufforderung zur Passworteingabe sollen nach Möglichkeit eingerichtet werden
- Betriebssysteme müssen gepatcht und die Firmware aktuell gehalten werden
- Die Konfiguration von Logs muss auf allen Geräten aktiviert sein
- Nicht benützte Services und Accounts müssen deaktiviert werden
- Nicht sichere Services, wie Telnet, Remote Shell oder rlogin, müssen durch sichere Alternativen wie SSH ersetzt werden
- Benutzer sollten nicht in der Lage sein, Services zu deaktivieren
- Backups von Systemen müssen gemacht und geprüft werden, besonders, wenn diese nicht zentral gesteuert werden
- Vom Betriebssystem bereitgestellte Sicherheitsmodule, wie z. B. Sicherheitsscanner, sollten aktiviert oder durch eine adäquate Software ersetzt werden
- Für Laptops und andere mobile Geräte, welche nicht durchgehend mit dem Firmennetz verbunden sind, gelten die gleichen Richtlinien. Zusätzlich soll jedoch bei mobilen Geräten die Harddisk verschlüsselt werden

1.6.14 Security-Monitoring

Der Einsatz von Monitoring-Systemen und Netzwerk-Komponenten, welche anomale Verhaltensweisen und Angriffssignaturen erkennen, bringt zusätzliche Komplexität in eine IT- oder ICS-Umgebung. Allerdings sind die Überwachungs- und Erkennungsfunktionen für das Defense-in-Depth-Konzept zum Schutz kritischer Betriebsmittel unerlässlich. Um kritische Assets vor unbefugtem Zugriff zu schützen, reicht eine elektronische Grenze um das ICS-Netzwerk nicht aus. Nach dem Defense-in-Depth-Konzept soll ein Monitoring-System eine Organisation bei einem

Sicherheitsvorfall frühzeitig alarmieren. Die meisten Organisationen haben ein gewisses Standard-Monitoring in der IT-Umgebung, das sie aber mehrheitlich nicht in den ICS-Netzwerken einsetzen.

Unerlässlich ist:

- die Durchführung gründlicher, unabhängiger und regelmässiger Audits des Sicherheitsstatus (kritische Geschäftsumgebungen, Prozesse, Anwendungen und unterstützende Systeme/Netzwerke)
- die Überwachung der Informationsrisiken, die Einhaltung der sicherheitsrelevanten Elemente der rechtlichen, regulatorischen und vertraglichen Anforderungen sowie die regelmässige Berichterstattung über die Informationssicherheit an die Geschäftsleitung

1.6.15 Informationssicherheitsstrategie

Die Definition, Aufrechterhaltung und Überwachung einer umfassenden Informationssicherheitsstrategie ermöglichen es der Geschäftsleitung, klare Richtlinien zu setzen und unterstützt sie sowohl bei der Durchsetzung von Vorgaben als auch im Risikomanagement.

1.6.16 Lieferantenmanagement

Das Lieferantenmanagement befasst sich mit der Identifizierung und der Verwaltung von Informationsrisiken zu externen Anbietern (d.h. Lieferanten von Hard- und Software, Outsourcing-Anbietern und Cloud-Service-Anbietern etc.). Durch die Implementierung von Informationssicherheitsanforderungen in formale Verträge sollen die Risiken minimiert werden.

1.6.17 Das Element Mensch

Die von Menschen verursachten Fehlmanipulationen stellen Organisationen vor zahlreiche Herausforderungen. Technische Massnahmen können mutwillige oder unbedarfte Fehlmanipulationen nie vollständig ausschliessen. Unternehmen sind umso fehleranfälliger, je grösser ihr Anteil an unerfahrenen oder unqualifizierten Mitarbeitern ist. Auch die Bekämpfung von Aktivitäten von Insidern mit bösartigen Absichten stellt eine weitere Herausforderung dar. Im Umgang mit diesen Herausforderungen sind Unternehmen gehalten, sich mit den nachfolgenden Themen zu befassen.

1.6.17.1 Beschäftigungszyklus von Mitarbeitenden

Informationssicherheit soll Teil des gesamten Beschäftigungszyklus sein, von der Einstellung bis zum Austritt. Dazu gehören sicherheitsrelevante Massnahmen bspw. bei der Übertragung von Arbeitsmitteln (Hardware, Zugang zu Systemen) oder beim Zutritt von Gebäuden/Räumlichkeiten und der damit einhergehenden Schutzverantwortung. Ein entsprechendes Schulungsprogramm für Mitarbeitende soll einerseits das Sicherheitsbewusstsein fördern, andererseits das Sicherheitsverhalten definieren. Der Stand und die Durchführung der Schulungen sollen durch die Organisation dokumentiert werden.

Ziel ist es, sicherzustellen, dass die Mitarbeitenden mit den Fähigkeiten, Kenntnissen und Werkzeugen ausgestattet sind, um die Werte der Organisation zu unterstützen und die Informationssicherheitsrichtlinien einzuhalten.

1.6.17.2 Weisungen/Richtlinien

Klare, umsetzbare Weisungen und Richtlinien für Mitarbeitende regeln ihr Verhalten im Umgang mit sicherheitsrelevanten Themen. Sie setzen einen Rahmen und ermöglichen Kontrollen mit dem Ziel, Systeme zu schützen und die Richtlinien durchzusetzen. Sie legen zudem Verfahren fest und definieren die Erwartungen der Organisation an ihre Mitarbeitenden. Richtlinien und Weisungen definieren, was eingehalten werden muss, und wie Verletzungen sanktioniert werden.

1.6.17.3 Prozesse

Sicherheitsmanagement ist in der Verantwortung der IT-Sicherheitsorganisation und prozessual organisiert. Ihre Funktion ist der Schutz von Unternehmensinformationen und -daten. Organisationen sind gehalten, Sicherheitsmanagementprozesse auch auf industrielle Kontrollsysteme anzuwenden. Dazu gehört die Definition von Prozessen, wie Verfahren durchgeführt oder ein bestimmtes System konfiguriert werden sollen. Diese Prozesse sollten standardisiert und wiederholbar sein. So werden neue Mitarbeitende stets auf gleichbleibendem Sicherheitsniveau geschult, und es kann sichergestellt werden, dass alle erforderlichen Vorschriften und Standards bekannt sind. Der Prozess zur Erkennung eines Cyberincidents (Intrusion Detection) ist von besonderer Bedeutung. Im Umgang mit herstellerspezifischen Protokollen und Legacy-Systemen sind netzwerkbasierte Sicherheitsverfahren besonders wichtig.

1.6.17.4 Aufgaben und Verantwortlichkeiten in kritischen Geschäftsumgebungen

Aufgaben und Verantwortlichkeiten in kritischen Geschäftsumgebungen, Prozessen, Anwendungen (einschliesslich unterstützender Systeme/Netzwerke) und Informationen sollten klar definiert und kompetenten Personen zugewiesen werden.

