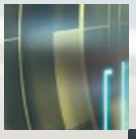
Handbuch Cybersecurity
für Betriebe des öffentlichen Verkehrs



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

VÖV UTP
Verband öffentlicher Verkehr
Union des transports publics
Unione dei trasporti pubblici

Vorwort

Liebe Anwenderinnen und Anwender
des Handbuchs Cybersecurity für Betriebe
des öffentlichen Verkehrs,

Sie arbeiten für ein Transportunternehmen, das zu einer kritischen Infrastruktur der Schweiz gehört, und kennen die hohen Erwartungen bezüglich Sicherheit, Zuverlässigkeit und Pünktlichkeit an unsere Branche. Sie sind sich bewusst, dass durch die zunehmende Vernetzung der Systeme/Anlagen und die steigende Komplexität der Informatik-Systeme neue Risiken entstehen und dass insbesondere die Gefahr von gezielten Cyber-Angriffen auf den öffentlichen Verkehr nicht ignoriert werden darf. Um diese Infrastrukturen auch in Zukunft bestmöglich zu schützen, braucht es einen ausgewogenen Mix von modernen Sicherheitstechnologien, angemessenen Richtlinien, stabilen Prozessen und auf das Thema Cybersecurity sensibilisierte Mitarbeitende.

Das vorliegende Handbuch unterstützt Sie dabei, die wichtigsten Schutzmassnahmen wirksam einzusetzen, damit Störungen durch Cyber-Vorfälle vermieden oder innert nützlicher Zeit behoben werden können. Das Handbuch kann sowohl von kleinen wie auch von grossen Transportunternehmen angewendet werden. Mit der Anwendung des Handbuchs mit anerkannten Richtlinien und Empfehlungen setzen Sie den vom Bundesamt für wirtschaftliche Landesversorgung (BWL) empfohlenen «IKT-Minimalstandard» in Ihrem Unternehmen um und leisten gleichzeitig einen Beitrag zur Verbesserung der IKT-Resilienz Ihres Betriebs und auch der gesamten Schweizer öV-Branche.

Die hier vorliegende erste Fassung des Handbuchs wurde im Auftrag des VöV durch Branchenexperten gemeinsam mit Fachexperten des BWL ausgearbeitet und wird zukünftig regelmässig aktualisiert und wenn nötig erweitert. Der VöV hofft, dass er seinen Mitgliedern damit umsetzbare Empfehlungen an die Hand gibt, die helfen werden, die Herausforderungen Cybersecurity gemeinsam zu meistern.

Viel Erfolg wünscht

Ueli Stückelberger
Direktor VöV

Zusammenfassung

Das vorliegende Dokument adressiert Betriebe des öffentlichen Verkehrs in der Schweiz und stellt eine Empfehlung dar, wie Cyber-Risiken auf ein akzeptables Mass reduziert werden können. Das vorliegende Branchendokument des öffentlichen Verkehrs «Handbuch Cybersecurity» ist ein Leitfaden zum Aufbau der Cybersecurity[1] im Unternehmen. Kern der Empfehlung ist die Implementierung einer sogenannten «Defense-in-Depth»-Strategie, welche heutzutage als die anerkannte defensive Strategie gegenüber Cyber-Bedrohungen gilt. Die Strategie beinhaltet Empfehlungen zu Informations- und Kommunikations-Technologien (IKT), welche durch den Menschen in effektiven und effizienten Prozessen eingesetzt werden sollen. Zum anderen verweist die Branchenempfehlung auf verschiedene Hilfsmittel und bietet insbesondere ein Framework mit einem begleitenden Excel Tool, das Unternehmen erlaubt, die eigenen Fähigkeiten zu erfassen, zu beurteilen und zu vergleichen sowie gezielt weiterzuentwickeln. Das Handbuch Cybersecurity ist kompatibel zu internationalen Standards, basiert auf dem NIST Cybersecurity Framework Core[2] und berücksichtigt die Erkenntnisse und notwendigen Massnahmen aus den Risiko- und Verwundbarkeitsanalysen des Teilsektors Transport und Logistik des Bundesamtes für wirtschaftliche Landesversorgung[3].

[1] Unter dem Begriff «Cybersecurity» werden alle organisatorischen und technischen Massnahmen zum Schutz der Verfügbarkeit, Unversehrtheit (Integrität) und Vertraulichkeit von Informationen sowohl der IKT als auch bei den Information and Communication Systems (ICS) verstanden.

[2] Das NIST Cybersecurity Framework (NIST CSF) ist ein Cybersecurity-Rahmenwerk, welches von der US-Bundesbehörde (National Institut of Standards and Technology) entwickelt wurde und in zahlreichen Ländern als Standard eingesetzt wird.

[3] Risiko- und Verwundbarkeitsanalyse des Teilsektors Transport und Logistik. Bundesamt für wirtschaftliche Landesversorgung, Bern 2017

Inhaltsverzeichnis

Ausgangslage und Zielsetzung

Die Schweiz ist in grossem Masse auf ein möglichst kontinuierliches Funktionieren von kritischen Infrastrukturen angewiesen. Die kritischen Infrastrukturen stellen die Verfügbarkeit von wichtigen Gütern und Dienstleistungen wie Energie, Kommunikation oder Verkehr sicher. Teilweise oder vollständige Ausfälle von kritischen Infrastrukturen haben schwerwiegende Auswirkungen auf die Wirtschaft und die Bevölkerung und beeinträchtigen die Funktionsfähigkeit, die Sicherheit und das Wohlergehen der Schweiz. Der Bund ist gemäss Art. 2 Abs. 2 der Bundesverfassung verpflichtet, «die gemeinsame Wohlfahrt, die nachhaltige Entwicklung, den inneren Zusammenhalt und die kulturelle Vielfalt des Landes» zu fördern. Der Schutz dieser kritischen Infrastrukturen ist deswegen eine zentrale Aufgabe des staatlichen Handelns. Dieser Auftrag kann nur in Zusammenarbeit mit der Wirtschaft umgesetzt werden.

1.1 Hintergrund und Überblick

Das neue Landesversorgungsgesetz, welches per 01.06.2017 in Kraft getreten ist, gibt dem Bundesamt für wirtschaftliche Landesversorgung (BWL) neu die Kompetenz, subsidiär präventive Massnahmen zur Verbesserung der Versorgungssicherheit umzusetzen. Das hier vorliegende Handbuch Cybersecurity ist eine solche präventive Massnahme im Sinne des Landesversorgungsgesetzes. Gemäss dem Subsidiaritätsprinzip wurde das Handbuch als Branchenempfehlung abgefasst.

Die wirtschaftliche Landesversorgung (WL), beziehungsweise das BWL, überprüfte im Rahmen der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) den Bereich öffentlicher Verkehr auf IKT-Verwundbarkeiten. Die Risiko- und Verwundbarkeitsanalysen für die Teilsektoren Strassenverkehr (2015) und Schienenverkehr (2017) wurden gemeinsam von Bund und Mitgliedern der WL erarbeitet und verifiziert. Darin wurde unter anderem auch die Abhängigkeit von IKT-Ressourcen innerhalb dieser Teilsektoren untersucht. Dabei hat sich gezeigt, dass diese Abhängigkeit im Schienenverkehr tendenziell höher ist als im Strassenverkehr.

Der öffentliche Verkehr in der Schweiz ist weltweit einzigartig. Dank des vernetzten Taktfahrplans und guten Umsteigemöglichkeiten steht den Reisenden eine durchgehende Transportkette über alle Verkehrsmittel (Bahn, Bus, Tram, Schiff, Seilbahn) zur Verfügung (wie in Abbildung 1 dargestellt). Neben der Erfüllung der wachsenden Mobilitätsbedürfnisse hat der öffentliche Verkehr aber auch eine grosse volkswirtschaftliche Bedeutung und sichert eine flächendeckende Versorgung der Schweiz.

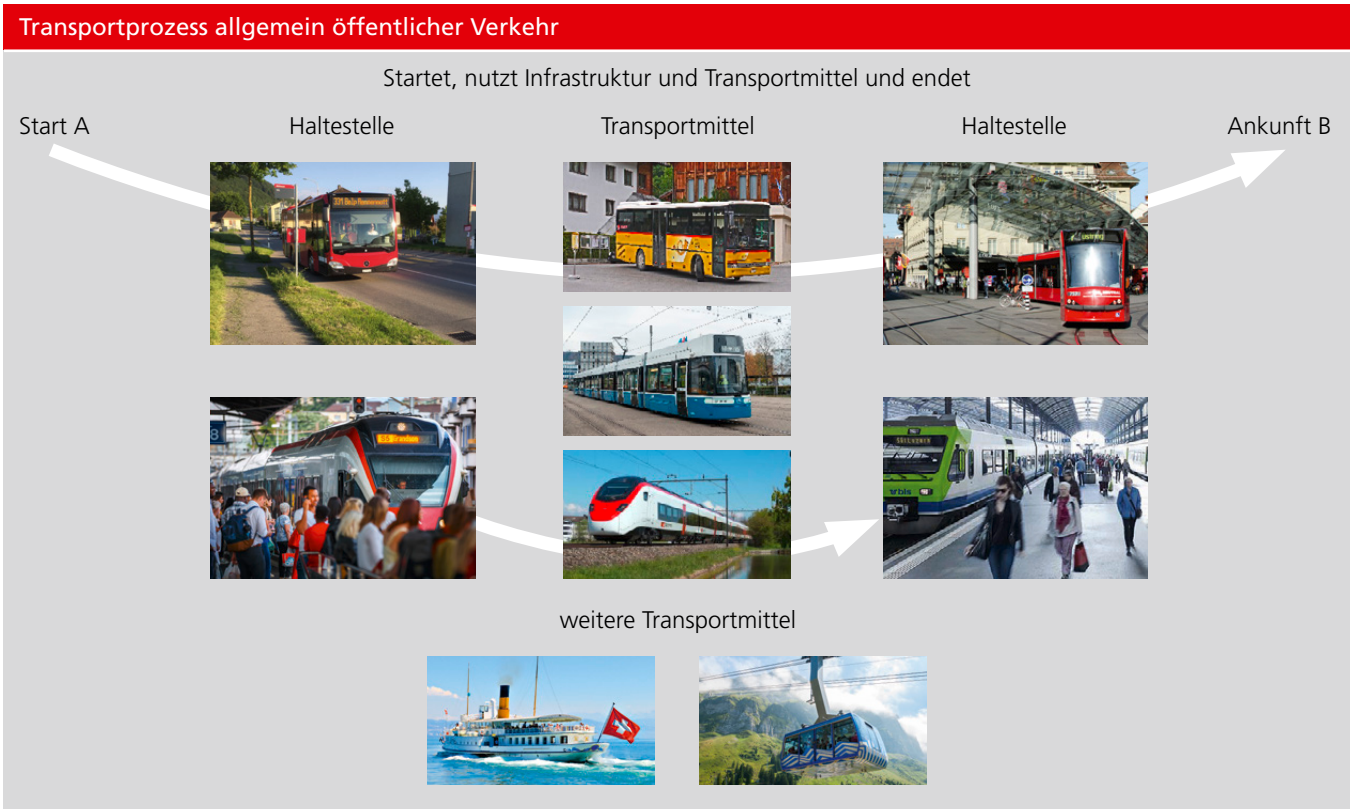


Abbildung 1: Transportmittel im öffentlichen Verkehr

Die immer stärker vernetzten Transportmittel erleichtern das Reisen von A nach B, erhöhen aber gleichzeitig den Aufwand um die zunehmenden gesetzlichen Regularien zu erfüllen und die immer komplexeren Steuerungskomponenten und -systeme nach innen und aussen abzusichern.

Die nachfolgende Abbildung illustriert eine mögliche Entwicklung und Erweiterung der Mobilitätskette im Kontext Smart City durch sogenannte Mobilitätshubs, welche immer mehr Verkehrsträger (Car-Sharing, E-Bikes, etc.) in das Angebot des öffentlichen Verkehrs integrieren.

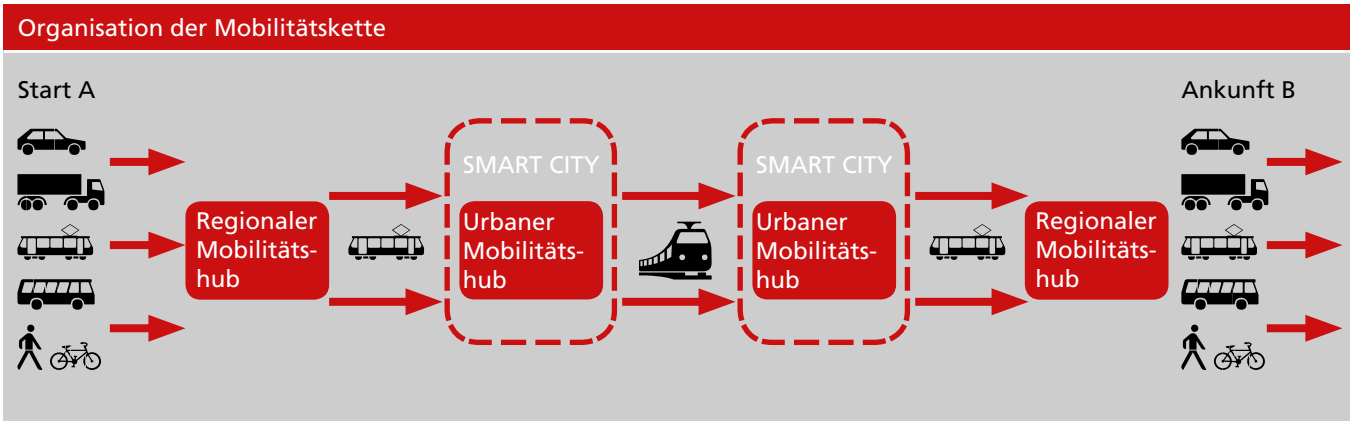


Abbildung 2: Die Mobilitätskette in der Zukunft

Die zunehmende IT-Durchdringung und Vernetzung praktisch aller Lebensbereiche eröffnet Potenziale, auf die ein hochentwickeltes und industrialisiertes Land wie die Schweiz nicht verzichten kann. Im öffentlichen Verkehr ist die Technologisierung bereits stark fortgeschritten. Alle wichtigen Prozesse werden schon heute durch IKT-Systeme unterstützt. Nur mit der Unterstützung dieser IKT-Systeme kann der eng getaktete öffentliche Verkehr aufrechterhalten werden. Durch die weiterhin zunehmende Digitalisierung aller Elemente im öffentlichen Verkehr nimmt die Abhängigkeit von IKT-Systemen und dadurch der Anspruch an Cybersecurity stetig zu. Dies bietet neue Risiken, Angriffsstellen und Fehlerquellen für potentielle Störungen, welche negativen Einfluss auf die Geschäftstätigkeit haben können und somit adressiert werden müssen. Durch die hohen Sicherheitsanforderungen an den öffentlichen Verkehr dürfen Fahrzeuge bei einem Ausfall sicherheitsrelevanter Systeme nur mit verminderter Geschwindigkeit oder gar nicht weiterfahren, was zu wesentlichen Einschränkungen bei der Verfügbarkeit der Infrastruktur führt.

1.2 Motivation für die Erstellung des Cybersecurity Handbuchs

Betriebe des öffentlichen Verkehrs stellen grundsätzlich interessante Ziele für Cyber-Angriffe dar. Sie verfügen insbesondere mit vielen ihrer IKT-Plattformen, SCADA-Systemen und -Anlagen über Schnittstellen ins Internet. Damit könnten sie potentiell zum Opfer von Hacker-Angriffen werden. Noch unbekannte Ransomware-Versionen, die Zunahme von Angriffsvektoren und Schwachstellen bieten die Möglichkeiten für neuartige «Angriffsszenarien». Damit Prozesse und IKT-Systeme eine möglichst kleine Angriffsfläche bieten, sind die Betriebe des öffentlichen Verkehrs bestrebt, robuste Prozesse, System und Anlagen zu unterhalten. Diese müssen regelmässig getestet werden, damit Effekte auf die Verfügbarkeit und Integrität im öffentlichen Verkehr ausgeschlossen werden können.

Alle Betriebe des öffentlichen Verkehrs müssen sich weiterhin vor Angriffen schützen und vorbeugende Massnahmen stetig verbessern. Bei den präventiven Massnahmen ist es wichtig einen soliden standardisierten Basisschutz zu haben. Trotzdem können nicht alle Risiken durch vorbeugende Massnahmen angemessen abgedeckt werden – und erst recht nicht wirtschaftlich sinnvoll. Deshalb erhalten zukünftig auch Massnahmen zur Erkennung von Angriffen oder Angriffsversuchen und einer adäquaten, zeitnahen Reaktion ein deutlich grösseres Gewicht. Nur so werden die Betriebe des öffentlichen Verkehrs Cyber-Risiken genügend gut beherrschen können. Der Austausch und die Zusammenarbeit mit anderen Unternehmen, Partnern/innen und der Wissenschaft ist dabei integraler Bestandteil.

IKT-Sicherheit bedingt also ein risikobasiertes Verhalten und den Einsatz sicherer Systeme im Verantwortungsbereich der jeweiligen Betreiberinnen. Bereits durch die Umsetzung von bewährten Massnahmen, wie sie in vorliegendem Handbuch Cybersecurity dargestellt werden, können eine Vielzahl von IKT-Störungen und -Angriffen mit vertretbarem Aufwand abgewendet werden. Das Handbuch 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 das Handbuch Cybersecurity die Umsetzung unterschiedlich ambitionierter Schutzniveaus, jeweils angepasst an die Bedürfnisse der Organisation.

1.3 Abgrenzung und Gültigkeitsbereich

Das vorliegende Handbuch Cybersecurity wurde durch die wirtschaftliche Landesversorgung in Zusammenarbeit mit externen Experten/innen erarbeitet. Es existieren heute bereits mehrere international anerkannte Standards zur IKT-Sicherheit, die meist deutlich über das vorliegende Dokument hinausgehen (siehe Tabelle 54). Das Handbuch versteht sich explizit nicht als Konkurrenz zu existierenden Standards, sondern ist mit diesen kompatibel, bei gleichzeitig reduziertem Umfang. Es soll einen einfacheren Einstieg in die Thematik ermöglichen und trotzdem ein hohes Schutzniveau gewährleisten.