Ziel ist es, bei den Mitarbeitenden ein individuelles Verantwortungsbewusstsein zu schaffen. Die so etablierte Unternehmenskultur trägt dazu bei, dass Mitarbeitende ihre Aufgaben unter Berücksichtigung der Informationssicherheit wahrnehmen.

1.6.17.5 Kommunikation/Security Awareness Programm

Ein Security Awareness Programm und eine damit verbundene Kommunikation fördern das Bewusstsein und das gewünschte Verhalten aller Mitarbeitenden über sämtliche Hierarchiestufen der Unternehmung.

Ziel ist eine Unternehmenskultur, welche das individuell gewünschte Sicherheitsverhalten fördert. Jeder Einzelne soll in seinem persönlichen Wirkungsradius befähigt sein, risikobasierte Entscheidungen zu treffen.

1.7 NIST Framework

Ziel des NIST Framework und seinen Empfehlungen ist es, den Betreibern von kritischen Infrastrukturen und weiteren von IKT abhängigen Organisationen ein Instrument zur Verfügung zu stellen, mit dem diese selbständig und eigenverantwortlich ihre Resilienz gegenüber IKT-Sicherheitsrisiken erhöhen können. Das Framework basiert auf einer Auswahl an existierenden Standards, Richtlinien und Best-Practice-Vorgaben und ist technologieneutral.

1.7.1 NIST Framework Core

Das NIST Framework Core ist risikobasiert. Es besteht aus fünf Funktionen:

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

1.7.2 Implementation Tiers

Das NIST Framework kennt vier Implementation Tiers (dt. «Stufen»). Diese beschreiben die Ausbaustufe (Schutzniveau), welche ein Unternehmen umgesetzt hat. Sie reichen von teilweise (Tier 1) bis dynamisch (Tier 4). Zur Festlegung des eigenen Schutzniveaus (Tier Level) soll eine Organisation ihre Risikomanagementpraktiken, die Bedrohungsumgebung sowie rechtliche und regulatorische Anforderungen, Geschäftsziele und organisatorischen Vorgaben genau kennen.

2 Teil 2 – Umsetzung

2.1 Übersicht

Dieses Kapitel beschreibt die auszuführenden Aufgaben zur Umsetzung des IKT-Minimalstandards. Sie sind gegliedert nach den fünf Funktionen des NIST Framework Core (siehe 1.7.1). Die fünf Funktionen heissen Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen. Die englischen Originalbezeichnungen aus dem NIST Framework Core sind jeweils zusätzlich angefügt. Die auszuführenden Aufgaben (siehe untenstehende Tabelle) werden wie folgt kategorisiert:

Die ersten beiden Buchstaben (z. B. «ID» = «Identify») bezeichnen jeweils eine der fünf Funktionen. Das zweite Buchstabenpaar bezeichnet die Kategorie (z. B. «AM» = «Asset Management»). Die Nummer bezeichnet schliesslich die einzelne Aufgabe. Sie sind innerhalb der Kategorie fortlaufend nummeriert. Lesebeispiel: «ID.AM-1» entspricht der ersten Aufgabe in der Kategorie «Asset Management» der Funktion «Identify».

Jeder Tabelle mit Aufgaben aus dem NIST Framework Core ist eine zusätzliche Tabelle mit Referenzen zu anderen internationalen IKT-Standards beigefügt. Die Tabellen referenzieren jeweils auf die Kategorie, z. B. «Asset Management». Dies soll Anwendern, die ihre IKT-Sicherheitsaufgaben nach anderen Standards organisieren, die Zuordnung erleichtern.

2.2 Identifizieren (Identify)

2.2.1 Inventar Management (Asset Management)

Die Daten, Personen, Geräte, Systeme und Anlagen einer Organisation sind identifiziert, katalogisiert und bewertet. Die Bewertung soll ihrer Kritikalität hinsichtlich der zu erfüllenden Geschäftsprozesse sowie der Risikostrategie der Organisation entsprechen.

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

Tabelle 3: Aufgaben ID.AM

Standard	Referenz
CCS CSC 1	1, 2
COBIT 5	BAI09.01, BAI09.02, BAI09.05, DSS05.02, APO02.02, APO03.03, APO03.04, PO01.02, DSS06.03
ISA 62443-3:2013	SR 7.8
ISO 27001:2013	A.6.1.1, A.8.1.1, A.8.1.2, A.8.2.1, A.11.2.6
NIST-SP-800-53 Rev. 4	AC-4, CA-3, CA-9, PL-8, CM-8, AC-20, SA-9, CP-2, RA-2, SA-14, CP-2, PS-7, PM-11
BSI 100-2	M 2.225, M 2.393, B 2.10, M 2.193

Tabelle 4: Referenzen ID.AM

2.2.2 Geschäftsumfeld (Business Environment)

Die Ziele, Aufgaben und Aktivitäten des Unternehmens sind priorisiert und bewertet.
Diese Informationen dienen als Grundlage für die Zuweisung der Verantwortlichkeiten.

Bezeichnung	Aufgabe
ID.BE-1	Identifizieren, dokumentieren und kommunizieren Sie die exakte Rolle Ihres Unternehmens innerhalb der (kritischen) Versorgungskette.
ID.BE-2	Die Bedeutung der Organisation als kritische Infrastruktur und ihre Position innerhalb des kritischen Sektors ist identifiziert und kommuniziert.
ID.BE-3	Die Ziele, Aufgaben und Aktivitäten innerhalb der Organisation sind bewertet und priorisiert.
ID.BE-4	Bciąohjhlfjufo voe Isjujtdif Gvolujpofo gîs Isjujtdif Ejfotumfjtuvohfo tjoe fubcmjfsu/
ID.BE-5	Sftjmjfo{ Bogpsefsvohfo gîs Isjujtdif Ejfotumfjtuvohfo tjoe fubcmjfsu/

Tabelle 5: Aufgaben ID.BE

Standard	Referenz
CCS CSC 1	1, 2
COBIT 5	BAI09.01, BAI09.02, BAI09.05, DSS05.02, APO02.02, APO03.03, APO03.04, PO01.02, DSS06.03
ISA 62443-3:2013	SR 7.8
ISO 27001:2013	A.6.1.1, A.8.1.1, A.8.1.2, A.8.2.1, A.11.2.6
NIST-SP-800-53 Rev. 4	AC-4, CA-3, CA-9, PL-8, CM-8, AC-20, SA-9, CP-2, RA-2, SA-14, CP-2, PS-7, PM-11
BSI 100-2	B 1.11, M 2.256, B 2.2, B 2.12, M 2.214

Tabelle 6: Referenzen ID.BE

2.2.3 Vorgaben (Governance)

Die Governance regelt Zuständigkeiten, überwacht und stellt sicher, dass regulatorische, rechtliche und operationelle Anforderungen aus dem Geschäftsumfeld eingehalten werden.