Die Empfehlungen werden von den Unternehmen der Branche im Sinne einer «Selbstregulierung» freiwillig umgesetzt. Das Handbuch richtet sich grundsätzlich an alle Unternehmen/Betriebe, die an der Organisation des öffentlichen Verkehrs beteiligt sind. Es wird künftig bei Bedarf aktualisiert.

Die Branchenempfehlung fokussiert auf Unternehmens-Prozesse, welche einen direkten Einfluss auf das Erstellen und Erbringen von Verkehrsleistungen haben von:

Eisenbahninfrastrukturbetreiberinnen (ISB)	Unternehmen, die über eine Konzession und eine Sicherheitsgenehmigung nach Artikel 5 Eisenbahngesetz (EBG) für den Bau und Betrieb einer Eisenbahninfrastruktur verfügen. Die Eisenbahninfrastruktur umfasst die Betriebsanlagen der Eisenbahn einschliesslich der Bahnstromübertragungsleitungen.
Eisenbahnverkehrsunternehmen (EVU)	Unternehmen, die Eisenbahnverkehrsleistungen erbringen. Für die Durchführung von Personen- oder Gütertransporten auf einer Eisenbahninfrastruktur sind eine Netzzugangsbewilligung und einer Sicherheitsbescheinigung nach Artikel 8c EBG erforderlich.
Konzessionierte Personenbeförderungsunternehmen	Unternehmen, die über eine Konzession nach Artikel 6 Personenbeförderungsgesetz (PBG) für die regelmässige, gewerbsmässige Beförderung von Personen mit Eisenbahnen, Trams, Seilbahnen, Schiffen oder Motorfahrzeugen mit thermischem oder elektrischem Antrieb verfügen.

Tabelle 1: Akteure/innen im öffentlichen Verkehr

Das Schutzniveau soll insbesondere auf allen Strecken gewährleistet werden, die eine Erschliessungsfunktion nach Artikel 5 der Verordnung über die Personenbeförderung vom 4. November 2009 (VPB, SR 745.11) haben. Die Erschliessungsfunktion ist gegeben, wenn sich an mindestens einem Linienende ein Verknüpfungspunkt mit dem übergeordneten Netz des öffentlichen Verkehrs und am anderen Ende oder zwischen den Linienenden eine Ortschaft befindet. Als Ortschaften gelten Siedlungsgebiete, in denen das ganze Jahr über mindestens 100 Personen wohnen in:

- zusammenhängenden Bauzonen nach dem Raumplanungsgesetz vom 22. Juni 1979, einschliesslich Schutzzonen für Gewässer, bedeutender Ortsbilder, geschichtlicher Stätten und Kulturdenkmäler;
- traditionellen Streusiedlungen;
- Talschaften im Berggebiet, die von einem gemeinsamen Punkt aus erschlossen werden.

1.4 Anleitung zum Einsatz des Handbuchs

Das Handbuch Cybersecurity gliedert sich in mehrere Kapitel: Kapitel 1 und 2 bieten eine Einführung in den öffentlichen Verkehr. Kapitel 3 erläutert den «Defense-in-Depth»-Ansatz. Kapitel 4 und 5 beschreiben die umzusetzenden Massnahmen und stellen Hilfsmittel zur Umsetzung vor.

Zur Einschätzung des Maturitätsniveaus des Unternehmens oder der Organisation steht das Assessment Tool «IKT-Minimalstandard» zur Verfügung. Der IKT-Minimalstandard gilt dann als erfüllt, wenn das «Overall Cybersecurity Maturity Rating» den gewünschten Soll-Wert erreicht.

Kritische Prozesse im öffentlichen Verkehr

Die Definition und Abgrenzung der wichtigsten Akteure/innen im öffentlichen Verkehr, ebenso wie der kritischen Prozesse sowie die Abhängigkeiten der systemrelevanten Systeme im öffentlichen Verkehr sind ein integraler Bestandteil einer ersten Auseinandersetzung mit dem Thema Cybersicherheit im öffentlichen Verkehr.

2.1 Übergeordnete Geschäftsprozesse

Mit dem Handbuch Cybersecurity wird sichergestellt, dass die Cybersecurity in den wichtigen Prozessen im Sektor Transport und hier mit Fokus auf die Bereiche öffentlicher Verkehr Schiene und Strasse sichergestellt werden kann. Auch auf die Bereiche der Beförderung von Personen mit Seilbahnen oder Schiffen können die Vorgaben und Umsetzungsmassnahmen angewendet werden.

Im Folgenden werden die IKT-gesteuerten Geschäftsprozesse aufgezeigt:

2.1.1 Schienenverkehr

Um den Schienenverkehr aufrechterhalten zu können sind drei Netze notwendig. Erstens das *Kommunikationsnetz* (Fest- und Mobilnetz), mit welchem Daten ausgetauscht werden, die für die Sicherheit, Qualität, und die Aufrechterhaltung und Fortführung des Verkehrs benötigt werden. Das *Stromnetz* als Hauptenergielieferant bildet das zweite wichtige Netz. Drittens muss das *Schienennetz* und die dazugehörenden Infrastrukturen (inkl. den nötigen Sicherungsanlagen) erbaut und danach regelmässig gewartet werden, sodass die Züge und Strassenbahnen ohne Zwischenfälle fahren können. Die untenstehende Grafik gibt eine Übersicht über die IKT-gesteuerten Prozesse im Schienenverkehr.

Zudem sind Instandhaltungs- oder Bahnsicherungsanlagen zunehmend hochkomplexe, digitale «Systeme». Bahnsicherungsanlagen beinhalten unter anderem auch die Signalisierungssysteme (z. B. ETCS) und werden in der Regel zentral aus einer Betriebszentrale mit IKT-Systemen ferngesteuert (Leittechnik). Digitale Kommunikationsnetze vernetzen und integrieren die gesamten Bahntechnikanlagen inklusive den IKT-Anwendungen des Bahnbetriebs (Traffic Management Systeme etc.). Sie sind für die Aufrechterhaltung und Fortführung des Bahnbetriebs unerlässlich.

Die IKT reicht von der Vernetzung der festen Anlagen über den Bahnbetrieb bis in die Fahrzeugtechnik. Die Systeme und Anlagen lassen sich unterteilen in Informations-, Steuerungs- und Safety-relevante Systeme und Anlagen.

Abbildung 3: Prozesslandkarte der IKT-gesteuerten Prozesse im Schienenverkehr

2.1.2 Strassenverkehr

Der öffentliche Strassenverkehr ist ein System mit mehreren Akteuren/innen und sich ergänzenden, wie auch zeitlich und örtlich überlagernden Prozessen. IKT kommt zur Steuerung und Überwachung der Infrastruktur-Elemente (Strassenbeleuchtung, Tunnelbelüftung, etc.) zum Einsatz, aber auch zur Verkehrslenkung und Verkehrsüberwachung (Staudetektoren, Kameras, Umleitungen, umschaltbare Geschwindigkeitsanzeigen) und zur Information der Verkehrsteilnehmer/innen (Staumeldungen, Navigationsgeräte). Stetig wachsend ist zudem der Anteil an IKT-gesteuerten Elementen in den Fahrzeugen selbst. Von der Wegfahrsperre über die Unterhaltungselektronik bis zur Kontrolle der Motorleistungen, der Traktionskontrolle oder Spurassistenten, sind in modernen Fahrzeugen verschiedenste Komponenten IKT-gesteuert.

Als Strassenbenützer sind die Bus- und Tramunternehmen auch von diesen Systemen betroffen. Zusätzlich verfügen sie über eine Vielfalt an Steuerungssystemen (z. B. Leitsystem, Funk/VoIP, Ortungssysteme) und Informationssystemen (im und am Fahrzeug, an der Haltestelle, Online via Internet).

Einige Systeme im Strassennetz haben eine Verbindung zu den öffentlichen Verkehrs-Unternehmen (z. B. Ampelsteuerung).

Aus Sicht IKT gibt es im öffentlichen Verkehr auf der Strasse zwei Aspekte zu berücksichtigen: Zum einen die IKT der Strasseneigentümer/innen (Bund, Kantone, Gemeinden) auf welche die konzessionierten Transportunternehmen keinen oder nur einen geringen Einfluss haben. Zum anderen die eigene IKT für die es allein verantwortlich ist.

2.2 Kritische Prozesse im öffentlichen Verkehr

In den letzten Jahren hat es in der Transport- und Logistikleistungskette eine noch stärkere Verlagerung zu IT- bzw. IKT-Systemen gegeben. Dieser technologische Wandel ermöglicht das zentrale Steuern und Regeln von Echtzeitinformationen. Dadurch wird man in der Netzbetriebsführung viel agiler und kann auf zeitnahe, kritische Ereignisse viel schneller und automatisiert reagieren. Doch dieser Wandel hin zur Informationstechnologie bringt auch neue Risiken mit sich, welche die Transport- und Logistikunternehmen anerkennen, bewerten und behandeln müssen, um ihren gesetzlichen Auftrag erfüllen zu können.

Kritische Prozesse		
Infrastruktur	Verkehr/Transport	Unternehmensführung
• Life Cycle Infrastruktur	• Life Cycle Fahrzeuge	• Unternehmenssteuerung (Norm., Strat., Operativ)
• Infrastruktur Instandhaltung	• Verkehrsleistung planen	• Betrieb IKT & Schnittstelle zu ICS
• Verkehrswege bewirtschaften	• Verkehrsleistung erbringen	• Finanz- und Rechnungswesen
• Verkehr leiten	• Verkehrsleistung verkaufen	• Notfall- und Krisenmanagement

Tabelle 2: Kritische Prozesse im öffentlichen Verkehr

Im Folgenden werden die kritischen Prozesse kurz beschrieben.

2.2.1 Prozesse Infrastruktur

Life Cycle Infrastruktur

Zur Infrastruktur des konzessionierten Transportunternehmens gehören sämtliche Netze, Systeme und Anlagen, die für den Betrieb des öffentlichen Verkehrs notwendig sind, wie zum Beispiel Schiene (Unterbau), Fahrleitungen (Oberbau), Sicherungsanlagen oder Betriebszentralen. Der Lebenszyklus der Infrastruktur umfasst alle Schritte vom Konzept über Entwicklung, Realisierung bis zur Ausserbetriebnahme und Entsorgung.

Infrastruktur Instandhaltung

Der Unterhalt von Infrastrukturen ist eng durchgeplant. Dazu gehören auch die regelmässigen Zustandskontrollen der Infrastruktur-Anlagen. Einige öffentliche Verkehrs-Unternehmen verwenden für die Planung der Unterhaltsarbeiten ERP-Systeme (Enterprise Ressource Planning). Oftmals bestehen darauf basierende Eigenlösungen für die unterschiedlichen Arbeiten.

Verkehrswege bewirtschaften
Verkehrswege werden bewirtschaftet, indem die vorhandenen Trassen (Slots) eingeplant und den konzessionierten Transportunternehmen (KTU) zugeteilt werden können. Die Trassen sind in Backend-Systemen (Datenbanken) der öffentlichen Verkehrs-Unternehmen abgelegt.

Verkehr leiten
Durch diesen Steuerungsprozess werden die Züge, Trams und Busse überwacht und gesteuert, sowie die Weichen und Signale gestellt. Eine Überwachung und Steuerung des öffentlichen Verkehrs ohne ICS (Industrielle Kontrollsysteme, vgl. Abs. 3.5.1) ist heute nicht mehr vorstellbar. Ein Ausfall dieser Kontrollsysteme – zum Beispiel durch einen Cybervorfall – hätte Kapazitätseinbussen oder sogar einen Unterbruch auf den betroffenen öffentlichen Verkehrsstrecken zur Folge.

2.2.2 Prozesse Verkehr/Transport

Life Cycle Fahrzeuge
Der ganze Lebenszyklus der Fahrzeuge wird umfassend durch IKT-Systeme geplant und gesteuert. Ohne IKT stehen die öffentlichen Verkehrs-Unternehmen vor einer grossen Herausforderung, welche nach einigen Tagen zu Ausfällen von Verkehrsverbindungen führen kann. Eine IKT-unabhängige Durchführung der Life Cycle Prozesse ist über einen grösseren Zeitraum nur eingeschränkt möglich.

Verkehrsleistungen planen
Obwohl die Planung des Fahrplans mindestens ein Jahr im Voraus bereits koordiniert wird, ist der Fahrplan kein statisches Dokument. Dank der zunehmenden Digitalisierung steigt die Flexibilität. Anpassungen bzw. Optimierungen in Echtzeit sind heute möglich und werden teilweise sogar automatisch ausgeführt. Der Fahrplan bildet eine Datengrundlage für den Einsatz der Fahrzeuge und des Personals. Ein Ausfall der entsprechenden Systeme hätte schwerwiegende Konsequenzen für den öffentlichen Verkehr.

Verkehrsleistungen erbringen
Die Durchführung einer Zug-, Tram- oder auch Busfahrt ist in höchstem Masse auf ICS (Industrielle Kontrollsysteme) und IKT-Systeme (z. B. für Kundeninformation) angewiesen. Beispielsweise können neuere Bahnstrecken ausschliesslich mit ETCS-Standard befahren werden, da die Signale nur noch auf einem Bildschirm im Führerstand angezeigt werden. Beim Bus- und Trambetrieb kann zum Beispiel die Einhaltung der Abstände zwischen mehreren Fahrzeugen auf einer Linie über das Leitsystem gesteuert werden. Ohne Leitsystem wäre das Erbringen von Verkehrsleistungen unter dem Aspekt der Pünktlichkeit und Zuverlässigkeit heute nicht mehr möglich.

Verkehrsleistungen verkaufen
Der Verkaufsprozess kann über verschiedene Kanäle erfolgen: am Schalter, auf einer Webseite, mit einer App oder am Billettautomaten. Ausfälle der Verkaufssysteme oder der Schnittstellen zu externen Finanzdienstleitern (SIX-Payment, Banken etc.) können zu Verlusten der Transportunternehmer/innen führen. Ebenfalls wichtig ist hier die Fahrgastzählung zur Einnahmensicherung.

2.2.3 Prozesse der Unternehmensführung

Unternehmenssteuerung
Fallen zentrale Informationssysteme zur Unternehmenssteuerung (z. B. ERP System) aus, kann heute kein grösseres Unternehmen mehr geführt werden. Im Bereich des öffentlichen Verkehrs betrifft dies unter anderem Systeme wie Management-Cockpits, Finanzsysteme, Projektinformationssysteme oder auch Personalmanagement.

Betrieb IKT & Schnittstelle zu ICS
Alle wichtigen Prozesse des öffentlichen Verkehrs werden durch IKT- und ICS-Systeme unterstützt. Dazu gehören unter anderem Rechenzentren, Kommunikationsnetze sowie IKT- und ICS-Anwendungen. Ohne funktionierende IKT-Systeme kann der öffentliche Verkehr längerfristig nicht aufrechterhalten werden.

Finanz- und Rechnungswesen
Hierzu gehört die Finanz- und Betriebsbuchhaltung, die meist mittels zentraler Systeme (z. B. ERP) betrieben wird. Ausfälle (z. B. bei Lohnzahlungen) oder schwerwiegende Fehler in diesen Systemen können mittelfristig existentielle Auswirkungen für die konzessionierten Transportunternehmen haben.

Krisenmanagement
Für das Krisenmanagement sind insbesondere die Kommunikationssysteme von wesentlicher Bedeutung. Je nach Art der Krise, können jedoch auch diese nur eingeschränkt oder gar nicht zur Verfügung stehen. Für die konzessionierten Transportunternehmen ist es zentral, im Falle einer Krise gut vorbereitet zu sein. Dazu ist eine umfassende Notfallvorsorge mit aktuellen und regelmässig getesteten Notfallplänen und -systemen unerlässlich.

2.3 IKT-Systemabhängigkeit der kritischen Prozesse

Die obenstehenden Prozesse sind abhängig von der stabilen und sicheren Einsatzfähigkeit der dazu benötigten IKT-Systeme. Dadurch sind die Systeme und Anlagen selbst kritische Ressourcen für den öffentlichen Verkehr. Ein Prozess kann dabei von mehreren IKT-Systemen abhängig sein und umgekehrt kann ein IKT-System auch eine kritische Ressource für mehrere kritische Geschäftsprozesse sein.

Es ist also unerlässlich für jeden Betrieb des öffentlichen Verkehrs, dass die jeweils eigenen Prozesse, Systeme und Anlagen (System-Architekturen) genau und nachhaltig dokumentiert werden. Nur was man kennt, lässt sich risikoorientiert schützen.

Die nachfolgenden Darstellungsvarianten zeigen Möglichkeiten auf, wie die Abhängigkeiten der Geschäftsprozesse von wichtigen IKT-Systemen bzw. deren Funktionalitäten visualisiert und dokumentiert werden können. Dabei sind verschiedene Granulationsstufen möglich. Es sind selbstverständlich auch Kombinationen von mehreren Dokumentationsformen möglich.

Abbildung 4 zeigt die Komplexität der kritischen Prozesse. Die Anzahl abgehender Verbindungen von einem kritischen Prozess zu den verschiedenen Systemen zeigt die starke Abhängigkeit von IKT- und SCADA-Systemen.