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

Tabelle 7: Aufgaben ID.GV

Standard	Referenz
COBIT 5	APO01.03, EDM01.01, EDM01.02, APO13.02, MEA03.01, MEA03.04, DSS04.02
ISA 62443-3:2013	
ISO 27001:2013	A.5.1.1, A.6.1.1, A.7.2.1, A.18.1
NIST-SP-800-53 Rev. 4	PM-1, PS-7, PM-9, PM-11
BSI 100-2	M 2.192, M 2.193, M 2.336, B 1.16

Tabelle 8: Referenzen ID.GV

2.2.4 Risikoanalyse (Risk Assessment)

Die Organisation kennt die Auswirkungen von Cyber-Risiken auf die Geschäftstätigkeit, auf Betriebsmittel und Individuen, inklusive Reputationsrisiken.

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

Tabelle 9: Aufgaben ID.RA

Standard	Referenz
COBIT 5	APO12.01, APO12.02, APO12.03, APO12.04, APO 12.05, APO 13.02, DSS04.02
ISA 62443-3:2013	4.2.3, 4.2.3.9, 4.2.3.12
ISO 27001:2013	A.12.6.1, A.18.2.3, A.6.1.4
NIST-SP-800-53 Rev. 4	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5, PM-15, PM-16, SI-5, RA-3, SI-5, PM-12, RA-2, PM-9, PM-11, SA-14
BSI 100-2	M 2.35, M 2.199, M 2.546

Tabelle 10: Referenzen ID.RA

2.2.5 Risikomanagementstrategie (Risk Management Strategy)

Legen Sie die Prioriäten, Einschränkungen und maximal tragbaren Risiken Ihrer Organisation fest. Beurteilen Sie Ihre operativen Risiken auf dieser Grundlage.

Bezeichnung	Aufgabe
ID.RM-1	Etablieren Sie Risikomanagementprozesse, bewirtschaften Sie diese aktiv und lassen Sie sich diesen von den beteiligten Personen/Anspruchsgruppen bestätigen.
ID.RM-2	Definieren und kommunizieren Sie die maximal tragbaren Risiken Ihrer Organisation.
ID.RM-3	Stellen Sie sicher, dass die maximal tragbaren Risiken unter Berücksichtigung der Bedeutung Ihrer Organisation als Betreiber einer kritischen Infrastruktur bewertet werden. Berücksichtigen Sie dazu auch die sektorspezifischen Risikoanalysen.

Tabelle 11: Aufgaben ID.RM

Standard	Referenz
COBIT 5	APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02, APO12.06
ISA 62443-3:2013	4.3.4.2, 4.3.2.6.5
ISO 27001:2013	
NIST-SP-800-53 Rev. 4	PM-8, PM-9, PM-11, SA-14

Tabelle 12: Referenzen ID.RM

2.2.6 Lieferketten-Risikomanagement (Supply Chain Riskmanagement)

Legen Sie die Prioritäten, Einschränkungen und maximalen Risiken fest, die Ihre Organisation in Zusammenhang mit Lieferantenrisiken zu tragen gewillt ist.

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

Tabelle 13: Aufgaben ID.SC

Standard	Referenz
COBIT 5	APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05
ISA 62443-3:2013	4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14, 4.3.2.6., 4.3.2.5.7, 4.3.4.5.11 7
ISO 27001:2013	A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2, A.15.2.1, A.15.2.2, A.17.1.3
NIST-SP-800-53 Rev. 4	SA-9, SA-12, PM-9, RA-2, RA-3, SA-12, SA-14, SA-15, SA-11, CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
BSI	B 1.11, B 1.17, M 2.256, B 1.3

Tabelle 14: Referenzen ID.SC

2.3 Schützen (Protect)

2.3.1 Zugriffsmanagement und -steuerung (Access Control)

Stellen Sie sicher, dass der physische und logische Zugriff auf IKT-Betriebsmittel und -Anlagen nur für autorisierte Personen, Prozesse und Geräte möglich ist, und dass der Zugriff nur für zulässige Aktivitäten möglich ist.

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

Tabelle 15: Aufgaben PR.AC

Standard	Referenz
COBIT 5	DSS05.04, DSS06.03, DSS01.04, DSS05.05, APO13.01, DSS01.04, DSS05.03, DSS05.04, DSS05.05, DSS05.07, DSS06.03, BAI08.03
ISA 62443-3:2013	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.13, SR 2.1, SR 2.6, SR 3.1, SR 3.8, SR 2.2, SR 2.3
ISO 27001:2013	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3, A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.6.1.2, A.7.1.1, A.9.1.2, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6, A.9.4.1, A.9.4.4
NIST-SP-800-53 Rev. 4	AC-2, IA Family, PE-2, PE-3, PE-4, PE-5, PE-6, PE-9, AC-17, AC-19, AC-20, AC-2, AC-3, AC-5, AC-6, AC-16, AC-24, IA-2, IA-4, IA-5, IA-8
BSI	M 2.30, M 2.220, M 2.11, M 4.15, M 1.79, M 2.17, B 2.2, B 2.12, B 5.8, B 4.1, M 2.393, M 2.5, B 1.18, M 2.220, M 2.8, M 4.135, B 4.1, M 5.77, M 2.393, M 2.5, M 3.33, M 2.31, M 2.586, M 4.135

Tabelle 16: Referenzen PR.AC

2.3.2 Sensibilisierung und Ausbildung

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

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

Tabelle 17: Aufgaben PR.AT

Standard	Referenz
COBIT 5	APO07.03, BAI05.07, APO07.02, DSS06.03, APO07.03, APO10.04, APO10.05
ISA 62443-3:2013	4.3.2.4.2, 4.3.2.4.3
ISO 27001:2013	A.7.2.2, A.6.1.1
NIST-SP-800-53 Rev. 4	AT-2, AT-3, PM-13, PS-7, SA-9, AT-3, PM-7
BSI	M 2.193, B 1.13

Tabelle 18: Referenzen PR.AT

2.3.3 Datensicherheit (Data Security)

Stellen Sie sicher, dass Informationen, Daten und Datenträger so gemanaged werden, dass die Vertraulichkeit, Integrität und Verfügbarkeit der Daten gemäss der Risikostrategie der Organisation geschützt werden.