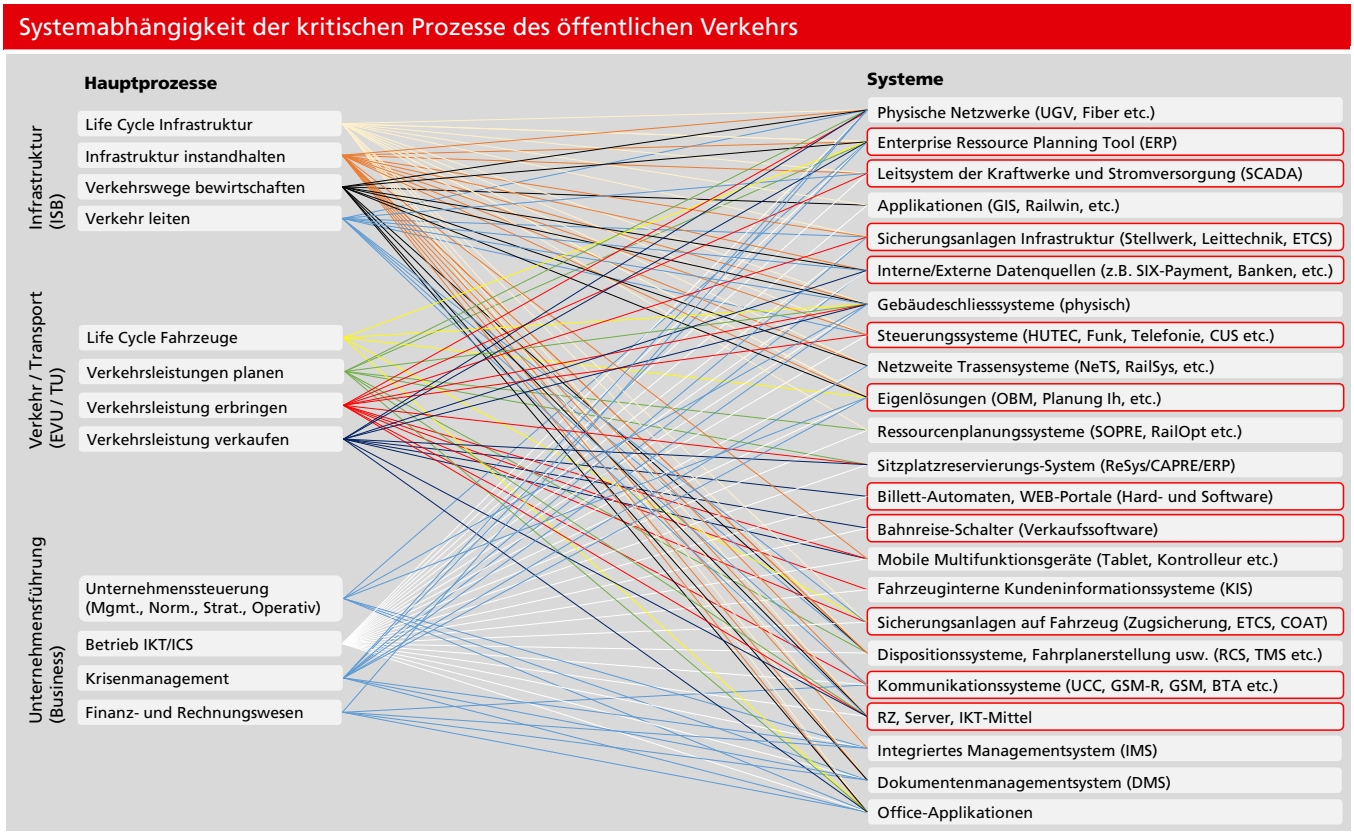


Abbildung 4: Vernetzung IKT- und SCADA-Systeme

In der folgenden Tabelle werden die Systemabhängigkeiten der kritischen Prozesse des öffentlichen Verkehrs mittels einer Matrix aufgezeigt. Es ist zu beachten, dass jedes Unternehmen für sich überprüft, ob die jeweilige Abhängigkeit tatsächlich in dieser Form gegeben ist. Dazu werden von den Autoren/innen konkrete Analysen vorgeschlagen, die auf Basis der im jeweiligen Unternehmen durchgeführten Business Impact Analysen (BIA) erfolgen sollten. Beispiele für einfache Fragestellungen zum Design einer BIA sind im Anhang zu finden.

Unternehmensführung (Business)					Verkehr/Transport (EVU/TU)				Infrastruktur (ISB)				Systemabhängigkeit der kritischen Prozesse des öffentlichen Verkehrs
Krisenmanagement	Finanz- und Rechnungswesen	Betrieb IKT/ICS	normativ., strategisch, operativ)	Unternehmenssteuerung (Managementprozess:	Verkehrsleistung verkaufen	Verkehrsleistung erbringen	Verkehrsleistung planen	Life Cycle Fahrzeuge	Verkehr leiten	Verkehrswege bewirtschaften	Infrastruktur Instandhaltung	Life Cycle Infrastruktur	
X	X	X			X	X	X		X	X	X	X	Physische Netzwerke (UGV, Fiber, etc)
	X	X	X		X		X	X		X	X	X	Enterprise Ressource Planing Tool (ERP)
		X				X			X		X	X	Leitsystem der Kraftwerke (SCADA)
		X								X	X	X	Applikationen (Geoapplikationen, GIS, Railwin, etc.)
X		X				X			X		X	X	Sicherungsanlagen Infrastruktur (Stellwerk, Leittechnik, ETCS)
	X	X			X				X	X	X		Interne/Externe Datenquellen (z. B. SIX Payment, Banken, Lieferanten)
	X	X	X		X	X	X	X	X	X	X	X	Gebäudeschliesssysteme (physisch)
		X				X			X		X	X	Steuerungssysteme (HUTEC, Funk, Telefonie, CUS, etc.)
	X	X								X	X	X	Netzweite Trassensysteme (NeTS, RailSys, etc.)
	X	X	X					X		X	X	X	Eigenlösungen (OBM, Planung, etc.)
		X					X					X	Ressourcenplanungssysteme (SOPRE, RailOpt, etc.)
		X			X	X	X						Sitzplatzreservierungs-System (ReSys, CAPRE, ERP)
		X			X								Billett-Automaten, WEB-Portale (Hard- und Software)
		X			X								Bahnreise-Schalter (Verkaufssoftware)
		X			X	X					X		Mobile Multifunktionsgeräte (Tablet, Kontrolleur, etc.)
		X				X							Fahrzeuginterne Kundeninformations-systeme (KIS)
		X				X		X	X			X	Sicherungsanlagen auf Fahrzeug (Zugsicherung, ETCS, COAT)
		X				X	X		X	X	X		Dispositionssystem, Fahrplanerstellung usw. (RCS, TMS etc.)
X		X				X			X		X		Kommunikationssysteme (UCC, GSM-R, GSM, BTA etc.)
		X			X	X	X		X	X	X	X	RZ, Server, IKT-Mittel
X	X	X	X								X	X	Integriertes Managementsystem (IMS)
X	X	X	X							X	X	X	Dokumentenmanagementsystem (DMS)
X	X	X	X		X		X	X		X	X	X	Office Applikationen

Tabelle 3: Systemabhängigkeit der kritischen Prozesse des öffentlichen Verkehrs

In der untenstehenden Tabelle wird der Grad der IKT-Abhängigkeit für jeden der oben evaluierten kritischen Prozesse wiedergegeben. Die grundlegende Frage, welche in diesem Kapitel beantwortet wird, ist: «Kann der Prozess ohne IKT durchgeführt werden (IKT-Abhängigkeit)»? Der Grad der IKT-Abhängigkeit wird in den Kategorien «gering», «mittel» und «hoch» ausgedrückt. Eine «geringe IKT-Abhängigkeit» wird einem Prozess zugewiesen, wenn dieser Prozess auch weitgehend ohne IKT-Mittel durchgeführt werden kann. Kann ein Prozess nur unter Einbezug zusätzlicher Ressourcen (Zeit, Mitarbeitende, etc.) durchgeführt werden, so wird diesem Prozess eine «mittlere IKT-Abhängigkeit» bescheinigt. Kann ein Prozess bei Ausfall der IKT-Mittel nicht mehr durchgeführt werden, so hat dieser Prozess eine «hohe IKT-Abhängigkeit».

Ausserdem ist ein Vorschlag für eine einheitliche minimale Maturitätsanforderung (vgl. Abs. 4.3 «Implementation Tiers») definiert:

Kritische Prozesse im öffentlichen Verkehr		
Prozesse	Grad der IKT-Abhängigkeit	Anforderung an Maturität
Infrastruktur	(gering/mittel/hoch)	(gemäss Kap. 4)
Life Cycle Infrastruktur	mittel	2–3
Infrastruktur Instandhaltung	hoch	2–3
Verkehrswege bewirtschaften	hoch	3–4
Verkehr leiten	hoch	3–4
Verkehr/Transport		
Life Cycle Fahrzeuge	mittel	3–4
Verkehrsleistung planen	hoch	2–3
Verkehrsleistung erbringen	hoch	3–4
Verkehrsleistung verkaufen	mittel	2–3
Unternehmensführung		
Unternehmenssteuerung (Normativ, strategisch, operativ)	mittel	3–4
Betrieb IKT (& Schnittstelle ICS)	hoch	2–3
Finanz- und Rechnungswesen	mittel	2–3
Notfall- und Krisenmanagement	hoch	2–3

Tabelle 4: Grad der IKT-Abhängigkeit der kritischen Prozesse

Dieser Vorschlag ist aufgrund der in den Unternehmen konkret durchgeführten BIAs und Schnittstellenanalysen individuell anpassbar. Das Maturitätslevel sollte das Level 2 allerdings sinnvollerweise nicht unterschreiten.

2.4 Resilienz der IKT Prozesse und Systeme/Anlagen

Allgemein steht der Begriff «Resilienz» für die Fähigkeit von Systemen, auf Störungen zu reagieren. Im Zusammenhang mit der Nationalen Cyber Strategie steht «Resilienz» (oder «IKT-Resilienz») für die Widerstandsfähigkeit der evaluierten kritischen Prozesse gegenüber Störungen der IKT-Systeme.

Resilienz umfasst jedoch mehr, als nur die Frage nach redundanten Systemen. Resilienz bei IKT-Systemen umfasst immer auch organisatorische Aspekte. Organisatorische Massnahmen zur Steigerung der Resilienz wären beispielsweise Berechtigungs- und Backuprichtlinien, ein straff organisiertes Patchmanagement, frühzeitige Erkennung von Gefahren, etc. Ausserdem stellt sich immer auch die Frage nach einem redundanten, nicht IT-basierten System zur Durchführung eines Prozesses. Wenn ein spezifisches Informationssystem plötzlich ausfällt, können Informationen möglicherweise mündlich von Person zu Person, per Email oder telefonisch übermittelt werden.

Es muss immer auch die systemische Resilienz betrachtet werden. So können beispielsweise mehrere Systeme dieselbe Funktion übernehmen oder einige Systeme schneller oder langsamer arbeiten, um den Ausfall eines anderen Systems zu übernehmen. Der Ausfall eines Produzenten beispielsweise im Stromnetz (z. B. ein Wasserkraftwerk) kann beispielsweise durch den Import von Strom aus anderen Quellen ausgeglichen werden. Diese systemische Resilienz muss bei der Beurteilung der IKT-Resilienz berücksichtigt werden.

Die Resilienz kann mit der Konkretisierung und der Umsetzung der Anforderungen und Massnahmen in den folgenden beiden Kapiteln, sowie der Berücksichtigung der für die jeweiligen Unternehmen relevanten Security Standards erhöht werden.

2.5 Security vs. Safety

Von Fachleuten wird unter dem Begriff «Safety» insbesondere der Schutz von Personen und Umwelt hinsichtlich Gefahren die von einem «System» ausgehen, verstanden. Hierzu gehören beispielsweise Prävention von Personenunfällen. Unter dem Begriff «Security» wird der Schutz von Personen oder «Systemen» gegenüber Einwirkungen wie beispielsweise höhere Gewalt oder widerrechtliche Handlungen mit oder ohne Gewalteinwirkung, verstanden.

Bei Analysen und der Umsetzung von Massnahmen muss immer auch auf Safety-relevante Aspekte geachtet werden. Betriebe des öffentlichen Verkehrs stellen der Schweizer Bevölkerung eine Dienstleistung zur Verfügung (Durchführung von Bus-, Zug-, Schifffahrten etc.). Hier geht es immer um Menschenleben, die transportiert werden.

Entsprechend sind Vorgaben und Massnahmen betreffend der Safety mit den Vorgaben und Massnahmen der Security zu kombinieren und zu einer sinnvollen Einheit zu designen.

Elemente einer Defense in Depth-Strategie

Unter «Defense in Depth» versteht man einen koordinierten Einsatz mehrerer Sicherheitsmassnahmen, um die Datenbestände und die Informationsverarbeitung in einem Unternehmen zu schützen.

3.1 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-Strategie 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 eine/n Feind/in schwieriger ist, ein komplexes und mehrschichtiges Abwehrsystem zu überwinden als eine einzige Barriere. Gleichzeitig werden die Methoden und Vorgehensweisen der potenziellen Angreifer/innen beobachtet, um darauf basierend entsprechende Abwehrdispositive vorzubereiten. Im IKT-Sicherheitsumfeld zielt Defense in Depth darauf ab, Verletzungen der IKT-Sicherheit zu erkennen, darauf zu reagieren, sowie die Konsequenzen der Sicherheitsverletzung zu minimieren, bzw. zu mildern (engl: mitigate).

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 sollen die Gesamtheit der IKT-Systeme schützen. Dazu gehören Personen, Prozesse, Objekte, Daten und Geräte. Ein/e potenzielle/r Angreifer/in stellt erst dann eine Bedrohung für ein IKT-System dar, wenn es ihm/ihr 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.

Bezüglich der Implementierung von Defense in Depth-Konzepten gibt es wichtige Unterschiede. Zwischen der Büroautomation und einem OT bzw. ICS/SCADA bestehen bereits in den Grundeigenschaften bzw. den Handhabungsmethoden sehr grosse Unterschiede. Im Folgenden sollen anhand von ein paar Beispielen zu sicherheitsrelevanten Themenfeldern diese Unterschiede aufgesetzt werden (vgl. Tabelle 4: Grad der IKT-Abhängigkeit der kritischen Prozesse):

Sicherheitsthema	IKT (z. B. Büroinformatik)	OT/ICS/SCADA (z. B. Produktionssteuerung)
Sicherheitsvorgaben	Allgemeine regulatorische Vorgaben, abhängig vom Sektor (nicht alle Sektoren)	Spezifische regulatorische Richtlinien, abhängig vom Sektor (nicht alle Sektoren)
Technologielebenszyklus (Technology Support Life Cycle)	2–3 Jahre, mehrere Anbieter, laufende Weiterentwicklung und Upgrades.	10–20 Jahre, typischerweise der/dieselbe Lieferant/in/Dienstleister/in über den gesamten Lebenszyklus; Ende des Lebenszyklus verursacht neue Sicherheitsgefährdungen.
Sicherheitsaktualisierungen (Update Management)	Klar definiert, unternehmensweit ausgeführt, automatisiert über Fernzugriff.	Lange Vorlauf- und Planungszeit bis zur erfolgreichen Patch-Installation; immer Hersteller/innenspezifisch; kann das ICS (temporär) zum Erliegen bringen. Notwendigkeit, das diesbezüglich akzeptable Risiko zu definieren.
Methoden zum Testen und Aufdatieren (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.

Tabelle 5: Unterschiede zwischen IKT und OT/ICS

Sicherheitsthema	IKT (z. B. Büroinformatik)	OT/ICS/SCADA (z. B. Produktionssteuerung)
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 Systementwicklung (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/innen von ICS haben diesbezüglich Fortschritte gemacht, jedoch langsamer als in der IKT-Welt. Kernelemente von ICS lassen oft keine nachträglichen Sicherheitslösungen zu, bzw. sind diese nicht verfügbar.
Antivirus	Weit verbreitet. Einfach zu verteilen und zu aktualisieren. Anwender/innen 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.

Tabelle 5: Unterschiede zwischen IKT und OT/ICS

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

- Die Kosten, um alte Systeme nach zeitgemässen Bedürfnissen abzusichern
- Der wachsende Trend, ICS mit Geschäftsnetzwerken zu verbinden
- Die Möglichkeit, Fernzugriffe für Anwender/innen 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 u.a. für die Implementierung von Technologien, die ein Eindringen ins System erkennen können (Intrusion Detection Technology).

Eine Auswahl wichtiger Elemente einer Defense in Depth-Strategie finden sich in Tabelle 6: Elemente einer Defense in Depth-Strategie:

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 (IDS) • Sicherheits-Audit Logging • Sicherheits-Vorfall und Event Überwachung
Vendor Management	• Lieferketten-Überwachung & -Management • Managed Services & Outsourcing • Nutzung von Cloud Diensten
Das Element Mensch	• Richtlinien • Vorgehensweisen • Training und Wahrnehmung

Tabelle 6: Elemente einer Defense in Depth-Strategie

3.2 Organisation, Strategie und Governance

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

3.2.1 ICT-Security-Governance

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

- «was wird getan»
- «wie wird es getan»
- «wer ist verantwortlich»
- «wie soll gemessen werden»

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

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

3.2.2 Organisation und Verantwortlichkeiten

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

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

Stellt sicher, dass

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

3.2.3 Weisungen und Richtlinien

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

Die Antworten zu diesen strategischen Fragen sollen in einer unternehmensweiten Sicherheitspolitik behandelt und beantwortet werden. Die Sicherheitspolitik ist durch die Geschäftsleitung zu erstellen und durch den Verwaltungsrat abzunehmen. Normalerweise wird die Sicherheitsorganisation im Auftrag der Geschäftsleitung die Sicherheitspolitik erarbeiten. Folgende strategische Inhalte sollten durch eine Sicherheitspolitik definiert werden und somit Ankerpunkt für jegliche Tätigkeiten und Vorgaben im Bereich Informationssicherheit sein:

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

Nebst der Sicherheitspolitik, welche das Dach der Informationssicherheit bildet, benötigt es je nach Grösse und Struktur des Unternehmens weitere Dokumente mit Weisungscharakter.

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

3.3 Risiko und Business Continuity Management

3.3.1 Asset-Inventar erstellen, bewerten und bewirtschaften

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

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

3.3.2 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 Cyber-Risiken erkennen, bewerten und adressieren können. 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 Aussagen im Umgang mit Risiken gelten generell. Verschiedene IKT-Anwendungen sind aufgrund ihrer Kritikalität aber von spezieller Bedeutung. Dazu gehören insbesondere Industrielle Kontrollsysteme (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/innen auf allen Ebenen der Organisation müssen die Bedeutung von Cyber-Risiken kennen und sich aktiv in den Risikomanagementprozess einbringen. Regelmässige Risikoanalysen für ausgewählte Systeme, Applikationen und Prozesse, inklusive der zugehörigen Netzwerke, sind unabdingbar. Diese Analysen sollten nach strengen Vorgaben durchgeführt werden und dabei sollte ein strukturierter, systematischer Ansatz verwendet werden.

3.3.3 Risikomanagementframework

IKT-Risikoanalysen sollen in ein Risikomanagementframework eingebettet sein und regelmässig (in der Regel jährlich) für klar definierte Untersuchungsobjekte durchgeführt werden. Dies gilt beispielsweise für geschäftskritische Anlagen, Prozesse und Applikationen (auch in der Entwicklungsphase) sowie für deren Abhängigkeiten von weiteren Systemen, Netzen und Diensten.

Das Ziel des Risikomanagementframeworks ist, 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).

3.3.4 Risiko- und Bedrohungsanalyse

Die Risikoanalyse ist im Risikomanagement die Analyse der durch Risikoidentifikation ermittelten Risiken eines Unternehmens. Die Risikoanalyse macht qualitative und quantitative Aussagen über Ausfälle und eintretende Gefahren. Die Kosten und Konsequenzen für das Transportunternehmen stehen dabei im Mittelpunkt. Die Bedrohungsanalyse ist ein Teilbereich der Risikoanalyse. Während die Risikoanalyse die Risiken im Kontext eines IKT- oder OT-Systems betrachtet, konzentriert sich die Bedrohungsanalyse konkret auf die einzelnen Bedrohungen. Aus den identifizierten Bedrohungen und der Einschätzung der Gefährdungslage lassen sich als Ergebnis die einzelnen Risiken für das Risikomanagement ableiten.

Mögliche Bedrohungsszenarien durch Cyber Vorfälle für den öffentlichen Verkehr können beispielsweise sein:

- Erpressung von Geld
- Ausnützung der Rechen-Leistung (Cryptomining, Botnetz, Trittbrett für weitere Angriffe)
- Das Unternehmen als Versuchsziel/Angriffstest (zufällig oder gezielt)
- Manipulation oder Diebstahl von Kunden- oder Prozessdaten
- Sabotage (Störung oder Unterbruch von Verkehrsverbindungen)
- Spionage (Prozesswissen, Personendaten, Marktdaten)
- Diebstahl durch Auslösen oder Umleiten von Geldzahlungen

Der Untersuchungsbereich einer Risikoanalyse soll klar definiert sein. Die betroffenen Geschäftsprozesse und die betreffenden IKT- und OT-Systeme sowie mögliche externe Faktoren sollen möglichst genau beschrieben werden.

3.3.5 Business Continuity Management

Das Notfallmanagement, auch als «Business Continuity Management» (BCM) oder «betriebliches Kontinuitätsmanagement» bezeichnet, ist ein Managementprozess mit dem Ziel, gravierende Risiken für eine Institution, die das Überleben gefährden, frühzeitig zu erkennen und Massnahmen dagegen zu etablieren. Um die Funktionsfähigkeit und damit das Überleben eines Unternehmens/Organisation zu sichern, sind geeignete Präventivmassnahmen zu treffen, die zum einen die Robustheit und Ausfallsicherheit der Geschäftsprozesse erhöhen und zum anderen ein schnelles und zielgerichtetes Reagieren in einem Notfall oder einer Krise ermöglichen.

Das Notfallmanagement umfasst das geplante und organisierte Vorgehen, um die Widerstandsfähigkeit der (zeit-)kritischen Geschäftsprozesse einer Institution nachhaltig zu steigern, auf Schadensereignisse angemessen reagieren und die Geschäftstätigkeiten so schnell wie möglich wieder aufnehmen zu können.

Ziel des Notfallmanagements ist sicherzustellen, dass wichtige Geschäftsprozesse – selbst in kritischen Situationen – nicht oder nur temporär unterbrochen werden und die wirtschaftliche Existenz der Institution auch bei einem grösseren Schadensereignis gesichert bleibt.

Eine ganzheitliche Betrachtung ist daher ausschlaggebend. Es sind alle Aspekte zu betrachten, die zur Fortführung der kritischen Geschäftsprozesse bei Eintritt eines Schadensereignisses erforderlich sind, nicht nur die Ressource Informationstechnik. IKT-Notfallmanagement ist somit ein Teil des Notfallmanagements (z.B. ISO 22301 oder BSI-Standard 100-4).

Business Continuity umfasst Strategien, Pläne, Massnahmen und Prozesse, Schäden durch die Unterbrechung des Betriebs in einem Unternehmen oder einer Organisation zu minimieren. Sie soll sowohl den Betrieb unter Krisenbedingungen sicherstellen als auch den problemlosen und schnellen Wiederanlauf der Prozesse nach einem Ausfall ermöglichen. Allgemeines Ziel ist es, den Fortbestand des Unternehmens und seiner wirtschaftlichen Tätigkeit zu sichern.

Es ist unerlässlich, dass eine methodisch klare Abgrenzung zwischen Risiko-, Krisen- und Kontinuitätsmanagement vorhanden ist, welche die Basis einer erfolgreichen Krisenorganisation bildet. Aufbauend auf einer klaren Abgrenzung können Verantwortlichkeiten eindeutig definiert und Massnahmenpläne (Notfall-, Kontinuitäts-, Recovery-Pläne) zeitlich richtig gestaffelt werden.

Gemäss ISO 22301 ist das BCM als Prozess definiert, der für die Organisation potentielle Bedrohungen identifiziert. Zudem bietet das BCM einen Rahmen für die Etablierung von betrieblicher Widerstandsfähigkeit (Resilienz) und stellt sicher, dass die Organisation angemessen reagieren kann, um die Interessen der (Key-)Stakeholder, die Reputation, das Markenimage und die Wertschöpfungsketten zu schützen.

Es ist der «Plan B» für das Unternehmen zur Aufrechterhaltung der Betriebsfähigkeit, wenn ein Ereignis (Business Impact: z. B. Unfall, Sabotage, etc.) eintritt und das Unternehmen nicht mehr in der Lage ist seine Dienstleistungen/Produkte anzubieten oder weiter herzustellen.

3.3.6 Business Impact-Analyse

Im Rahmen einer Business Impact Analyse sollen die potenziell realistischste 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.

Die Business Impact Analyse (BIA) ist ein Prozess zur Analyse der Tätigkeiten und des Einflusses, den die Störung(en) des Betriebes auf diese haben kann.

Die zentrale Aufgabe einer Business Impact Analyse ist es, zu verstehen, welche Geschäftsprozesse wichtig für die Aufrechterhaltung des Geschäftsbetriebs und damit für die Institution sind, und welche Folgen ein Ausfall haben kann. Diese «kritischen» Geschäftsprozesse werden im Rahmen des Notfallmanagements besonders abgesichert und Vorsorge für die Krise getroffen.

«Kritisch» im Sinne des Notfallmanagements bedeutet «zeitkritisch», also, dass dieser Prozess eine schnellere Wiederaufnahme der Tätigkeit erfordert, da sonst ein hoher Schaden für die Institution zu erwarten ist. Der hohe Schaden kann dabei sowohl aus finanziellen Verlusten, Verstössen gegen Gesetze oder Verträge, aus Imageschäden oder weiteren Schadensszenarien entstehen. Ein bei der BIA als «unkritisch» eingestufter Geschäftsprozess bedeutet nicht, dass dieser für die Institution unwichtig ist, sondern lediglich, dass er eine geringere Priorität in der Wiederherstellung hat (BSI-Standard 100-4, Kapitel 5.1).

Um eine Business Impact Analyse durchzuführen, gibt es verschiedene Methoden und Wege. Ein möglicher Ablauf wäre z. B. eine Übersicht über Stammdaten und Geschäftsprozesse zu erstellen:

- Einzubeziehenden Organisationseinheiten und Geschäftsprozesse abgrenzen (Grenzen festlegen, d.h. nur relevante Geschäftsprozesse für das Notfallmanagement einbeziehen)
- Schadensanalyse durchführen (Rahmenbedingungen für Schadenskategorien und Schadensszenarien definieren, Bewertungsperioden sowie die Strategie zur Behandlung besonderer Verfügbarkeiten festlegen, für jeden einzelnen Prozess und jede Bewertungsperiode bei Ausfall den allfällig entstehenden Schaden bewerten)
- Wiederanlaufparameter festlegen (Maximal tolerierbare Ausfallzeit, die Wiederanlaufzeit und das Wiederanlauf-Niveau für jeden Geschäftsprozess festlegen)
- Abhängigkeiten berücksichtigen (Wiederanlaufparameter in Bezug auf Prozessabhängigkeiten und strategische Geschäftsziele berücksichtigen, allfällige Korrekturen durchführen)
- Priorisierung und Kritikalität der Geschäftsprozesse festlegen (Reihenfolge der Geschäftsprozesse für den Wiederanlauf festlegen, Kritikalitätskategorien und ihre Abgrenzungen definieren)
- Ressourcen für Normal- und Notbetrieb erheben (Ressourcen und die benötigte Kapazität für den Normalbetrieb und den Notbetrieb erheben)
- Kritikalität und Wiederanlaufzeiten der Ressourcen ermitteln (Für die kritischen Prozesse verwendeten Ressourcen die Wiederanlauf- und Wiederherstellungszeiten sowie deren Kritikalität ermitteln)

Im BSI-Standard 100-4 wird das Notfallmanagement im Sinne eines Leitfadens ausführlich abgehandelt.

3.3.7 BCM 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 tragbare Risiko bestimmt werden, so dass die (kumulierten) IKT-Risiken kalkuliert werden können.

3.4 Architekturen

3.4.1 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 den IKT-Betriebsmitteln abgestimmt sein, um ein ganzheitliches Verständnis der Informationsflüsse innerhalb der Organisation sicherzustellen.

Die Cybersecurity-Architektur soll im Einklang mit dem NIST Cybersecurity 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.

3.4.2 Systemarchitektur

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

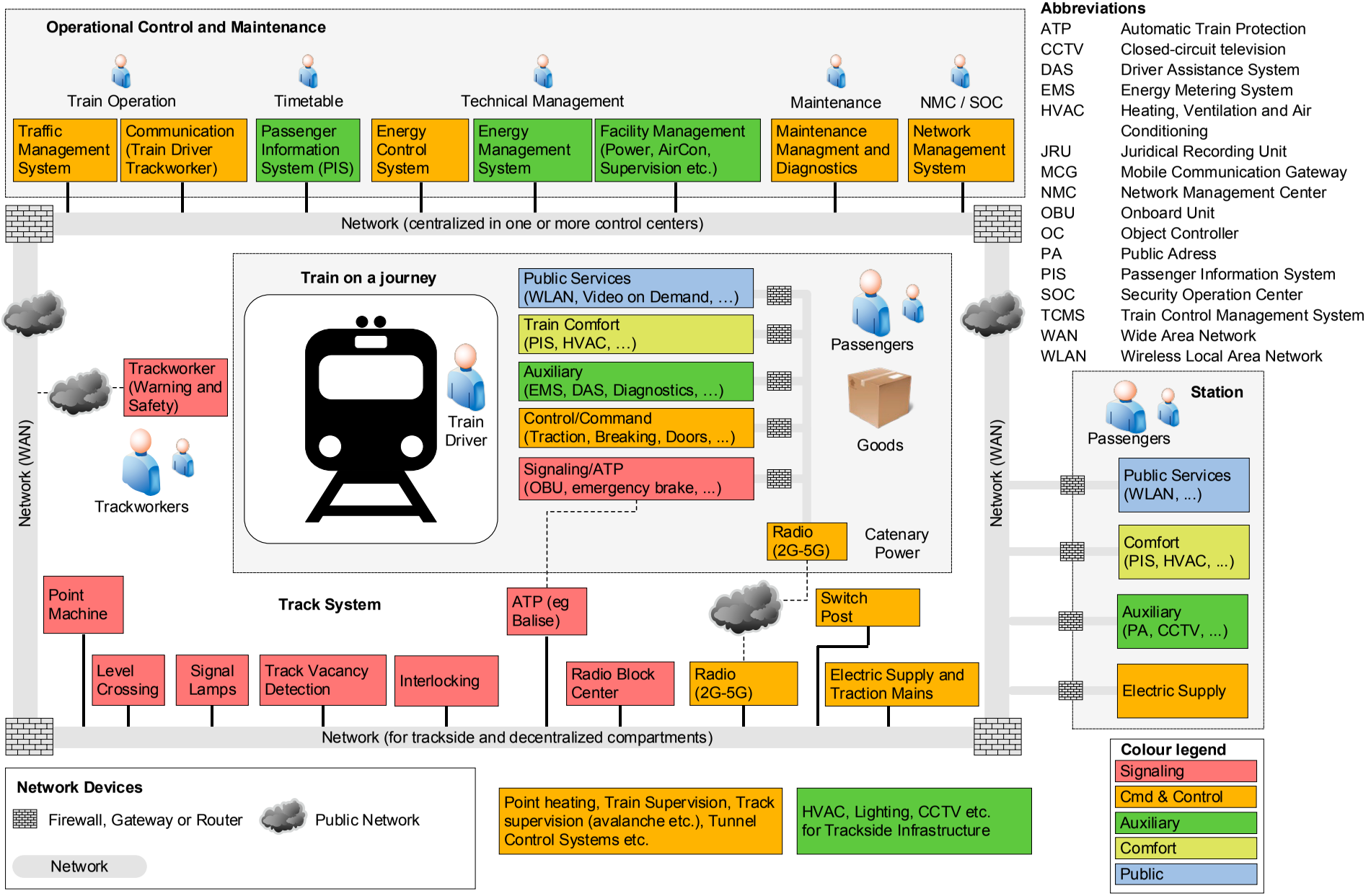
Eine sichere und robuste Netzwerkarchitektur stellt einen der wichtigsten Grundsätze für einen erfolgreichen Schutz gegen Angriffe dar. Jede Schnittstelle, jeder Übergang und jede Verbindung stellt eine potentielle Gefahr dar. Dafür ist es zwingend erforderlich, dass die gesamten Vorgänge in den verschiedenen Netzen und Anlagen bekannt sind und entsprechend behandelt werden. Dabei sind die richtige Gruppierung und das Segmentieren der Netzwerkarchitektur die Basis. Wichtig ist, dass das Netzwerk in Sicherheitszonen unterteilt wird.

Ebenso wichtig ist, dass die Architektur nicht nur auf die unbeweglichen (feste Anlagen) oder die beweglichen (Fahrzeugsysteme) Infrastrukturen begrenzt wird bzw. isoliert betrachtet wird. Es ist sicherzustellen, dass immer die gesamte Architektur in voller Ausprägung berücksichtigt wird, da in einer Gesamtarchitektur leider das schwächste Glied den erreichten Sicherheitslevel anzeigt.

Für kritische Infrastrukturbetreiberinnen ist es damit unerlässlich, Risikoanalysen der gesamten Systemarchitekturen durchzuführen und den dafür benötigten Sicherheitslevel sowie die dazu benötigte Maturität abzuleiten.

Nachfolgende Abbildung ist ein Beispiel einer schematischen Darstellung für eine/n Eisenbahnbetreiber/in. Es zeigt auf, welche IT (Information Technology) und ICS (Industrial Control Systems) Komponenten und welche Kommunikationswege für den sicheren Betrieb benötigt werden[4].

[4] Die dargestellte ICS-Netzwerk-Architektur ist ein Beispiel, welches auf die Bedürfnisse des Unternehmens anzupassen ist.



Abbreviations

ATP	Automatic Train Protection
CCTV	Closed-circuit television
DAS	Driver Assistance System
EMS	Energy Metering System
HVAC	Heating, Ventilation and Air Conditioning
JRU	Juridical Recording Unit
MCG	Mobile Communication Gateway
NMC	Network Management Center
OBU	Onboard Unit
OC	Object Controller
PA	Public Adress
PIS	Passenger Information System
SOC	Security Operation Center
TCMS	Train Control Management System
WAN	Wide Area Network
WLAN	Wireless Local Area Network

Abbildung 5: Beispiel einer Systemarchitektur (Auszug aus CENELEC prTS 50701 – D7E6)

3.5 Technische Sicherheitsmassnahmen

3.5.1 Industrielle Kontrollsysteme (Industrial Control Systems, ICS)

Aufgrund der komplexen Architektur von ICS, resp. SCADA-Systemen[5] können Verwundbarkeiten schlimmstenfalls sehr lange unentdeckt bleiben und entsprechende Exploits eine Bedrohung darstellen. 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 aus diesem erreichbares ICS, mit dem Ziel einen dauerhaften Fernzugriff zu etablieren
- Fernzugriffe auf das ICS unter Ausnutzung gestohlener Zugangsdaten
- Angriffe auf SCADA durch Ausnutzen von Schwachstellen des Web Interfaces (Webschnittstelle)
- 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

3.5.2 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/er Benutzer/in ermöglichen, verschiedene Betriebssysteme und Anwendungen zu nutzen, während er/sie einen adäquaten Schutz der Geräte sicherstellt.

Es müssen ein Konzept zu Passwortrichtlinien für alle Benutzer/innen auf einem System erstellt werden sowie die bekannten Accounts (wie z. B. «Administrator») umbenannt werden. Restriktive Passwortrichtlinien werden von den Anwendern/innen möglicherweise unterlaufen, indem die Passwörter unsicher aufbewahrt werden (z. B. Notizzettel), oder die Anwender/innen immer wieder ähnliche Passwörter verwenden. Die Komplexität der Passwortbestimmungen soll der Berechtigungsstufe der Anwender/-innen 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 wo möglich gesetzt 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 FTP, müssen durch sichere Alternativen wie sTelnet, SSH, sFTP usw. ersetzt werden
- Benutzer/innen 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. Bei mobilen Geräten soll die Harddisk zusätzlich verschlüsselt werden

3.5.3 Netzwerk-Perimeter-Security

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

[5] In diesem Dokument werden die Begriffe OT, ICS und SCADA synonym verwendet.