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

Tabelle 19: Aufgaben PR.DS

Standard	Referenz
COBIT 5	APO01.06, BAI02.01, BAI06.01, DSS06.06, BAI09.03, APO13.01, BAI07.04, BAI03.05.4
ISA 62443-3:2013	SR 3.4, SR 4.1, SR 3.1, SR 3.8, SR 4.1, SR 4.2, SR 7.1, SR 7.2, SR 5.2
ISO 27001:2013	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7, A.12.3.1, A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3
NIST-SP-800-53 Rev. 4	SC-28, SC-8, CM-8, MP-6, PE-16, AU-4, CP-2, SC-5, AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4, SI-7, CM-2, SA-10
BSI	M 2.217, B 4.1, M 2.393, B 5.3, B 5.4, B 5.21, B 5.24, B 1.7, M 2.3, B 1.15, M 5.23, M 3.33, M 2.226, M 3.2, M 3.6, B 1.18, M 2.220, M 2.8, M 4.135, M 4.494, M 5.77, M 2.393, B 5.3, M 3.55, B 5.4, B 5.21, B 5.24, B 1.7, B 1.6, B 1.9, B 5.4, B 5.21, B 5.24, M 2.62, M 2.4

Tabelle 20: Referenzen PR.DS

2.3.4 Informationsschutzrichtlinien (Information Protection Processes and Procedures)

Erstellen Sie Richtlinien zum Schutz von Informationssystemen und Betriebsmitteln.
Nutzen Sie diese Richtlinien, um die Informationssysteme und Betriebsmittel zu schützen.

Bezeichnung	Aufgabe
PR.IP-1	Erstellen Sie eine Standardkonfiguration für die Informations- und Kommunikationsinfrastruktur sowie für die industriellen Kontrollsysteme. Stellen Sie sicher, dass diese Standardkonfiguration typische Security-Prinzipien (z. B. N-1-Redundanz, Minimalkonfiguration etc.) einhält.
PR.IP-2	Etablieren Sie einen Lebenszyklus-Prozess für den Einsatz von IKT-Betriebsmitteln.
PR.IP-3	Etablieren Sie einen Prozess zur Kontrolle von Konfigurationsänderungen.
PR.IP-4	Stellen Sie sicher, dass Sicherungen (Backups) Ihrer Informationen regelmässig durchgeführt, bewirtschaftet und getestet werden (Rückspielbarkeit der Backups testen).
PR.IP-5	Stellen Sie sicher, dass Sie alle (regulatorischen) Vorgaben und Richtlinien hinsichtlich den physischen Betriebsmitteln erfüllen.
PR.IP-6	Stellen Sie sicher, dass Daten gemäss den Vorgaben vernichtet werden.
PR.IP-7	Stellen Sie sicher, dass Ihre Prozesse zur Informationssicherheit kontinuierlich weiterentwickelt und verbessert werden.
PR.IP-8	Tauschen Sie sich bezüglich der Effektivität verschiedener Schutztechnologien mit Ihren Partnern aus.
PR.IP-9	Etablieren Sie Prozesse zur Reaktion auf eingetretene Cyber-Vorfälle (Incident Response-Planning, Business Continuity Management, Incident Recovery, Disaster Recovery).
PR.IP-10	Testen Sie die Reaktions- und Wiederherstellungspläne.
PR.IP-11	Etablieren Sie Aspekte der Cybersecurity bereits in den Personalrekrutierungsprozess (z. B. durch die Etablierung von Background-Checks/Personensicherheitsprüfungen).
PR.IP-12	Entwickeln und implementieren Sie einen Prozess zum Umgang mit erkannten Schwachstellen.

Tabelle 21: Aufgaben PR.IP

Standard	Referenz
COBIT 5	BAI10.01, BAI10.02, BAI10.03, BAI10.05, APO13.01, BAI06.01, BAI01.06, APO13.01, DSS01.04, DSS05.05, BAI09.03, APO11.06, DSS04.05, DSS04.03, APO07.01, APO07.02, APO07.03, APO07.04, APO07.05
ISA 62443-3:2013	SR 7.6
ISO 27001:2013	A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5, A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4, A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3, A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3, A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7, A.16.1.6, A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3, A.12.6.1, A.18.2.2
NIST-SP-800-53 Rev. 4	CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8, CP-4, CP-6, CP-9, PE-10, PE-12, PE-13, PE-14, PE-15, PE-18, MP-6, A-2, CA-7, CP-2, IR-8, PL-2, PM-6, AC-21, CA-7, SI-4, CP-2, IR-8, IR-3, PM-14, RA-3, RA-5, SI-2
BSI	B 1.4, B 1.3, M 2.217, B 1.14, B 1.9, M 2.62, B 5.27, M 4.78, M 2.9, B 1.0, M 2.80, M 2.546, B 5.27, B 5.21, B 5.24

Tabelle 22: Referenzen PR.IP

2.3.5 Unterhalt (Maintenance)

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

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

Tabelle 23: Aufgaben PR.MA

Standard	Referenz
COBIT 5	BAI09.03, DSS05.04, APO11.04, DSS05.02, APO13.01
ISA 62443-3:2013	
ISO 27001:2013	A.11.1.2, A.11.2.4, A.11.2.5, A.15.1.1, A.15.2.1
NIST-SP-800-53 Rev. 4	MA-2, MA-3, MA-4, MA-5
BSI	M 2.17, M 2.4, M 2.218, M 2.4, B 1.11, B 1.17, M 2.256

Tabelle 24: Referenzen PR.MA

2.3.6 Einsatz von Schutztechnologie (Protective Technology)

Installieren Sie technische Security-Lösungen, um die Sicherheit und Resilienz Ihrer IKT-Systeme und Ihrer Daten gemäss den Vorgaben und Prozessen zu garantieren.

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

Tabelle 25: Aufgaben PR.PT

Standard	Referenz
COBIT 5	APO11.04, DSS05.02, APO13.01, BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05
ISA 62443-3:2013	SR 2.3, SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.4, SR 2.5, SR 2.6, SR 2.7, SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.2, SR 7.6
ISO 27001:2013	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9, A.9.1.2, A.13.1.1, A.13.2.1, A.17.1.2, A.17.2.1
NIST-SP-800-53 Rev. 4	AU Family, MP-2, MP-4, MP-5, MP-7, AC-3, CM-7, AC-4, AC-17, AC-18, CP-8, SC-7, CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6
BSI	B 5.22, M 2.500, M 2.220, M 2.64, M 4.227, M 2.64, B 1.18, B 4.1, M 2.393, B 1.3, B 2.4, B 2.9

Tabelle 26: Referenzen PR.PT

2.4 Erkennen (Detect)

2.4.1 Auffälligkeiten und Vorfälle (Anomalies and Events)

Stellen Sie sicher, dass Auffälligkeiten (abnormes Verhalten) und sicherheitsrelevante Ereignisse zeitgerecht erkannt werden und potenzielle Auswirkungen des Vorfalls verstanden werden.

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

Tabelle 27: Aufgaben DE.AE

Standard	Referenz
COBIT 5	DSS03.01, APO12.06
ISA 62443-3:2013	SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2
ISO 27001:2013	
NIST-SP-800-53 Rev. 4	AC-4, CA-3, CM-2, SI-4, AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
BSI	B 1.8

Tabelle 28: Referenzen DE.AE

2.4.2 Überwachung (Security Continous Monitoring)

Stellen Sie sicher, dass das IKT-System inkl. aller Betriebsmittel in regelmässigen Intervallen überwacht wird, um einerseits Cybersecurity-Vorfälle zu entdecken und anderseits die Effektivität der Schutzmassnahmen überprüfen zu können.