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

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 Demilitarized Zone (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.

3.5.4 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.

3.5.5 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, umfasst 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 an deren Arbeit oder in Notfallverfahren gehindert 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 Mobilgeräte), 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 Systeme und Netzwerkausrüstung, Bürogeräte (z. B. Netzwerkdrucker und Multifunktionsgeräte) und Spezialausrüstung (z. B. industrielle 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 die Sicherheitseinstellungen konfiguriert, der Zugang beschränkt, Sicherheitssoftware installiert und die Geräte zentral verwaltet werden.

3.6 Lieferantenmanagement, Betriebsmodelle, Monitoring

3.6.1 Lieferantenmanagement

Das Lieferantenmanagement befasst sich mit der Identifizierung und der Verwaltung von Informationsrisiken zu externen Anbietern/innen (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.

3.6.2 Outsourcing/Managed Services

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

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

Wenn es sich um eine externe Partei handelt, die technische Beurteilungen durchführt oder prüft, sollten alle Parteien Regeln für die Zusammenarbeit festlegen und vereinbaren. Cyber-Vulnerability Assessments zum Beispiel erfordern typischerweise ein gewisses Mass an passivem oder aktivem Scannen oder Testen auf den Zielsystemen, was bedeutet, dass die Assessoren entweder selber Zugriff darauf haben oder Zugriffe anderer auf kritische Cyber-Assets innerhalb der Kontrollsystemumgebung beobachten müssen. Das Assessment-Team arbeitet mit seinem organisatorischen Pendant zusammen, um sicherzustellen, dass die Testaktivitäten nicht den Kundenbetrieb stören und sich auch auf Massnahmen zum Monitoring von Protokollen einigen, falls die Aktivitäten irgendwelche Probleme für das Unternehmen verursachen. Die Rules of Engagement (RoE) beinhalten, welche Aktivitäten in welchen Systemen stattfinden können und wer diese Aktivitäten ausführen kann. Es umfasst Entscheidungen darüber, ob das Testen innerhalb des primären (aktiven Produktions-) Steuerungssystems oder eines glaubwürdigen Ersatzes wie eines Backup- oder sekundären Kontrollsystems, eines Testnetzwerks oder eines eigenständigen Systems stattfindet. Aktive Scans von Produktionssystemen sind zu vermeiden, da sie Betriebsstörungen verursachen oder eine Denial-of-Service-Bedingung erzeugen können. Passive Aktivitäten wie Netzwerk-Sniffing können angemessen sein. Wenn ein Ersatzsystem verwendet wird, sollte man es mit dem aktiven System vergleichen, um sicherzustellen, dass sie im Betrieb identisch sind. Das Assessment-Team und die Organisation müssen sich darüber einigen, wer während der Testphase ihre «Hände auf der Tastatur» haben wird – besonders, wenn aktive (Produktions-) Steuerungssysteme das Ziel sind. Lokales Personal sollte alle Tests an einer aktiven Steuerung des Assessment-Teams durchführen.

3.6.3 Einsatz von Cloud-Diensten

Der Bezug von IKT-Leistungen aus der Cloud ist heute kein Hype-Thema mehr, sondern tägliche Realität. Cloud-Computing ist ein Modell zur Ermöglichung eines allgegenwärtigen, bequemen, bedarfsgerechten Netzwerkzugriffs auf einen gemeinsamen Pool von konfigurierbaren Computing-Ressourcen (z. B. Netzwerke, Server, Speicher, Anwendungen und Dienste), die mit minimalem Verwaltungsaufwand oder Interaktion mit dem/der Dienstanbieter/innen schnell bereitgestellt und freigegeben werden können. Neben wirtschaftlichen Aspekten ist dabei auch die Informationssicherheit von zentraler Wichtigkeit, gerade für die Anbieter/innen des öffentlichen Verkehrs. Im Zuge der Digitalisierung wirken sich Aspekte der Cloud-Sicherheit nicht nur auf IKT-, sondern zunehmend auch auf ICS-Themen aus. Dennoch lassen sich Weichen, Züge und Autobusse nur schwer virtualisieren und containerisieren, was dazu führt, dass zumindest einige der zugehörigen Leitsysteme mittel- oder sogar längerfristig lokal betrieben werden müssen.

Dies führt fast immer zu einem hybriden Ansatz, der ein Sicherheitskonzept verlangt, welches gleichsam auf Cloud-Services und lokale Services angewendet werden kann.

Die Cloud bringt Prinzip bedingte Bedrohungen mit sich. Die relevantesten aus Sicht des öffentlichen Verkehrs sind:

- Ausfall der Internet- oder Netzverbindung, der den Zugriff auf Daten bzw. Anwendungen unmöglich macht.
- Denial-of-Service Angriffe auf Cloud-Anbieter/innen, die sicher noch zunehmen werden.
- Fehler in der Cloud-Administration, die aufgrund der sehr hohen Komplexität zu erheblichen Sicherheitsproblemen (Dienstausfall, Datenverlust, etc.) führen können. Kleine Fehler oder Pannen können in einer Cloud-Infrastruktur grosse Auswirkungen (nicht nur auf die Sicherheit) haben.
- Identitätsdiebstahl bzw. Missbrauch von Accounts.
- Verlust der Kontrolle über die Daten und Anwendungen.
- Verletzung geltender Vorgaben und Richtlinien (z. B. Datenschutzanforderungen).
- Sicherheit der Endgeräte, mit denen die Cloud-Dienste verwendet werden.
- Nicht vorhandene Cloud-Strategie und deshalb sind die Ziele, die mittels Cloud-Computing erreicht werden sollen, weder klar noch überprüfbar.
- Grosser Wille, Cloud-Computing auf jeden Fall einzusetzen, führt zu illusorischen Annahmen und zu «geschönten» Kosten-Nutzen-Analysen. Im Endeffekt kommt es zu finanziellen Einbussen.
- Der Weg in die Cloud kann sehr schwierig sein und dabei wird übersehen, dass auch an einen Weg aus der Cloud heraus gedacht werden muss. Andernfalls entsteht eine starke Abhängigkeit von der/m Cloud-Anbieter/in, die finanziell von Nachteil sein kann.
- Ein/e Cloud-Anbieter/in bezieht selbst häufig Dienste (z. B. Administration oder Backup von Daten) von Unterauftragnehmern. Dadurch können beispielsweise personenbezogene Daten an nicht erlaubte Stellen gelangen (was ggf. bussgeldbewehrt ist) oder es kann dadurch ein Sicherheitszertifikat gefährdet werden, weil ein Auditor diesen Unterauftragnehmer nicht überprüfen kann.
- Durch die Fehlannahme, dass die Cloud immer da ist, haben Cloud-Anwender/innen oft keinen Notfallplan.

Daher gilt es beim Einsatz von Cloud-Diensten die folgenden Aspekte zu beachten:

Cloud-Strategie erstellen

Unabhängig von der Grösse des Cloud-Vorhabens ist es notwendig, die grundlegenden Anforderungen und Rahmenbedingungen zu kennen und daraus eine Handlungsanleitung zu schaffen. Andernfalls ist das Vorhaben von Anfang an in einer Schieflage. Nur zu gerne folgen Unternehmen den Versprechungen der Anbieter/innen und fallen hart auf den Boden der Realität, wenn sie feststellen müssen, dass sich weder der gewünschte Nutzen noch die gewünschte Kostenersparnis oder die benötigte Sicherheit einstellen.

Machbarkeitsstudien erstellen

Mittels einer Machbarkeitsstudie sollten unter anderem die folgenden Punkte adressiert werden:

- Untersuchung der rechtlichen Rahmenbedingungen (z. B. Datenschutz, Geheimschutz, Aufsichtsbehörden) und der unternehmens- bzw. behördeneigenen Richtlinien (Compliance). Welche Art von Daten soll in der Cloud verarbeitet werden? Dürfen die Daten in eine Cloud? Gibt es Einschränkungen bzgl. des Speicher- und Verarbeitungsorts (z. B. aufgrund von Zugriff auf die Informationen durch Dritte, Spionage)?
- Hat die IT des Unternehmens die nötige Reife, Cloud-Dienste nutzen zu können? Bei der Nutzung von Infrastructure as a Service (IaaS) in grösserem Stil ist zu fragen: Lassen sich die betroffenen Dienste überhaupt virtualisieren? Lassen sie sich standardisieren? In Unternehmungen des öffentlichen Verkehrs ist dies nicht immer der Fall, da viele Spezialanwendungen und -systeme betrieben werden müssen.
- Festlegen des Service- und Bereitstellungsmodells (SaaS, PaaS, IaaS).

Cloud-Risiken ermitteln und managen

Entscheidend für die Definition der Anforderungen an einen Cloud-Dienst ist die Klassifikation (Schutzbedarf) der zu verarbeitenden Informationen bezüglich Vertraulichkeit, Verfügbarkeit und Integrität.

Während die öffentliche Diskussion über die Cloud-Sicherheit stark auf den Aspekt der Vertraulichkeit fokussiert (Einflussnahme von Nachrichtendiensten, Strafverfolgungsbehörden, etc.) sind für die Unternehmen des öffentlichen Verkehrs die Aspekte der Verfügbarkeit und der Integrität mindestens gleich kritisch. Wenn die Systeme nicht verfügbar sind, fahren die Fahrzeuge nicht, wenn sie falsche Informationen bearbeiten, kann es für den Verkehr sogar gefährlich werden.

In der Risikoanalyse sollen daher mindestens folgende Gefährdungen speziell betrachtet werden:

- Zugriff auf die Daten durch den/die Cloud-Anbieter/in
- Zugriffsmöglichkeiten durch staatliche Behörden aufgrund der (ggf. ausländischen) Jurisdiktion, die für den/die Cloud-Anbieter/in zutrifft

- Nicht-Verfügbarkeit der Daten und Diensten
- Kompromittierung der Authentisierung
- Datenverlust
- Datenmanipulation
- Vendor Lock-In: In der Regel ist es sehr aufwändig und nicht immer von Erfolg gekrönt, sich wieder aus den Fängen eines/r Anbieters/in zu befreien
- Brain-Drain: Durch einen längerfristigen Bezug von Cloud-Services sinken im Unternehmen die technischen Fähigkeiten für die selbstständige Bereitstellung eigener Services

Diese Analyse liefert bereits Bereiche, in denen besondere Sicherheitsmassnahmen notwendig werden bzw. bei denen Risiken entstehen, die nicht behandelt werden können. Für die Unternehmen des öffentlichen Verkehrs dürften vor allem Risiken im Bereich der Nicht-Verfügbarkeit von Daten und Diensten, sowie eine allfällige Datenmanipulation im Fokus stehen, da deren Eintreten über kurz oder lang betriebsverhindert wirkt. Wichtig: Ein für alle Anwendungsfälle sicheres Cloud-Computing gibt es nicht.

Kosten-Nutzen-Abschätzung

Sind die oben genannten Punkte geklärt, folgt eine grobe Kosten-Nutzen-Abschätzung, die mindestens folgende Aspekte betrachtet:

- Nutzungskosten des Service
- interner Administrationsaufwand
- Schulung von Mitarbeitern und Administratoren/innen
- bei Bedarf neue IKT oder neue Netzanbindung
- Kosten der Anpassung von Prozessen
- Kosten der Migration
- Interne Einsparungen

Diese Abschätzung liefert einen ersten Eindruck, ob sich ein Cloud-Service rechnen könnte. Die Ergebnisse werden zusammengefasst und den Entscheidungsträgern vorgelegt. Sie entscheiden über den Fortgang des Projekts.

Sicherheitsanforderungen definieren

Wurde auf Basis der Machbarkeitsstudie, der Risikoanalyse und der Kosten-Nutzen Abschätzung entschieden, den Einsatz eines Cloud-Service weiter voranzutreiben, folgen nun konkrete Umsetzungsschritte.

Neben den funktionalen Anforderungen sind die Anforderungen an die Informationssicherheit und die Verfügbarkeit des Cloud-Dienstes darzulegen. Darunter sind nicht nur diejenigen an den Cloud-Anbietern/innen zu verstehen, sondern auch an das eigene Unternehmen. Wichtig ist, dass die Sicherheitsanforderungen nicht durch die Hosting-Entscheidung beeinflusst werden, resp. diese nicht so zurechtgebogen werden, dass der Bezug eines Cloud-Dienstes erst möglich wird.

Wer bisher noch keine eigenen Sicherheitsanforderungen aufgestellt hat, wird sich schwertun, dem/der Cloud-Anbieter/in konkret zu sagen, was er von ihm/ihr erwartet. Von dem/der Cloud-Anbieter/in eine «sichere» und «immer verfügbare» Cloud zu fordern, ohne konkrete Anforderungen zu stellen, kann nur schiefgehen: Entweder reicht das Sicherheitsniveau nicht aus oder die angebotene Lösung ist zu teuer. Sollten die Sicherheitsanforderungen so hoch sein, dass sie mit einer Cloud-Nutzung nicht zu erfüllen sind, ist der Prozess zur Cloud-Nutzung abzubrechen.

Sicherheitskonzeption erstellen

Die bestehende Sicherheitsdokumentation muss um Aspekte des Cloud-Computings erweitert werden. Wichtig ist, dass das Konzept so gestaltet wird, dass sich die beschriebenen Massnahmen gleichsam für lokale Systeme als auch für die Cloud eignen. Wichtige Aspekte dabei sind:

- Übergreifende IAM-Konzepte: Es sollte darauf geachtet werden, dass die digitalen Identitäten und Rollen des Unternehmens möglichst zentral und möglichst nur einmal bewirtschaftet werden. Die Authentisierung kann dann dezentral, mittels föderativer Verfahren (OAuth2, SAML2.0. etc.) erfolgen.
- Sicherheitssysteme: Logging- und Monitoring-Systeme (z. B. SIEM) sollten so gestaltet sein, dass sie gleichsam Cloud- und lokale Services überwachen und korrelieren können. Eine Schwachstelle im Perimeter kann sich sofort auf Cloud-Dienste auswirken und umgekehrt.
- Zero-Trust-Modelle: Da in der Cloud gegenüber dem im Kapitel 3 beschriebenen Defense in Depth-Ansatz gewisse Schichten des Abwehrsystems fehlen, oder sich diese nicht mehr mit den im Unternehmen vorhandenen koordinieren lassen (typischerweise die Perimeter-Sicherheit), fallen neben dem Monitoring, dem Schutz der Identität, der Qualität der Authentisierung, sowie der Zugriffsteuerung besondere Bedeutung zu. D. h., die Systeme und Prozesse müssen so designt werden, dass sie auch in einer nicht vertrauenswürdigen Umgebung (z.B. Internet) sicher funktionieren können. Einem sicheren möglichst gut gehärteten Endgerät fällt diesbezüglich eine grosse Bedeutung zu.

Datenschutz/Compliance sicherstellen

Werden in der Cloud personenbezogene Daten erhoben, verarbeitet oder genutzt, muss der Schutz personenbezogener Daten gemäss den datenschutzrechtlichen Bestimmungen gewährleistet sein.

Neben datenschutzrechtlichen Anforderungen muss der Cloud-Nutzer die geforderten rechtlichen Bestimmungen einhalten (Compliance). In allen Fällen gilt, dass bei einer Bearbeitung solcher Daten in einer Cloud die Verantwortung (in der Regel) bei dem/der Cloud-Nutzer/in bleibt und er/sie sicherstellen muss, dass die Daten bei dem/der Cloud-Anbieter/in gemäss diesen Vorschriften und Gesetzen behandelt werden.

3.6.4 Security-Monitoring

Der Einsatz von Monitoring-Systemen und Netzwerk-Komponenten, welche anomale Verhaltensweisen und Angriffssignaturen erkennen, bringen 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, welches 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); sowie
- 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.

3.6.5 Hardware Life Cycle 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 Life Cycle hinweg nicht beeinträchtigt.

3.7 Faktor Mensch

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

3.7.1 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 das Sicherheitsbewusstsein fördern und das Sicherheitsverhalten definieren. Die Durchführung der Schulungen soll durch die Organisation dokumentiert werden.

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

3.7.2 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.

3.7.3 Prozesse

Sicherheitsmanagement ist in der Verantwortung der IT-Sicherheitsorganisation und prozessual organisiert. Seine 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 soll. Diese Prozesse sollten stets standardisiert und wiederholbar sein. So werden neue Mitarbeitende stets auf gleichbleibenden Sicherheitsniveaus geschult und es kann sichergestellt werden, dass alle erforderlichen Vorschriften und Standards bekannt sind.

3.7.4 Aufgaben und Verantwortlichkeiten in kritischen Geschäftsumgebungen

Aufgaben und Verantwortung 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.

3.7.5 Kommunikation/Security Awareness Programm

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

Ziel ist eine Unternehmenskultur, welche das individuell gewünschte Sicherheitsverhalten fördert. Jede/r Einzelne soll in seinem/ihrem persönlichen Zuständigkeitsbereich befähigt sein, risikobasierte Entscheidungen zu treffen.

Vorgaben und Assessment Framework

4 Framework

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. Wo sinnvoll, sollte er unbedingt durch weitere international anerkannte Industriestandards ergänzt werden.

Das vorliegende Handbuch Cybersecurity für Betriebe des öffentlichen Verkehrs basiert auf dem internationalen NIST Cybersecurity Framework Core[6]. 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.

Das NIST Framework ist damit auch kompatibel zu den Standards ISO 2700x und ISO/IEC 62443, deren Anwendung gemäss AB-EBV 2020 anzustreben ist. Zur Anwendung des IKT-Minimalstandards werden die einzelnen Standards in Kapitel 4 gegenseitig referenziert.