Bezeichnung	Aufgabe
DE.CM-1	Etablieren Sie ein kontinuierliches Netzwerkmonitoring, um potentielle Cybersecurity-Vorfälle zu entdecken.
DE.CM-2	Etablieren Sie ein kontinuierliches Monitoring/Überwachung aller physischen Betriebsmittel und Gebäude, um Cybersecurity-Vorfälle entdecken zu können.
DE.CM-3	Etablieren Sie ein Monitoring der IKT-Nutzung der Mitarbeitenden, um potentielle Cybersecurity-Vorfälle zu entdecken.
DE.CM-4	Stellen Sie sicher, dass Schadsoftware entdeckt werden kann.
DE.CM-5	Stellen Sie sicher, dass Schadsoftware auf Mobilgeräten entdeckt werden kann.
DE.CM-6	Stellen Sie sicher, dass die Aktivitäten von externen Dienstleistern überwacht werden, so dass Cybersecurity-Vorfälle entdeckt werden können.
DE.CM-7	Überwachen Sie ihr System laufend, um sicherzustellen, dass Aktivitäten/Zugriffe von unberechtigten Personen, Geräten und Software erkannt werden.
DE.CM-8	Führen Sie Verwundbarkeitsscans durch.

Tabelle 29: Aufgaben DE.CM

Standard	Referenz
COBIT 5	DSS05.01, DSS05.07, APO07.06, BAI03.10
ISA 62443-3:2013	SR 6.2, SR 3.2, SR 2.4
ISO 27001:2013	A.12.4.1, A.12.2.1, A.12.5.1, A.14.2.7, A.15.2.1, A.12.6.1
NIST-SP-800-53 Rev. 4	AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4, AU-13, CM-10, CM-11, SI-3, SC-18, SI-4, SC-44, PS-7, SA-4, SA-9, CM-8, PE-3, PE-6, PE-20, SI-4, AU-12, RA-5
BSI	B 5.22, M 2.500, B 1.6, B 2.9, B 1.9, B 5.25, B 1.11, M 2.256, M 2.35

Tabelle 30: Referenzen DE.CM

2.4.3 Detektionsprozess (Detection Processes)

Prozesse und Handlungsanweisungen zur Detektion von Cybersecurity-Vorfällen werden gepflegt, getestet und unterhalten.

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

Tabelle 31: Aufgaben DE.DP

Standard	Referenz
COBIT 5	DSS05.01, APO13.02, APO12.06, APO11.06, DSS04.05
ISA 62443-3:2013	SR 3.3, SR 6.1
ISO 27001:2013	A.6.1.1, A.18.1.4, A.14.2.8, A.16.1.2, A.16.1.6
NIST-SP-800-53 Rev. 4	CA-2, CA-7, PM-14, SI-3, SI-4, AU-6, CA-2, CA-7, RA-5
BSI	M 2.193, M 2.568, B 1.8

Tabelle 32: Referenzen DE.DP

2.5 Reagieren (Respond)

2.5.1 Reaktionsplanung (Response Planning)

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

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

Tabelle 33: Aufgaben RS.RP

Standard	Referenz
COBIT 5	BAI01.10
ISA 62443-3:2013	
ISO 27001:2013	A.16.1.5
NIST-SP-800-53 Rev. 4	CP-2, CP-10, IR-4, IR-8
BSI	B 1.8

Tabelle 34: Referenzen RS.RP

2.5.2 Kommunikation (Communications)

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

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

Tabelle 35: Aufgaben RS.CO

Standard	Referenz
COBIT 5	
ISA 62443-3:2013	
ISO 27001:2013	A.6.1.3, A.16.1.2
NIST-SP-800-53 Rev. 4	CP-2, CP-3, IR-3, IR-8, CA-2, CA-7, IR-4, IR-8, PE-6, RA-5, SI-4, PM-15, SI-5
BSI	B 1.3, B 1.8, M 2.193

Tabelle 36: Referenzen RS.CO

2.5.3 Analyse (Analysis)

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

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

Tabelle 37: Aufgaben RS.AN

Standard	Referenz
COBIT 5	DSS02.07
ISA 62443-3:2013	SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1
ISO 27001:2013	A.12.4.1, A.12.4.3, A.16.1.5, A.16.1.6, A.16.1.7, A.16.1.4
NIST-SP-800-53 Rev. 4	AU-6, CA-7, IR-4, IR-5, PE-6, SI-4, CP-2, IR-4, AU-7, CP-2, IR-5, IR-8
BSI	B 5.22, M 2.500, M 2.64, B 1.8

Tabelle 38: Referenzen RS.AN

2.5.4 Schadensminderung (Mitigation)

Handeln Sie so, dass die weitere Ausbreitung eines Cybersecurity-Vorfalls verhindert und der mögliche Schaden verringert wird.

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

Tabelle 39: Aufgaben RS.MI

Standard	Referenz
COBIT 5	
ISA 62443-3:2013	SR 5.1, SR 5.2, SR 5.4, A.12.2.1, A.16.1.5
ISO 27001:2013	A.12.2.1, A.16.1.5, A.12.6.1
NIST-SP-800-53 Rev. 4	IR-4, CA-7, RA-3, RA-5
BSI	B 1.6, B 1.8, M 2.35

Tabelle 40: Referenzen RS.MI

2.5.5 Verbesserungen (Improvements)

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

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

Tabelle 41: Aufgaben RS.IM

Standard	Referenz
COBIT 5	BAI01.13
ISA 62443-3:2013	
ISO 27001:2013	A.16.1.6
NIST-SP-800-53 Rev. 4	CP-2, IR-4, IR-8
BSI	B 1.8

Tabelle 42: Referenzen RS.IM

2.6 Wiederherstellen (Recover)

2.6.1 Wiederherstellungsplanung (Recovery Planning)

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

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

Tabelle 43: Aufgaben RC.RP

Standard	Referenz
COBIT 5	DSS02.05, DSS03.04
ISA 62443-3:2013	
ISO 27001:2013	A.16.1.5
NIST-SP-800-53 Rev. 4	CP-10, IR-4, IR-8

Tabelle 44: Referenzen RC.RP

2.6.2 Verbesserungen (Improvements)

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

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

Tabelle 45: Aufgaben RC.IM

Standard	Referenz
COBIT 5	BAI05.07
ISA 62443-3:2013	
ISO 27001:2013	
NIST-SP-800-53 Rev. 4	CP-2, IR-4, IR-8

Tabelle 46: Referenzen RC.IM

2.6.3 Kommunikation (Communications)

Koordinieren Sie Ihre Wiederherstellungsaktivitäten mit internen und externen Partnern, z. B. Internet Service Providern, CERT, Behörden, Systemintegratoren etc.