4.1 Grundsätze

Folgende Grundsätze sind für die Umsetzung relevant:

1. Eigenverantwortung: Betreiberinnen von kritischen Infrastrukturen sind grundsätzlich selbstverantwortlich für das Aufrechterhalten ihrer kritischen IKT/ICS-Prozesse.
2. Risikomanagement: Es ist Aufgabe der Anwender/innen dieses Handbuchs, 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.
3. Business Continuity Management: Alle Aspekte der IKT/ICS-Sicherheit sollen in ein übergeordnetes Business Continuity Management eingegliedert werden.
4. Vollständigkeit: Der/die Anwender/in dieses Handbuchs bekommt einen Leitfaden für die wesentlichen Umsetzungsbausteine. Die Vollständigkeit der anzuwenden Sicherheits massnahmen ergibt sich aus den Business Impact und Risikoanalysen. Die entsprechend dazu notwendigen zusätzlichen Standards und externen und internen Handlungsanweisungen sind dabei zu berücksichtigen.
5. Sicherheitskultur: Um eine nachhaltige Cybersecurity sicherzustellen ist eine Sicherheitskultur in den Unternehmen/-Betrieben zu fördern.

4.2 Überblick

Das NIST Cybersecurity Framework Core verfolgt einen risikobasierten Ansatz um Cybersecurity-Risiken zu adressieren und zu managen. Es besteht aus fünf Funktionen:

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

4.3 Implementation Tiers

Das NIST Cybersecurity Framework (NIST CSF) kennt vier Implementation Tiers (dt. «Stufen»). Diese beschreiben die Ausbaustufe (Schutzniveau), welche ein Unternehmen umgesetzt hat. Sie reichen von nicht umgesetzten Massnahmen (Tier 0) bis hin zu voll dynamischen Umsetzungen (Tier 4). Zur Festlegung des eigenen Schutzniveaus (Tier Levels) soll eine Organisation ihre Risikomanagementpraktiken, die Bedrohungsumgebung sowie rechtliche und regulatorische Anforderungen, Geschäftsziele und organisatorischen Vorgaben genau kennen.

Die Tier Definitionen sind wie folgt:

Tier 0: Nicht umgesetzt

Obschon sich die Organisation/das Unternehmen bewusst ist, dass die betroffene Massnahme eigentlich umgesetzt werden sollte, wurde noch nichts unternommen.

[6] *https://www.nist.gov/cyberframework/online-learning/components-framework*

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.

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.

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/innen 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.

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.

n/a: Nicht zutreffend

Diese Massnahme wird von der Organisation/dem Unternehmen entsprechend der eigenen Risikobewertung bewusst nicht umgesetzt.

Profile

Ein Profil kann als eine Angleichung von Standards, Richtlinien und Praktiken aus dem Cybersecurity Framework mit einem individuellen Implementierungsszenario charakterisiert werden. Profile können verwendet werden, um Optionen zur Verbesserung der Cybersecurity zu identifizieren, indem sie ein Ist-Profil mit einem Soll-Profil verknüpfen. Um ein solches Profil zu entwickeln, kann das mit diesem Handbuch Cybersecurity mitgelieferte Assessment Tool verwendet werden. Die Resultate aus der Beantwortung der 106 Aufgaben werden entsprechend den 5 Funktionen des NIST-Cybersecurity Frameworks dargestellt (Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen). Das Minimalniveau gilt dann als erreicht, wenn im «Overall Cybersecurity Maturity Rating» der Ist-Zustand mindestens den entsprechenden Minimalwerten (Soll-Zustand) entspricht. Eine Anleitung zum Umgang mit dem Assessment Tool befindet sich im Tool selbst.

Beispiel: Cyber Security Maturity Rating

Overall Cyber Security Maturity Rating	Ist	Soll
Identifizieren (Identify)	2.8	2.6
Schützen (Protect)	2.7	2.6
Erkennen (Detect)	2.9	2.6
Reagieren (Respond)	2.0	2.6
Wiederherstellen (Recover)	1.4	2.6

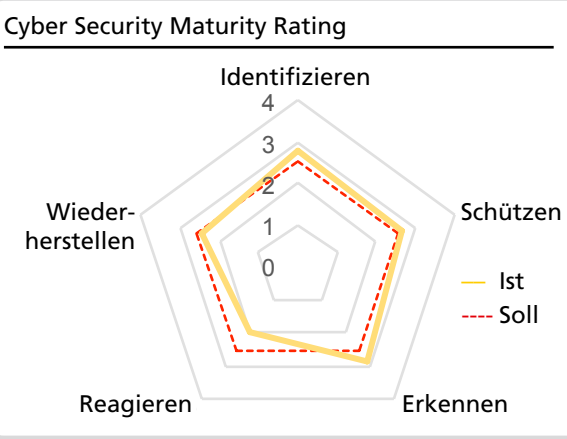


Abbildung 6: Beispiel Overall Cybersecurity Maturity Rating

4.4 Identifizieren (Identify [ID])

Inventar Management (Asset Management [AM])

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 7: Aufgaben ID.AM

Standard	Referenz
CCS CSC 1	1, 2, 12, 13, 14, 17,19
COBIT 5	BAI09.01, BAI09.02, BAI09.05, DSS05.02, APO02.02, APO10.04, DSS01.02, APO03.03, APO03.04, APO12.01, BAI04.02, APO01.02, APO07.06, APO13.01, 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, A.12.5.1, A.13.2.1, A.13.2.2
NIST-SP-800-53 Rev. 4	AC-4, CA-3, CA-9, PL-8, CM-8, PM-5, AC-20, SA-9, CP-2, RA-2, SA-14, SC-6, PS-7, PM-11

Tabelle 8: Referenzen ID.AM

Geschäftsumfeld (Business Environment [BE])

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	Abhängigkeiten und kritische Funktionen für kritische Dienstleistungen sind etabliert.
ID.BE-5	Resilienz Anforderungen für kritische Dienstleistungen sind etabliert.

Tabelle 9: Aufgaben ID.BE

Standard	Referenz
CCS CSC 1	1, 2
COBIT 5	APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05, APO02.06, APO03.01, APO02.01, APO10.01, BAI04.02, BAI03.02, DSS04.02, BAI09.02
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	SA-12, CP-2, SA-14, CP-2, PM-11, PM-8, CP-8, PE-9, PE-11, CP-11, SA-13

Tabelle 10: Referenzen ID.BE

Vorgaben (Governance [GV])

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 Cyber-Risiken Teil des unternehmensweiten Risikomanagements sind.

Tabelle 11: Aufgaben ID.GV

Standard	Referenz
COBIT 5	APO13.01, APO01.02, APO10.03, DSS05.04, APO13.02, MEA03.01, MEA03.04, DSS04.02, BAI02.01, EDM03.02, APO12.02, APO12.05
ISA 62443-3:2013	
ISO 27001:2013	A.5.1.1, A.6.1.1, A.7.2.1, A.15.1.1, A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5, Clause 6
NIST-SP-800-53 Rev. 4	PM-1, PM-2, PS-7, PM-9, PM-10, PM-11, Rev.4-1 controls from all security control families, SA-2, PM-3, PM-7

Tabelle 12: Referenzen ID.GV

Risikomanagement (Risk Assessment [RA])

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 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 13: Aufgaben ID.RA

Standard	Referenz
COBIT 5	APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02, BAI08.01, 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, Clause 6.1.2, A.16.1.6, Clause 6.1.3
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, PM-4

Tabelle 14: Referenzen ID.RA

Risikomanagement-Strategie (Risk Management Strategy [RM])

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 von den beteiligten Personen/Anspruchsgruppen bestätigen.
ID.RM-2	Definieren und kommunizieren Sie das maximal tragbare Risiko ihrer Organisation.
ID.RM-3	Stellen Sie sicher, dass die Definition des maximal tragbaren Risikos unter der Berücksichtigung der Bedeutung als kritischer Infrastruktur und unter Einbezug von sek-torspezifischen Risikoanalysen erstellt wurde.

Tabelle 15: Aufgaben ID.RM

Standard	Referenz
COBIT 5	APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02, APO12.06, APO12.02
ISA 62443-3:2013	4.3.4.2, 4.3.2.6.5
ISO 27001:2013	Clause 6.1.3, Clause 8.3, Clause 9.3
NIST-SP-800-53 Rev. 4	PM-8, PM-9, PM-11, SA-14

Tabelle 16: Referenzen ID.RM

Lieferketten-Risikomanagement (Supply Chain Riskmanagement [SC])

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 Supply Chain Risiken. Lassen Sie diese Prozesse durch alle beteiligten Anspruchsgruppen überprüfen und holen Sie ihre Zustimmung ein.
ID.SC-2	Identifizieren und priorisieren Sie Lieferanten und Dienstleistungsanbieter ihrer kritischen Systeme, Komponenten und 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 dem Supply Chain Risikomanagement-Prozess zu erfüllen.
ID.SC-4	Etablieren Sie ein Monitoring um sicherzustellen, dass all Ihre Lieferanten und Dienstleister ihre Verpflichtungen gemäss den Vorgaben erfüllen. Lassen Sie sich dies regelmässig durch Audit-Berichte oder technische Prüfergebnisse bestätigen.
ID.SC-5	Definieren Sie mit Ihren Lieferanten und Dienstleistern Reaktions- und Widerherstellungsprozesse nach Cybersecurity-Vorfällen. Testen Sie diese Prozesse in Übungen.

Tabelle 17: 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, BAI01.03, BAI02.03, BAI04.02, APO10.03, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05, DSS04.04
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
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-14, SA-15, SA-11, AU-2, AU-6, AU-12, AU-16, PS-7, CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9

Tabelle 18: Referenzen ID.SC

4.5 Schützen (Protect [PR])

Zugriffsmanagement und -steuerung (Access Control [AC])

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	Aktivität
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 Identitäten überprüft und bestätigt sind und nur bestätigten Berechtigungs-stufen und Zugangsdaten zugeordnet sind.

Tabelle 19: Aufgaben PR.AC

Standard	Referenz
COBIT 5	DSS05.04, DSS06.03, DSS01.04, DSS05.05, APO13.01, DSS01.04, DSS05.03, DSS01.05, DSS05.02, DSS05.07, DSS05.10, DSS06.10
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, SR 1.10
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.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8, A.6.2.1, A.6.2.2, A13.1.1, A.13.2.1, A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, 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.13.1.3, A.14.1.2, A.14.1.3, A.9.3.1, A.18.1.4, A.9.4.1, A.9.4.4
NIST-SP-800-53 Rev. 4	AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, AC-17, AC-19, AC-20, SC-15, AC-3, AC-5, AC-6,AC-14, AC-16, AC-24, AC-4, AC-10, SC-7, AC-7, AC-8, AC-9, AC-11, AC-12, AC-14

Tabelle 20: Referenzen PR.AC

Sensibilisierung und Ausbildung (Awareness and Training [AT])

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

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

Tabelle 21: Aufgaben PR.AT

Standard	Referenz
COBIT 5	APO07.03, BAI05.07, APO07.02, DSS05.04, DSS06.03, APO07.06, APO10.04, APO10.05, EDM01.01, APO01.02
ISA 62443-3:2013	4.3.2.4.2, 4.3.2.4.3
ISO 27001:2013	A.7.2.2, A.12.2.1, A.6.1.1, A.7.2.1
NIST-SP-800-53 Rev. 4	AT-2, AT-3, PM-13, PS-7, SA-9, SA-16, IR-2

Tabelle 22: Referenzen PR.AT

Datensicherheit (Data Security [DS])

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 IT-Betriebsmittel ein formaler Prozess etabliert ist, welcher die Daten bei Entfernung, Verschiebung oder Ersatz der Betriebsmittel schützt.
PR.DS-4	Stellen Sie sicher, dass Sie bezüglich der Verfügbarkeit der Daten über ausreichende Kapazitäts-reserven 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 23: Aufgaben PR.DS

Standard	Referenz
COBIT 5	APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06, DSS05.02, BAI09.03, APO13.01, BAI04.04, DSS05.04, DSS05.07, DSS.06.02, BAI03.08, BAI07.04, BAI03.05
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, SR 3.3
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.11.2.5, A.12.1.3, A.17.2.1, 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.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.3, A.13.2.1, A.13.2.4, A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3A.14.2.4, A.12.1.4, A.11.2.4
NIST-SP-800-53 Rev. 4	MP-8, SC-12, SC-28, SC-8, SC-11, 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-13, SC-31, SI-4, SI-7, SC-16, CM-2, SA-10

Tabelle 24: Referenzen PR.DS

Informationsschutzrichtlinien (Information Protection Processes and Procedures [IP])

Stellen Sie sicher, dass Daten während der Übertragung (vor Verletzungen der Vertraulichkeit, Integrität und Verfügbarkeit) geschützt sind.

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 die Entwicklung von Systemen.
PR.IP-3	Etablieren Sie einen Prozess zur Kontrolle von Konfigurationsänderungen.
PR.IP-4	Stellen Sie sicher, dass Sicherungen (Backups) Ihrer Informationen regelmässig durchgeführt, bewirtschaftet und getestet werden (Rückspielbarkeit der Backups testen).
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 Informationsschutzprozesse kontinuierlich weiterentwickelt und verbessert werden.
PR.IP-8	Tauschen Sie sich bezüglich der Effektivität verschiedener Schutztechnologien mit Ihren Partnern aus.
PR.IP-9	Etablieren Sie Prozesse zur Reaktion auf eingetretene 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 25: Aufgaben PR.IP

Standard	Referenz
COBIT 5	BAI10.01, BAI10.02, BAI10.03, BAI10.05, APO13.01, BAI03.01, BAI03.02, BAI03.03, BAI06.01, BAI01.06, APO13.01, DSS01.01, DSS04.07, DSS01.04, DSS05.05, BAI09.03, DSS 05.06, APO11.06, APO12.06, DSS04.05, BAI08.04, DSS03.04, DSS04.03, DSS04.04, APO07.01, APO07.02, APO07.03, APO07.04, APO07.05, BAI03.10, DSS05.02
ISA 62443-3:2013	SR 7.6, SR 7.3, SR 7.4, SR 4.2, SR 3.3
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, Clause 9, Clause 10, A.16.1.1, A.17.1.1, A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4, A.17.1.2, A.17.1.3, A.12.6.1, A.16.1.3, A.18.2.2, A.18.2.3
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-11, SA-12, SA-15, SA-17, PL-8, SI-12, SI-13, SI-14, SI-16, SI-17, CP-4, CP-6, CP-9, PE-10, PE-12, PE-13, PE-14, PE-15, PE-18, MP-6, CA-2, CA-7, CP-2, IR-8, PL-2, PM-6, AC-21, SI-4, CP-7, CP-12, CP-13, IR-7, IR-9, PE-17, IR-3, PM-14, PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21, RA-3, RA-5, SI-2

Tabelle 26: Referenzen PR.IP

Unterhalt (Maintenance [MA])

Stellen Sie sicher, dass Unterhalts- und Reparaturarbeiten an Komponenten des IT- 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 27: Aufgaben PR.MA

Standard	Referenz
COBIT 5	BAI03.10, BAI09.02, BAI09.03, DSS01.05, DSS05.04
ISA 62443-3:2013	
ISO 27001:2013	A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6, A.15.1.1, A.15.2.1
NIST-SP-800-53 Rev. 4	MA-2, MA-3, MA-4, MA-5, MA-6

Tabelle 28: Referenzen PR.MA

Einsatz von Schutztechnologie (Protective Technology [PT])

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

Bezeichnung	Aufgabe
PR.PT-1	Definieren Sie Vorgaben zu Audits und Log-Aufzeichnungen. Erstellen und prüfen Sie die regelmässigen Logs gemäss den Vorgaben und Richtlinien.
PR.PT-2	Stellen Sie sicher, dass Wechseldatenträger geschützt sind und dass sie nur gemäss den Richtlinien eingesetzt werden.
PR.PT-3	Stellen Sie sicher, dass Ihr System so konfiguriert ist, dass jederzeit eine Minimalfunktionalität gewährleistet wird (Systemhärtung).
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 29: Aufgaben PR.PT

Standard	Referenz
COBIT 5	APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01, DSS05.02, DSS05.06, APO13.01, DSS05.05, DSS06.06, BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05
ISA 62443-3:2013	SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 2.3, 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.8.2.1, 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.14.1.3, A.17.1.2, A.17.2.1
NIST-SP-800-53 Rev. 4	AU Family, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8, AC-3, CM-7, AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43, CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6

Tabelle 30: Referenzen PR.PT

4.6 Erkennen (Detect [DE])

Auffälligkeiten und Vorfälle (Anomalies and Events [AE])

Stellen Sie sicher, dass Auffälligkeiten (abnormales 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	Determinieren Sie die Auswirkungen möglicher Events.
DE.AE-5	Definieren Sie die Schwellenwerte, ab denen Cybersecurity-Vorfälle zu einer Alarmierung führen.

Tabelle 31: Aufgaben DE.AE

Standard	Referenz
COBIT 5	DSS03.01, DSS05.07, APO12.06, BAI08.02
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	A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2, A.12.4.1, A.16.1.1, A.16.1.4, A.16.1.7
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, CP-2, RA-3

Tabelle 32: Referenzen DE.AE

Überwachung (Security Continuous Monitoring [CM])

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 Cyber-Aktivitäten der Mitarbeitenden, um potentielle Cybersecurity-Vorfälle zu entdecken.
DE.CM-4	Stellen Sie sicher, dass Schadsoftware entdeckt werden kann.
DE.CM-5	Stellen Sie sicher, dass 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 33: Aufgaben DE.CM

Standard	Referenz
COBIT 5	DSS05.07, DSS05.01, APO07.06, BAI03.10, DSS01.03, DSS03.05, DSS01.04, DSS01.05, APO10.05, DSS05.02, DSS05.05
ISA 62443-3:2013	SR 6.2, SR 3.2, SR 2.4
ISO 27001:2013	A.11.1.1, A.11.1.2, A.12.4.1, A.12.4.3, A.12.2.1, A.12.5.1, A.12.6.2, 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, SI-8, SC-18, SC-44, PS-7, SA-4, SA-9, CM-8, PE-3, PE-6, PE-20, RA-5

Tabelle 34: Referenzen DE.CM

Detektionsprozess (Detection Processes [DP])

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 all ihre Vorgaben und Bedingungen erfüllen.
DE.DP-3	Testen Sie Ihre Detektionsprozesse.
DE.DP-4	Kommunizieren Sie detektierte Events an die zuständigen Stellen (z. B. Lieferanten, Kunden, Partner, Behörden etc.).
DE.DP-5	Verbessern Sie Ihre Detektionsprozesse kontinuierlich.