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

Tabelle 47: Aufgaben RC.CO

Standard	Referenz
COBIT 5	EDM03.02
ISA 62443-3:2013	
ISO 27001:2013	
NIST-SP-800-53 Rev. 4	CP-2, IR-4

Tabelle 48: Referenzen RC.CO

3 Teil 3 – Prüfung

3.1 Einführung

Dieser Abschnitt beschreibt das Vorgehen zur periodischen Überprüfung der Vollständigkeit und Wirksamkeit der eingesetzten Massnahmen. Als Ergebnis der Überprüfung soll eine Aussage zum Reifegrad der eigenen Cybersecurity vorliegen. Diese soll eine sektorspezifische oder sektorübergreifende Vergleichbarkeit ermöglichen.

Die hier vorgestellten Massnahmen zur Verbesserung der IKT-Resilienz (vgl. Kapitel 2) bleiben wirkungslos ohne Umsetzung durch die Unternehmen. Wichtig ist, dass die Verantwortlichen die Bedeutung des Themas Cybersecurity verstehen, Mitarbeiter und Partner sensibilisiert sind und ausreichend Ressourcen zur Umsetzung eingeplant und freigegeben werden. Es wird empfohlen, die Prüfung zum vorliegenden Minimalstandard mindestens jährlich durchzuführen und notwendige Massnahmen zur Verbesserung der Resilienz möglichst umgehend umzusetzen.

Sicherheit ist kein Zustand, der erreicht werden kann. Sicherheit ist ein Prozess, der laufend ausgeführt, evaluiert, angepasst und verbessert werden muss. Cybersecurity kann nicht länger ignoriert werden. Beginnen Sie umgehend mit geeigneten Massnahmen zur Verbesserung der Resilienz Ihrer kritischen IKT-Ressourcen.

Jede der in Kapitel 2 vorgestellten Aufgaben muss dazu mit einem Wert zwischen 0 und 4 bewertet werden, siehe untenstehendes Bewertungsschema (vgl. 3.2.1). Diese Bewertungen bilden die Grundlage zur Beurteilung des Tier Levels einer Organisation (siehe Kapitel 3.3).

3.1.1 Bewertungsschema der Aufgaben

0 = Nicht umgesetzt
1 = Partiell umgesetzt, nicht vollständig definiert und abgenommen
2 = Partiell umgesetzt, vollständig definiert und abgenommen
3 = Umgesetzt, vollständig oder grösstenteils umgesetzt, statisch
4 = Dynamisch, umgesetzt, kontinuierlich überprüft, verbessert

3.2 Beschreibung der Tier Level einer Organisation

Die Tiers reichen von partiell (Tier 1) bis dynamisch (Tier 4) und beschreiben einen zunehmenden Grad an Reife. Organisationen sollen das für sie zu erreichende Tier Level bestimmen und sicherstellen, dass das ausgewählte Niveau die organisatorischen Ziele erfüllt.

Die detaillierten Beschreibungen der vier Tier Level werden im nächsten Abschnitt vorgestellt.

3.2.1 Tier 1: Partiell

Der Tier Level 1 bedeutet, dass Risikomanagementprozesse und organisatorische Vorgaben zur IKT-Sicherheit nicht formalisiert sind, und dass IKT-Risiken üblicherweise nur ad hoc oder reaktiv verwaltet werden. Ein integriertes Risikomanagementprogramm auf organisatorischer Ebene besteht, aber ein Bewusstsein für IKT-Risiken und ein organisationsweiter Ansatz zur Bewältigung dieser Risiken sind nicht etabliert. Die Organisation verfügt typischerweise nicht über Prozesse, um Informationen zur Cybersecurity innerhalb der Organisation gemeinsam zu nutzen. Ebenso verfügt die Organisation für den Fall eingetretener IKT-Risiken oft nicht über standardisierte Prozesse zum Informationsaustausch oder zur koordinierten Zusammenarbeit mit externen Partnern.

3.2.2 Tier 2: Risiko-informiert

Organisationen, die sich selber auf dem Tier Level 2 einordnen, verfügen typischerweise über Risikomanagementprozesse für IKT-Risiken. Diese sind jedoch nicht als konkrete Handlungsanweisungen implementiert. Auf der organisatorischen Ebene sind IKT-Risiken ins unternehmensweite Risikomanagement integriert, und das Bewusstsein für IKT-Risiken ist auf allen Unternehmensstufen vorhanden. Hingegen fehlen typischerweise unternehmensweite Ansätze zur Steuerung und Verbesserung des Bewusstseins (Awareness) für aktuelle und zukünftige IKT-Risiken. Genehmigte Prozesse und Verfahren sind definiert und umgesetzt. Das Personal verfügt über ausreichende Ressourcen, um seine Aufgaben im Bereich der Cybersecurity wahrzunehmen. Cybersecurity-Informationen werden innerhalb der Organisation auf informeller Basis geteilt. Die Organisation ist sich ihrer Rolle bewusst und kommuniziert mit externen Partnern zum Thema Cybersecurity (z. B. Kunden, Lieferanten, Dienstleistern etc.). Es bestehen jedoch keine standardisierten Prozesse zur Kooperation oder zum Informationsaustausch mit diesen Partnern.

3.2.3 Tier 3: reproduzierbar

Organisationen auf Tier Level 3 verfügen über formell genehmigte Risikomanagementpläne und Vorgaben zu deren unternehmensweiten Anwendung. Der Umgang mit IKT-Risiken ist in unternehmensweit gültigen Richtlinien definiert. Die standardisiert erfassten IKT-Risiken sowie die Vorgaben zum Umgang mit denselben werden regelmässig aktualisiert. Dabei werden sowohl Veränderungen der Geschäftsanforderungen berücksichtigt als auch technische Weiterentwicklungen und eine sich verändernde Bedrohungslandschaft, etwa durch neue Akteure oder ein sich wandelndes politisches Umfeld.

Prozesse und Verfahren zum Umgang mit veränderten Risiken sind schriftlich definiert. Es werden standardisierte Methoden eingesetzt, um auf Veränderungen der Risiken zu reagieren. Das Personal verfügt über die notwendigen Kenntnisse und Fähigkeiten, um seine Aufgaben zu erfüllen.

Die Organisation kennt ihre Abhängigkeiten von externen Partnern und tauscht mit diesen Informationen aus, die Managemententscheidungen innerhalb der Organisation als Reaktion auf Vorfälle ermöglichen.