Tabelle 35: Aufgaben DE.DP

Standard	Referenz
COBIT 5	APO01.02, DSS05.01, DSS06.03, DSS06.01, MEA03.03, MEA03.04, APO13.02, DSS05.02, APO08.04, APO12.06, DSS02.05, APO11.06, DSS04.05
ISA 62443-3:2013	SR 3.3, SR 6.1
ISO 27001:2013	A.6.1.1, A.7.2.2, A.18.1.4, A.18.2.2, A.18.2.3, A.14.2.8, A.16.1.2, A.16.1.3, A.16.1.6
NIST-SP-800-53 Rev. 4	CA-2, CA-7, PM-14, AC-25, SA-18, SI-3, SI-4, PE-3, PM-14, AU-6, RA-5, PL-2

Tabelle 36: Referenzen DE.DP

4.7 Reagieren (Respond [RS])

Reaktionsplanung (Response Planning [RS])

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 37: Aufgaben RS.RP

Standard	Referenz
COBIT 5	APO12.06, 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

Tabelle 38: Referenzen RS.RP

Kommunikation (Communications [CO])

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 das Reporting und stellen Sie sicher, dass Cybersecurity-Vorfälle gemäss diesen Kriterien gemeldet und bearbeitet werden.
RS.CO-3	Teilen Sie Informationen und Erkenntnisse zu detektierten Cybersecurity-Vorfällen gemäss den definierten Kriterien.
RS.CO-4	Koordinieren Sie sich mit all Ihren Anspruchsgruppen gemäss den vordefinierten Kriterien.
RS.CO-5	Sorgen Sie für ein gesteigertes Bewusstsein hinsichtlich Cybersecurity-Vorfällen, indem Sie sich regelmässig mit Ihren Partnern austauschen.

Tabelle 39: Aufgaben RS.CO

Standard	Referenz
COBIT 5	EDM03.02, APO01.02, APO12.03, DSS01.03, DSS03.04, BAI08.04
ISA 62443-3:2013	
ISO 27001:2013	A.6.1.1, A.7.2.2, A.16.1.1, A.6.1.3, A.16.1.2, Clause 7.4, Clause 16.1.2, A.6.1.4
NIST-SP-800-53 Rev. 4	CP-2, CP-3, IR-3, IR-8, AU-6, IR-6, CA-2, CA-7, IR-4, PE-6, RA-5, SI-4, SI-5, PM-15

Tabelle 40: Referenzen RS.CO

Analyse (Analysis [AN])

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 41: Aufgaben RS.AN

Standard	Referenz
COBIT 5	DSS02.04, DSS02.07, DSS02.02, APO12.06, DSS03.02, DSS05.07, EDM03.02
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, AU-7, IR-8, SI-5, PM-15

Tabelle 42: Referenzen RS.AN

Schadensminderung (Mitigation [MI])

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 43: Aufgaben RS.MI

Standard	Referenz
COBIT 5	APO12.06
ISA 62443-3:2013	SR 5.1, SR 5.2, SR 5.4
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

Tabelle 44: Referenzen RS.MI

Verbesserungen (Improvements [IM])

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 45: Aufgaben RS.IM

Standard	Referenz
COBIT 5	BAI01.13, DSS04.08
ISA 62443-3:2013	
ISO 27001:2013	A.16.1.6, Clause 10
NIST-SP-800-53 Rev. 4	CP-2, IR-4, IR-8

Tabelle 46: Referenzen RS.IM

4.8 Wiederherstellen (Recover [RC])

Wiederherstellungsplanung (Recovery Planning [RP])

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 wird.

Tabelle 47: Aufgaben RC.RP

Standard	Referenz
COBIT 5	APO12.06, 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 48: Referenzen RC.RP

Weiterentwicklung der Widerherstellungsprozesse (Improvements [IM])

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

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

Tabelle 49: Aufgaben RC.IM

Standard	Referenz
COBIT 5	APO12.06, BAI05.07, DSS04.08, BAI07.08
ISA 62443-3:2013	
ISO 27001:2013	A.16.1.6, Clause 10
NIST-SP-800-53 Rev. 4	CP-2, IR-4, IR-8

Tabelle 50: Referenzen RC.IM

Weiterentwicklung der Kommunikationprozesse (Communications [CO])

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

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

Tabelle 51: Aufgaben RC.CO

Standard	Referenz
COBIT 5	EDM03.02, MEA03.02, APO12.06
ISA 62443-3:2013	
ISO 27001:2013	
NIST-SP-800-53 Rev. 4	CP-2, IR-4

Tabelle 52: Referenzen RC.CO

Schlussfolgerungen

Defense in Depth legt einen hohen Wert auf den risikobasierten Ansatz, der es jedem Unternehmen oder jeder Organisation ermöglicht die Risikobereitschaft selbst zu definieren und Massnahmen zur Verbesserung von Risiken selbst auszuwählen und zu priorisieren. Die Verantwortung für Cybersecurity bleibt weiterhin bei den Unternehmen selbst. Dieses Handbuch Cybersecurity bietet mit dem NIST Cybersecurity Framework Core ein Werkzeug, mit welchem die Akteure/innen des öffentlichen Verkehrs die Resilienz ihrer IKT-abhängigen Prozesse stärken können. Etliche weitere Anwendungsmöglichkeiten sind denkbar (Benchmarking, Informationsaustausch innerhalb der Branche/nationale Datenbank, Gap-Analysen, 3rd Party Audits etc.). In der praktischen Anwendung und im Austausch mit Akteuren/innen, Verbänden und Bund werden sich die Chancen weiterer Anwendungsmöglichkeiten zeigen.

Neben dem hier vorliegenden Handbuch Cybersecurity stellt die Wirtschaftliche Landesversorgung den Betrieben des öffentlichen Verkehrs einen IKT-Minimalstandard als Excel-basiertes Assessment Tool zur Verfügung[7]. Zur Einschätzung des Maturitätsniveaus des Unternehmens oder der Organisation ist insbesondere das Assessment Tool hilfreich. Der hier vorliegende Teil (Handbuch Cybersecurity) ist als Begleitdokument zu verstehen, welches an das Thema heranführt und bei Fragen herangezogen werden kann.

Das Handbuch ist keine Vorgabe, sondern soll die Akteure/innen des öffentlichen Verkehrs zur eigenen Reflektion hinsichtlich Cybersecurity anregen. IKT-Sicherheit ist kein Zustand, sondern ein Prozess. Das Handbuch Cybersecurity soll diesen Prozess anstossen und bei der Umsetzung helfen.

[7] *Download unter: https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html*

Anhang

6.1 Empfehlungen zur Verbesserung der Informationssicherheit

Das in dieser Branchenempfehlung vorgeschlagene Assessment Framework sowie das Assessment Tool offerieren eine umfassende Unterstützung zur Erhebung und Verbesserung der Informationssicherheit im Unternehmen. Informationssicherheit umfasst sämtliche Prozesse, Methoden und Regeln zur Gewährleistung von Vertraulichkeit, Korrektheit und Verfügbarkeit von Informationen. Dies gilt sowohl analog und digital. Cybersecurity ist ein Aspekt der Informationssicherheit. Es bestehen Überschneidungen der beiden Aufgaben. Zur Cybersecurity gehört z. B. auch der Schutz vor Unfällen (Zugskollisionen) während die Informationssicherheit z. B. auch persönliche Äusserungen von Mitarbeitern umfasst.

Organisationen mit entsprechenden Ressourcen und ausgebildeten Mitarbeitern werden keine Schwierigkeiten haben, diese Empfehlung umzusetzen. Möglicherweise werden Unternehmen des öffentlichen Verkehrs bereits das in diesem Dokument vorgeschlagene Framework oder ein anderes umgesetzt haben:

Technik

Technische Lösungen steigern die Komplexität und kosten viel. Es macht Sinn auf Good Practice-Massnahmen zu setzen und auf teure Experimente zu verzichten.

Beispiele:

- Zwei Rechencenter an verschiedenen Standorten; redundante Systeme;
- Verschlüsselung mobile Geräte;
- Firewall, Webfilter, Malware Protection;
- Sandbox;
- Network Access Control System;
- Mobile Device Management Software;
- elektronisches Zutrittssystem.

Organisation

Organisatorische Massnahmen werden dort eingesetzt, wo technische Massnahmen nicht sinnvoll und zu komplex sind.

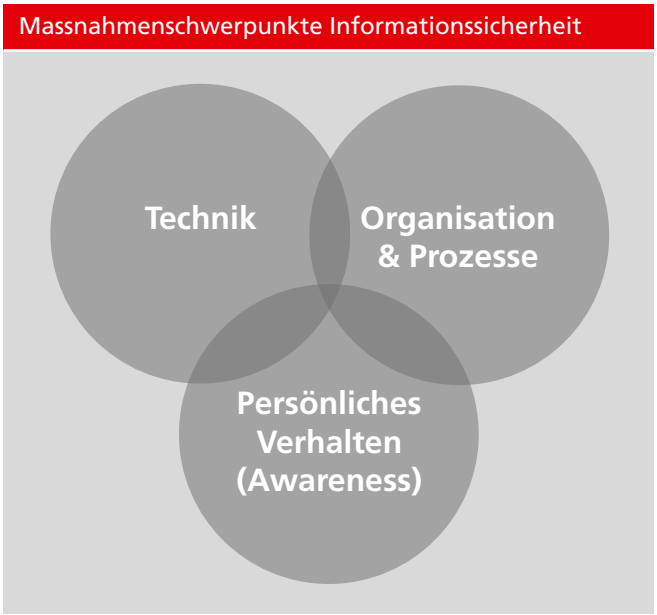


Abbildung 7: Massnahmenschwerpunkte Informationssicherheit

Beispiele:

- Prozess der Vergabe von Berechtigungen (4 Augenprinzip/doppelte Unterschrift);
- Notfallvorsorge (z. B. Szenarien, Alarmierung, Organisation, Sofortmassnahmen, vorbehaltene Entschlüsse, Notfallbetrieb, Rückkehr zum Normalbetrieb);
- Geheimhaltungsvereinbarung mit Mitarbeitenden;
- Vertraulichkeitsvereinbarung mit externen Partnern;
- Dokumentenklassifizierung;
- Entsorgungskonzept.

Persönliches Verhalten

Der Mensch kann neue Angriffsverfahren erkennen und entsprechende Schutzmechanismen einführen. Der Mensch ist aber auch eine der grössten Bedrohungen. Durch Sensibilisierung zum verantwortungsbewussten Umgang mit Informationen und Appell an die Eigenverantwortung sollen die Mitarbeitenden zur Verbesserung der Informationssicherheit beitragen.

Beispiele:

- Notebook und Aktenkoffer immer im Kofferraum verstauen;
- Starke Passwörter verwenden;
- Vorsicht im Umgang mit unbekannten E-Mails;
- Vertrauliche Papierdokumente zerstören (z. B. Shredder-Maschine) und nicht einfach in den Papierkorb werfen;
- Keine vertraulichen Telefongespräche im öffentlichen Raum.

6.2 Grundlagen, Dokumente und Standards

Vorliegendes Handbuch Cybersecurity berücksichtigt Konzepte, Empfehlungen und Massnahmen von verschiedenen Standards und anderen normativen Dokumenten (Tabelle 52)

Titel	Jahr	Herausgeber & Beschreibung
Massnahmen zum Schutz von industriellen Kontrollsystemen (SCADA)	2013	Hrsg.: **Melde- und Analysestelle Informationssicherung MELANI** Diese Anleitung beschreibt basierend auf US amerikanischen Unterlagen vom Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) sowie dem National Institute of Standards and Technology (NIST) knapp und pragmatisch auf 8 Seiten die wichtigsten 11 Massnahmen, die SCADA-Betreiber umsetzen müssen.
Risiko- und Verwundbarkeitsanalyse des Teilsektors	2015/ 2017	Hrsg.: **Bundesamt für wirtschaftliche Landesversorgung (BWL)** Die Risiko- und Verwundbarkeitsanalyse ist basierend auf der Nationalen Cyber Strategie (NCS) und der Strategie zum Schutz kritischer Infrastrukturen (SKI) entwickelt worden. Ziel ist die Analyse der Verwundbarkeit gegenüber Ausfällen oder Störungen der IKT.
Leitfaden Schutz kritischer Infrastrukturen (Leitfaden SKI)	2015	Hrsg.: **Bundesamt für Bevölkerungsschutz (BABS)** Der Leitfaden stellt ein Instrument zur Überprüfung und gegebenenfalls Verbesserung der Resilienz der kritischen Infrastrukturen dar. Insbesondere ist er in Hinblick auf die Anwendung in kritischen Teilsektoren durch Betreiber, Branchenverbänden und Fachbehörden konzipiert. Im Wesentlichen beschreibt der Leitfaden ein mögliches Risikomanagement-Vorgehen: Analyse (Ressourcen-Identifikation, Verwundbarkeiten, Risiken), Bewertung, Massnahmen sowie deren Sicherstellung (Umsetzung, Überprüfung, Verbesserung). Das Vorgehen kann durchaus bzw. sollte gar in bestehende Managementprozesse integriert oder darauf aufbauend ausgeführt werden.
Nationale Strategie zum Schutz kritischer Infrastrukturen (SKI)	2012	Hrsg.: **Bundesamt für Bevölkerungsschutz (BABS)** Die Strategie umschreibt den Geltungsbereich, bezeichnet die kritischen Infrastrukturen und hält die übergeordneten Grundsätze beim Schutz kritischer Infrastrukturen fest. Die nationale SKI-Strategie richtet sich an alle Stellen, die im Umfeld des Schutzes kritischer Infrastrukturen Verantwortlichkeiten aufweisen, insbesondere an die jeweils zuständigen Behörden, die politischen Entscheidungsträger und die Betreiber von kritischen Infrastrukturen.
Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)	2018	Hrsg.: **Informatiksteuerungsorgan des Bundes (ISB)** Da der Schutz der Informations- und Kommunikationsinfrastrukturen vor Cyber-Risiken im nationalen Interesse der Schweiz liegt, hat der Bundesrat die nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken in Auftrag gegeben. Diese Strategie soll aufzeigen, wie diese Risiken heute aussehen, wie die Schweiz dagegen gerüstet ist, wo die Mängel liegen und wie diese am wirksamsten und effizientesten zu beheben sind. Die Strategie identifiziert vorhandene Strukturen, definiert Zielsetzungen mit entsprechenden Massnahmen (z. B. Risiko- und Verwundbarkeitsanalysen eines Teilsektors).

Tabelle 53: Dokumente der Eidgenossenschaft, Verwaltungen sowie Verbänden.

Titel	Jahr	Herausgeber & Beschreibung
Bundesgesetz über die wirtschaftliche Landesversorgung (Landesversorgungs-gesetz, LVG)	2016	Hrsg.: **Die Bundesversammlung der Schweizerischen Eidgenossenschaft** Dieses Gesetz regelt Massnahmen zur Sicherstellung der Versorgung des Landes mit lebenswichtigen Gütern und Dienstleistungen in schweren Mangellagen, denen die Wirtschaft nicht selber zu begegnen vermag. Der Bund kann im Rahmen der bewilligten Mittel Massnahmen von privatrechtlichen und öffentlich-rechtlichen Unternehmen zur Sicherstellung der wirtschaftlichen Landesversorgung fördern, sofern die Massnahmen im Rahmen der Vorbereitung auf eine schwere Mangellage zu einer wesentlichen Stärkung lebenswichtiger Versorgungssysteme und Infrastrukturen beitragen. Eine dieser Massnahmen bildet das vorliegende Handbuch Cybersecurity.

Tabelle 53: Dokumente der Eidgenossenschaft, Verwaltungen sowie Verbänden.

Die folgende Tabelle zeigt eine weiterführende Auswahl an internationalen Standards die teilweise in das vorliegende Dokument eingeflossen sind.

Titel	Herausgeber & Beschreibung
ISO 27001 **Information technology – Security techniques – Information security management systems – Requirements**	Hrsg: **International Standard Organization (ISO)** Detailliert die Anforderungen an ein Information Security Management System (ISMS). Die ISO 27k Serie umfasst eine Reihe von *Information Security Standards,* wovon folgende hier von Interesse sind: • 27000 Übersicht und Vokabular • 27001 Anforderungen: Grundlagen mit Kontrollen und Kontrollzielen im Anhang • 27002 Leitfaden für Informationssicherheitsmassnahmen • 27003 Informationssicherheitsmanagementsysteme – Anleitung zur Umsetzung • 27005 Risikomanagement • 27019 Informationssicherheitsmassnahmen für die Energieversorgung Die ISO 27000 Security Normenreihe ist mittlerweile weit verbreitet und dürfte sich in den kommenden Jahren als die massgebende erweisen. Schon heute liegt durchaus richtig, wer ISO Security Standards befolgt. Im Gegensatz zu anderen Standards oder Frameworks, sind sie nicht so sehr detailliert, dementsprechend flexibel anwendbar und können über eine längere Zeitspanne kontinuierlich verbessert und erweitert werden. Das ISMS, der Inhalt der Massnahmen muss fachspezifisch adaptiert und umgesetzt werden.
ISO 27002 **Information technology – Security techniques – Code of practice for information security controls**	
ISO 22301 **Security and resilience – Business continuity management systems – Requirements**	Hrsg: **International Standard Organization (ISO)** Detailliert die Anforderungen an ein Business Continuity Management System.
IEC 62443 ff **Industrial communication networks – Network and system security**	Hrsg: **Internationale Elektrotechnische Kommission** Serie von insgesamt 13 *Industrial Automation and Control System (IACS)* Security Normen und technischen Spezifikationen. Die IEC 61508 ff. (Sicherheitsgrundnorm für programmierbare Steuerungssysteme) wird um das Thema Informationssicherheit erweitert und deckt das Thema für Automatisierung- und Steuerungssysteme für Industrieanlagen komplett und eigenständig ab. Es werden vier verschiedene Aspekte bzw. Ebenen der Informationssicherheit abgedeckt: • Allgemeine Aspekte wie Konzepte, Terminologie oder Metriken: IEC 62443-1-x • IT-Sicherheits-Management: IEC 62443-2-x • System-Ebene: IEC 62443-3-x • Komponenten-Ebene: IEC 62443-4-x Speziell zu erwähnen ist die Behandlung von Netzwerk- und Zonenarchitektur, die sich in anderen Standards kaum oder nicht so detailliert findet. Aktuell entwickelt sich diese Norm zur grundlegenden normativen Vorgabe im Kontext mit den RAMS-Normen der CENELEC (EN 50126 und weitere).