3.2.4 Tier 4: dynamisch

Der Tier Level 4 bedeutet, dass eine Organisation alle Anforderungen aus den Tier Leveln 1–3 vollständig erfüllt und zusätzlich die eigenen Prozesse, Methoden und Fähigkeiten ständig überprüft und bei Bedarf verbessert. Grundlage zur kontinuierlichen Verbesserung ist eine lückenlose Dokumentation sämtlicher Cybersecurity-Vorfälle. Die Organisation zieht die notwendigen Lehren aus der Analyse vergangener Vorfälle und passt die eigenen Prozesse und eingesetzten Sicherheitstechnologien dynamisch dem neusten Stand der Technik oder sich wandelnden Bedrohungslagen an. IKT-Risikomanagement ist fester Bestandteil der Unternehmenskultur. Erkenntnisse aus vergangenen Vorfällen, Informationen von externen Quellen und aus der permanenten Überwachung der eigenen Systeme und Netzwerke werden fortwährend in den Risikomanagementprozess integriert. Die Organisation teilt laufend Informationen mit Partnern und verfügt dazu über standardisierte Prozesse.

3.3 Assessment-Auswertung mit Beispiel

Die untenstehende Abbildung zeigt eine fiktive Auswertung sämtlicher beschriebener Aufgaben als Beispiel. Das Assessment kann mit Hilfe der Excel-Datei durchgeführt werden, welche auf der Webseite des Bundesamtes für wirtschaftliche Landesversorgung heruntergeladen werden kann.[9]

Die untenstehenden Diagramme geben dem Anwender Auskunft darüber, welchen Reifegrad an Cybersicherheit seine Organisation in jeder der fünf Kategorien (ID-Identify, PR-Protect, DE-Detect, RS-Response, RC-Recover) erreicht. Für jede der fünf Kategorien wurden alle Aufgaben mit einem Wert zwischen 0 und 4 bewertet (farbige Linie). Die gestrichelte Linie gibt den Durchschnittswert für jede Kategorie an. Das Diagramm oben links (Cybersecurity Maturity Bewertung) zeigt die Gesamtbewertung, welche aus den Durchschnittswerten der einzelnen Kategorien gebildet wird.

Es handelt sich bei diesen Diagrammen explizit um Beispiele und nicht um Richt- oder Sollwerte. Jede Organisation muss ihren Risikoappetit selbständig definieren und so das entsprechende Schutzniveau (je Kategorie) festlegen.

[9] *https://www.bwl.admin.ch*

Beispieldarstellung einer Assessment-Auswertung

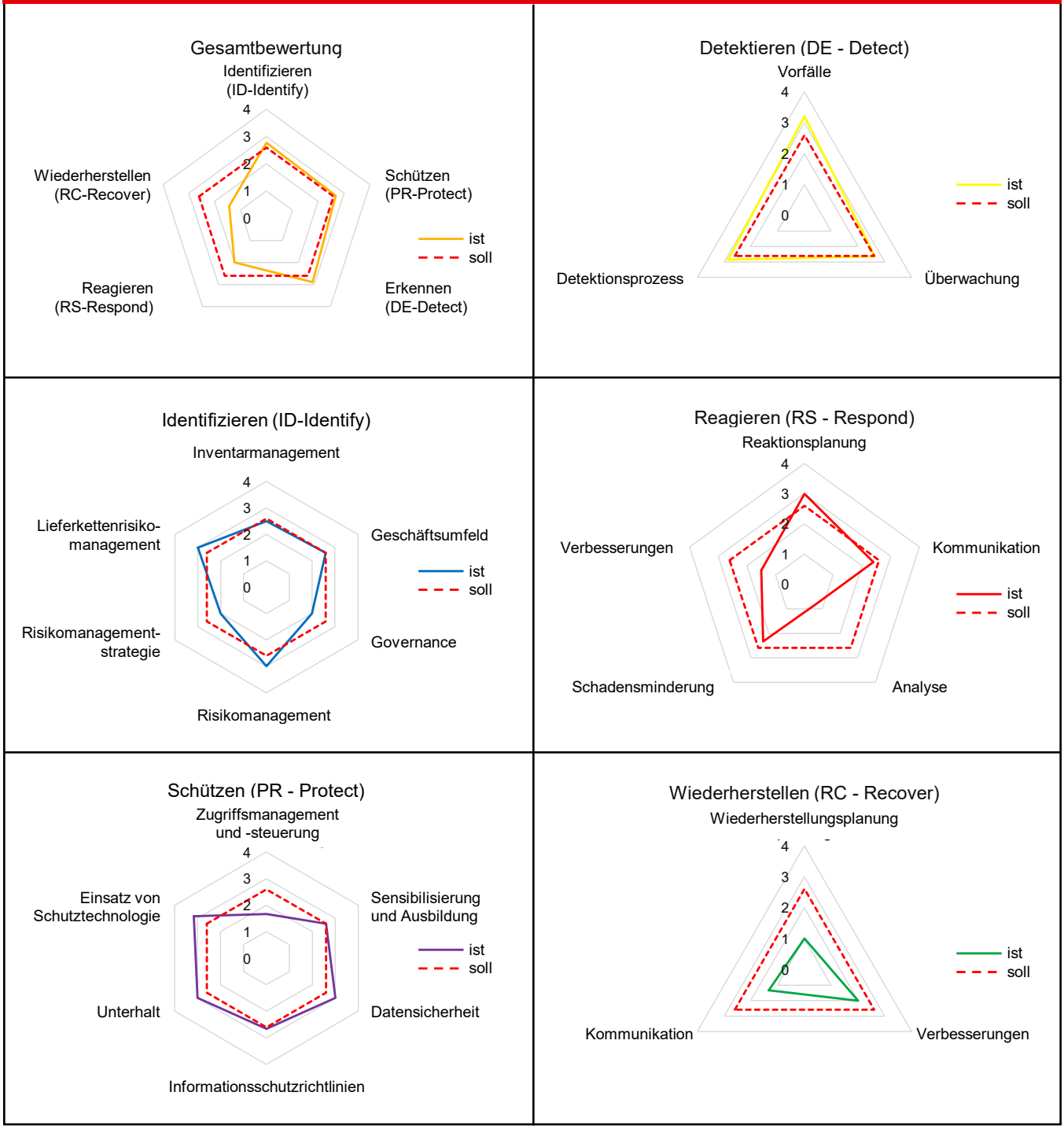

Abbildung 1: Beispieldarstellung einer Assessment-Auswertung

4 Anhang

4.1 Abbildungsverzeichnis

4.2 Tabellenverzeichnis

4.3 Glossar

Nachfolgend werden Begriffe aufgelistet, welche im Rahmen dieses Dokumentes eine spezifische Bedeutung haben. Auf das Auflisten von im IKT-Kontext allgemein gebräuchlichen Begriffen (z. B. Hardware, Software, Backup etc.) wird verzichtet.

Begriff	Bedeutung
Benchmarking	Ein Benchmark ist ein Vergleichsmassstab. Benchmarking bezeichnet die vergleichende Analyse von Prozessen oder Ergebnissen. In diesem Dokument ist explizit der Vergleich mit Organisationen gemeint, die ein ähnliches Schutzniveau anstreben.
Cyber-Angriffe	Cyber-Angriffe umfassen sämtliche bewussten Aktivitäten, die zum Ziel haben, die Verfügbarkeit, Integrität oder Vertraulichkeit von Daten zu verletzen.
Drive-By-Infektion	Unter Drive-By-Infektion versteht man die Infektion eines Computers mit Malware (z. B. Viren, Trojanern etc.) allein durch den Besuch einer Webseite. Das alleinige Aufrufen einer betroffenen Webseite genügt, um den Computer zu infizieren.
Hardware Lifecycle Management	Hardware Lifecycle Management ist ein umfassender Ansatz zur Bewirtschaftung von IKT-Hardware über deren gesamte Einsatzdauer hinweg.
Host Security	Host Security umfasst alle Sicherheitsmassnahmen, die auf dem Endgerät implementiert werden. Dazu gehören z. B. Firewalls oder Antivirenprogramme.
ICS Netzwerk Perimeter Security	Die Perimeter-Sicherheit betrifft die Sicherheit am Übergang zwischen Unternehmensnetz und einem öffentlichen Netz wie dem Internet. Die Perimeter-Sicherheit wird durch Perimeter-Firewalls realisiert, die einen ersten strategischen Schutz gegen Angriffe bieten.
IKT-Infrastruktur	Sämtliche Elemente der Informations- und Telekommunikationsausrüstung, die eine Organisation zur Erfüllung ihrer Geschäftsprozesse benötigt, wie z. B. Desktop-PCs, Mobiltelefone, Rechenzentren etc.
Industrielle Kontrollsysteme	Industrielle Kontrollsysteme ist ein Überbegriff für all diejenigen Elemente, die zur Steuerung und Überwachung von Anlagen oder Industrieprozessen eingesetzt werden. Ein industrielles Kontrollsystem umfasst typischerweise Sensoren, Rechenzentren, Leitstellen, Leitungen und Anlagen. Die englischen Begriffe «Industrial Control System, ICS» und «Supervisory Control and Data Acquisition System, SCADA» werden synonym verwendet.
Informationssicherheitsmanagementsystem (ISMS)	Ein Informationssicherheitsmanagementsystem (ISMS) ist ein unternehmensweit wirkendes Managementsystem, das die Einhaltung des Sicherheits- und Kontinuitätsniveaus von Informationen nachhaltig und effektiv sicherstellt.
Intrusion Detection Systeme	Ein Intrusion Detection System ist ein System zur Erkennung von Angriffen, die gegen ein Computersystem oder Netzwerk gerichtet sind. Das IDS kann eine Firewall ergänzen oder auch direkt auf dem zu überwachenden Computersystem laufen.

Begriff	Bedeutung
Kompromittierung	Ein System, eine Datenbank oder auch nur ein einzelner Datensatz werden als kompromittiert betrachtet, wenn Daten manipuliert sein könnten und wenn der Eigentümer (oder Administrator) des Systems keine Kontrolle über die korrekte Funktionsweise oder den korrekten Inhalt mehr hat.
Kritische Infrastruktur	Das Spektrum der kritischen Infrastrukturen (KI) umfasst neun Sektoren, unterteilt in 27 Teilsektoren (Branchen). Die vollständige Übersicht ist online verfügbar unter: https://www.babs.admin.ch/de/aufgabenbabs/ski/kritisch.html
Legacy Systeme	Legacy Systeme sind veraltete Systeme, die – aus welchem Grund auch immer – noch nicht ersetzt werden können. Solche Systeme können ein besonderes Risiko darstellen und erfordern entsprechende Schutzmassnahmen.
Man-in-the-Middle-Attacken	Ein Man-in-the-Middle-Angriff (MITM-Angriff) ist eine Angriffsform, die in IKT-Netzwerken angewendet wird. Der Angreifer steht dabei entweder physisch oder – heute meist – logisch zwischen den beiden Kommunikationspartnern, hat dabei mit seinem System vollständige Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmern und kann die Informationen nach Belieben einsehen und sogar manipulieren.
Mobile Device Konfiguration	Mobile Device Konfiguration umfasst alle technischen Massnahmen und Einstellungen, um Daten auf Mobilgeräten (Smartphones, Laptops etc.) auch bei physischem Verlust des Geräts weiter zu schützen.
Phishing-Mail	Unter dem Begriff Phishing (Neologismus von fishing, engl. für ‚Angeln') versteht man Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Anwenders zu gelangen und damit Identitätsdiebstahl zu begehen.
Security Awareness Programm	Ein Security Awareness Programm hat zum Ziel, das Bewusstsein für Sicherheitsthemen und entsprechendes Verhalten bei Mitarbeitern, Partnern, Lieferanten etc. zu verbessern.
Security Monitoring	Security Monitoring beschreibt den Prozess, mit dem laufend die Datenflüsse und Netzwerkaktivitäten im eigenen Netz beobachtet werden. Das Ziel ist es, auffälliges Verhalten frühzeitig zu entdecken. Zu diesem Zweck werden dedizierte Security-Monitoring-Systeme eingesetzt.

Projektorganisation

Projekt Auftraggeber
Werner Meier, Delegierter für wirtschaftliche Landesversorgung

Projektleitung
Daniel Caduff, Bundesamt für wirtschaftliche Landesversorgung
Stv. Geschäftsstellenleiter Fachbereich IKT

Strategische Leitung
Marcel von Vivis, Wirtschaftliche Landesversorgung
Leiter Fachbereich IKT

Autorengruppe

Operative Leitung
- Reto Häni, Wirtschaftliche Landesversorgung
  Leiter Abteilung Infrastrukturbetreiber, PwC

Expertengruppe
- Urs Küderli, Wirtschaftliche Landesversorgung
  Experte Abteilung Infrastrukturbetreiber, PwC
- Christian Weigele, Wirtschaftliche Landesversorgung
  Experte Abteilung Infrastrukturbetreiber, SAP
- Candid Wüest, Wirtschaftliche Landesversorgung
  Experte Abteilung Infrastrukturbetreiber, Symantec
- Marc Holitscher, Wirtschaftliche Landesversorgung
  Experte Abteilung Infrastrukturbetreiber, Microsoft
- Markus Pfyffer, Wirtschaftliche Landesversorgung
  Experte Abteilung Infrastrukturbetreiber, IBM
- Hansruedi Münger, Wirtschaftliche Landesversorgung
  Experte Abteilung Infrastrukturbetreiber, Atos

Kontakt

Eidgenössisches Departement für Wirtschaft,
Bildung und Forschung WBF
Bundesamt für wirtschaftliche Landesversorgung BWL

Bernastrasse 28, CH-3003 Bern
info@bwl.admin.ch, www.bwl.admin.ch
Telefon +41 58 462 21 71

Lizenz