Tabelle 54: Nationale und internationale Standards zur IKT-Sicherheit

Titel	Herausgeber & Beschreibung
(pr)TS 50701 Bahnanwendungen – Cybersecurity	Hrsg.: **Europäische Komitee für elektrotechnische Normung** Ziel dieser Technischen Spezifikation ist es, den Nachweis zu erbringen, dass ein Eisenbahnsystem bei der Anwendung dieser Technischen Spezifikation aus Sicht der Cybersicherheit auf dem neuesten Stand ist, dass es das angestrebte Sicherheitsniveau erfüllt und dass es während des Betriebs und der Wartung aufrechterhalten werden kann. Die Basis bildet die IEC 62443 ff. Bei der Definition dieser Technischen Spezifikation wurden folgende Ziele verfolgt: • Erarbeiten von Leitlinien für Cybersicherheitsdokumente, zu liefernde Ergebnisse und Prozessschritte • muss an verschiedene Systemlebenszyklen angepasst werden können und diese unterstützen • muss für sicherheitsrelevante als auch für nicht sicherheitsrelevante Bahnsystemsysteme (Referenzarchitektur) anwendbar sein • muss die Identifikation und den Umgang mit Schnittstellen zwischen der Cybersicherheit und anderen Aufgaben im Systemlebenszyklus unterstützen • muss kompatibel und konsistent zur EN 50126 und weitere sein • muss die Safety-Zulassung und die Security-Zusicherung so weit wie möglich trennen, aber auch ermöglichen • muss eine harmonisierte und standardisierte Möglichkeit bieten, technische Informationssicherheitsanforderungen festzulegen • legt Konstruktionsprinzipien zur Förderung einfacher und modularer Systeme fest • ermöglicht die Verwendung von Produkten wie z. B. industriellen COTS gemäss IEC 62443 auf Komponenten-Ebene
IEC 62264 ff Enterprise Control System Integration	Hrsg.: **Internationale Elektrotechnische Kommission** Eine Normenreihe von insgesamt 4 Standards zur Integration von Unternehmens-IT und Kontroll- und Leitsystemen.
IEC 62351 ff Power systems management and associated information exchange – Data and communications security	Hrsg.: **Internationale Elektrotechnische Kommission** Die Normreihe IEC 62351 beschreibt den Standard für Sicherheit in Energiemanagementsystemen und zugehörigem Datenaustausch. Sie beschreibt Massnahmen um die vier Grundforderungen für sichere Datenkommunikation/Datenverarbeitung zu erfüllen.
BDEW Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme	Hrsg.: **BDEW Bundesverband der Energie- und Wasserwirtschaft e.V., Österreichs E-Wirtschaft** Das «BDEW-White» wurde für die grundsätzlichen Sicherheitsmassnahmen der Steuerungs- und Telekommunikationssysteme der Energiewirtschaft mit entwickelt. Das strategische Ziel des Whitepapers ist die positive Beeinflussung der Produktentwicklung für die oben genannten Systeme im Sinne der IT-Sicherheit und die Vermittlung eines gemeinsamen Verständnisses in der Branche für den Schutz dieser Systeme. Das BDEW-Whitepaper hat sich in der DACH-Region im Bahnstrombereich zu einer massgebenden Grundlage für die Beschaffung entwickelt. Das Whitepaper wird durch Ausführungshinweise ergänzt.

Tabelle 54: Nationale und internationale Standards zur IKT-Sicherheit

Titel	Herausgeber & Beschreibung
Guide to Industrial Control Systems (ICS) Security SP 800-82	Hrsg.: **National Institute of Standards and Technology (NIST)** Dieser Leitfaden gibt eine umfassende Einführung in SCADA-Topologien und -Architekturen, identifiziert Bedrohungen und Verwundbarkeiten und gibt Empfehlungen zu Gegenmassnahmen und Risikominderung. Zudem werden SCADA-spezifische Kontrollen basierend auf dem NIST 800-53 Framework präsentiert.
Framework for Improving Critical Infrastructure Cybersecurity	Hrsg.: **National Institute of Standards and Technology (NIST)** Dieses Framework stammt aus der Forderung der US Presidential Executive Order «Improving Critical Infrastructure Cybersecurity» aus dem Jahre 2013. Es ist eine Zusammenstellung verschiedener Guidelines, um den aktuellen Status in einem Unternehmen zu ermitteln und eine Roadmap zu verbesserten Cybersecurity-Praktiken mit Verweisen zu anderen Frameworks und Standards wie ISO27001, ISA 62443, NIST 800-53 und Cobit zu definieren.
Recommended Practice: Improving Industrial Control System Cybersecurity with Defense in Depth Strategies	Hrsg.: **Department of Homeland Security (DHS) Industrial Control** Systems Cyber Emergency Response Team (ICS-CERT) Umfassende Einführung in die Defense in Depth-Sicherheitsstrategie für industrielle Kontrollsysteme.
IT-Grundschutz-Kompendium – Werkzeug für Informationssicherheit	Hrsg.: **Bundesamt für Sicherheit in der Informationstechnik (BSI)** Das IT-Grundschutz-Kompendium ist die grundlegende Veröffentlichung des IT-Grundschutzes. Zusammen mit den BSI-Standards bildet es die Basis für die umfassende Beschäftigung mit dem Thema Informationssicherheit. Im Fokus des IT-Grundschutz-Kompendiums stehen die sogenannten IT-Grundschutz-Bausteine. Im ersten Teil der IT-Grundschutz-Bausteine werden mögliche Gefährdungen erläutert, im Anschluss wichtige Sicherheitsanforderungen. Die IT-Grundschutz-Bausteine sind in zehn unterschiedliche Schichten aufgeteilt und reichen thematisch von Anwendungen (APP) über Industrielle IT (IND) bis hin zu Sicherheitsmanagement (ISMS). Es werden jeweils unterschiedliche Schutzniveaus adressiert.
BSI-Standards	Hrsg.: **Bundesamt für Sicherheit in der Informationstechnik** Die BSI-Standards sind ein elementarer Bestandteil der IT-Grundschutz-Methodik. Sie enthalten Empfehlungen zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Massnahmen zu unterschiedlichen Aspekten der Informationssicherheit. Beispiele: BSI-Standard 200-1 über ISMS; 200-2 zur IT-Grundschutz-Vorgehensweise, 200-3: Risikoanalyse auf der Basis von IT-Grundschutz und im BSI-Standard 100-4 wird das Notfallmanagement im Sinne eines Leitfadens ausführlich behandelt.
BSI-Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz	Sicherheit kann nach den vom BSI entwickelten Vorgehensweisen des IT-Grundschutzes, aber auch nach Standards der ISO 27000-Familie eingeführt und kontrolliert werden. Beide Möglichkeiten sind von ihrem Ansatz her kompatibel. Mit beiden wird ein ISMS aufgebaut und betrieben, mit den Risiken im Bereich der Informationssicherheit ermittelt und durch geeignete Massnahmen auf ein akzeptables Mass reduziert werden.
Zuordnungstabelle ISO zum modernisierten IT-Grundschutz	Der IT-Grundschutz interpretiert im BSI-Standard 200-2 die Anforderungen bzw. Massnahmen der ISO-Normen 27001 sowie 27002. Die IT-Grundschutz-Anwender werden mit einer Zuordnungstabelle bei der Abbildung der Inhalte von der ISO 27001/2 auf den IT-Grundschutz unterstützt.

Tabelle 54: Nationale und internationale Standards zur IKT-Sicherheit

Titel	Herausgeber & Beschreibung
Industrielle Steuerungs- und Automatisierungssysteme (ICS) – Allgemeine Empfehlungen	Hrsg.: **Bundesamt für Sicherheit in der Informationstechnik (BSI)** Das Kompendium stellt ein Grundlagenwerk dar und soll einen einfachen Zugang zur SCADA IT Security ermöglichen. Es werden einige allgemeine Grundlagen der Automation erläutert, sowie auf Besonderheiten und Standards in diesem Bereich aufmerksam gemacht. Abgerundet wird das Thema durch eine Sammlung von Massnahmen und einer Vorgehensweise um die Umsetzung zu prüfen. Auf dieser Seite erhält der Anwender zusätzliche fachspezifische Hilfestellungen.
Zuordnungstabelle – Mapping of Dependencies to International Standards	Hrsg.: **European Union Agency for Network and Information Security (ENISA)** In diesem Bericht wurden die Abhängigkeiten und Zusammenhänge zwischen Betreibern von essentiellen Diensten (OES) und Anbietern digitaler Dienste (DSP) analysiert und eine Reihe von Indikatoren für ihre Bewertung ermittelt. Diese Indikatoren sind internationalen Standards und Rahmenbedingungen zugeordnet, nämlich ISO/IEC 27002, COBIT5, Sicherheitsmassnahmen der NIS-Kooperationsgruppe und NIST Cybersecurity Framework.
Communication Network Dependencies for ICS/SCADA Systems	Hrsg.: **European Union Agency for Network and Information Security (ENISA)** Dieser Bericht konzentriert sich auf die Aspekte der Kommunikationsnetze und der Interkommunikation zwischen ICS/SCADA und der Erkennung von Schwachstellen, Risiken, Bedrohungen und Sicherheitsauswirkungen, die durch cyberphysische Systeme verursacht werden können. Der Bericht enthält auch eine Reihe von Empfehlungen zur Minderung der identifizierten Risiken. Das wichtigste Ergebnis der vorgängigen Studie ist eine Liste von bewährten Praktiken und Richtlinien, um die Angriffsfläche von ICS/SCADA-Systemen so weit wie möglich zu begrenzen. Das Hauptziel des Dokumentes ist es, einen Einblick in die Kommunikationsnetzwerkabhängigkeiten der ICS/SCADA-Systeme zu geben sowie kritische Sicherheitsressourcen und realistische Angriffsszenarien und Bedrohungen gegen diese Kommunikationsnetze zu identifizieren.
ENISA Threat Landscape/ Taxonomy	Hrsg.: **European Union Agency for Network and Information Security (ENISA)** Die ENISA Threat Landscape bietet einen Überblick über Bedrohungen sowie aktuelle und sich abzeichnende Trends. Sie basiert auf öffentlich zugänglichen Daten und bietet eine unabhängige Ansicht zu beobachteten Bedrohungen, Bedrohungsakteuren und Bedrohungstrends. In der Taxonomy werden die Bedrohungen systematische zusammengestellt.
Branchenanforderungen an die IT-Sicherheit (VDV Schrift 400)	Hrsg.: **Verband Deutscher Verkehrsunternehmen (VDV)** Das Dokument beschreibt Anforderungen an die IT-Sicherheit möglicher Anlagen kritischer Infrastrukturen. Sie gibt eine Orientierung zur möglichen Vorgehensweise bei der Umsetzung dieser Anforderungen durch geeignete Methoden, Prozesse und Verfahrensweisen. Mit der vorliegenden Schrift stellt der VDV seinen Mitgliedern einen branchenspezifischen Sicherheitsstandard (B3S) zur Verfügung, der sich an den Orientierungshilfen des BSI orientiert.

Tabelle 54: Nationale und internationale Standards zur IKT-Sicherheit

6.3 Weiterentwicklung der Standards

Der technologische Fortschritt und stetige Veränderungen im öffentlichen Verkehr erfordern die laufende Weiterentwicklung der Standards. Folgende Neuerungen sind zum Zeitpunkt der Erstellung des vorliegenden Handbuchs bekannt:

- AB-EBV 2020 Art. 5c: Ein Security Management System (ISMS) wird neu gefordert. Die Nutzung von Standards wird empfohlen.
- Interoperabilitätsrichtlinie der EU: Es ist vorgesehen, dass das Thema Cybersecurity in noch unbestimmten Umfang und Inhalt in den neuen TSI 2022 berücksichtigt wird.
- CENELEC prTS 50701 (vgl. Tabelle 54): Der Standard geht Mitte 2020 in den letzten Review.

6.4 Abkürzungsverzeichnis

Abkürzung	Beschreibung
AB-EBV	Ausführungsbestimmungen zur Eisenbahnverordnung
AC	Identity Management, Authentification and Access Control
AE	Anomalies and Events
AM	Asset Management
AN	Analysis
AT	Awareness and Training
ATP	Automatic Train Protection
BABS	Bundesamt für Bevölkerungsschutz
BAV	Bundesamt für Verkehr
BCM	Business Continuity Management (betriebliches Kontinuitätsmanagement)
BE	Business Environment
BIA	Business Impact Analyse
BLS	BLS AG (früher Bern-Lötschberg-Simplon-Bahn)
BSI	Bundesamt für Sicherheit in der Informationstechnik (Deutschland)
BTA	Betriebstechnische Anlage
BWL	Bundesamt für wirtschaftliche Landesversorgung
CAPRE	Capacity and Reservations (das Vorgängersystem hiess PLABE, Platzbewirtschaftungssystem)
CCTV	Closed-circuit television (Videoüberwachungssystem)
CENELEC	Comité Européen de Normalisation Électrotechnique (Europäisches Komitee für elektrotechnische Normung)

Tabelle 55: Abkürzungsverzeichnis

Abkürzung	Beschreibung
CM	Security Continous Monitoring
CO	Communications
COAT	CCS onboard application platform for trackside related functions
DAS	Driver Assistance System
DE	Detect
DMS	Dokumentenmanagementsystem
DMZ	Demilitarized Zone
DP	Detection Processes
DS	Data Security
EBG	Eisenbahngesetz
EMS	Energy Metering System
ENISA	European Union Agency for Network and Information Security
ERP	Enterprise Ressource Planning-System
ETCS	European Train Control System (Zugbeeinflussungssystem)
EVU	Eisenbahnverkehrsunternehmen
FTP	File Transfer Protocol
GIS	Geographisches Informationssystem
GSM	Global System for Mobile Communications
GSM-R	Global System for Mobile Communications – Rail(way)
GV	Governance
HVAC	Heating, Ventilation and Air Conditioning
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
ICS	Industrial Control System (industrielles Kontrollsystem; wird im vorliegenden Dokument als Synonym zu den Abkürzungen «OT» und «SCADA» verwendet)
ICT	Information and Communication Technology
ID	Identify
IDS	Intrusion Detection System
IKT	Informations- und Kommunikationstechnologie
IM	Improvements
IMS	Integriertes Management System
IP	Information Protection Processes and Procedures
IP	Internet Protocol
IPS	Intrusion Prevention System

Tabelle 55: Abkürzungsverzeichnis

Abkürzung	Beschreibung
ISA	Interconnection Security Agreement
ISA	International Society of Automation
ISB	Eisenbahninfrastrukturbetreiber
ISB	Informatiksteuerungsorgan des Bundes
ISMS	Information Security Management System
ISMS	Informationssicherheitsmanagementsystem
ISO	Internationale Organisation für Normung
IT	Informationstechnik/Information Technology
JRU	Juridical Recording Unit
KIS	Kundeninformationssystem
KPI	Key Performance Indicator
KTU	Konzessioniertes Transportunternehmen
LAN	Local Area Network
Leittechnik	Netz-, Stations-, Bahn- oder Kraftwerksleittechnik
MA	Maintenance
MCG	Mobile Communication Gateway
MELANI	Melde- und Analysestelle Informationssicherung (Informatiksteuerungsorgan des Bundes)
MI	Mitigation
MOU/MOA	Memorandum of Understanding/Agreement
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken
NeTS	Netzweites Trassen-System
NIS	Netz- und Informationssicherheit
NIST	National Institute of Standards and Technology
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
NMC	Network Management Center
OBM	Open-book Management
OBU	Onboard Unit
OC	Object Controller
OT	Operational Technology (wird im vorliegenden Dokument als Synonym zu den Abkürzungen «SCADA» und «ICS» verwendet)
PA	Public Address
PaaS	Platform as a Service
PBG	Personenbeförderungsgesetz

Tabelle 55: Abkürzungsverzeichnis

Abkürzung	Beschreibung
PIS	Passenger Information System
PR	Protect
PT	Protective Technology
RA	Risk Assessment
RailOpt	Planungsprogramm (zwischen Infrastruktur und Betriebsplanung)
RailSys	Planungsprogramm
RC	Recover
RCS	Rail Control System (Dispositionsebene)
ReSys	Reservierungssystem
RhB	Rhätische Bahn AG
RM	Risk Management Strategy
RoE	Rules of Engagement
RP	Recovery Planning
RS	Respond
RZ	Rechenzentrum
SaaS	Software as a Service
SBB	Schweizerische Bundesbahnen AG
SC	Supply Chain Riskmanagement
SCADA	Supervisory Control and Data Acquisition (wird im vorliegenden Dokument als Synonym zu den Abkürzungen «ICS» und «OT» verwendet)
sFTP	Secure File Transfer Protocol
SIEM	Security Incident and Event Management
SLA	Service Level Agreement (Dienstleistungsvereinbarung)
SOB	Schweizerische Südostbahn AG
SOC	Security Operation Center
SOPRE	Software zur Personal- und Rollmaterialplanung
SSH	Secure Shell
TCMS	Train Control and Management System
tl	Transports publics de la région lausannoise
TMS	Traffic Management System
TPF	Transports publics fribourgeois Holding (TPF) SA
TSI	Technical Specifications for Interoperability
TU	Transportunternehmung

Tabelle 55: Abkürzungsverzeichnis

Abkürzung	Beschreibung
UCC	Unified Communications and Collaboration
UGV	Universelle Gebäudeverkabelung
VBZ	Verkehrsbetriebe der Stadt Zürich
VoIP	Voice over IP
VöV	Verband öffentlicher Verkehr
VPB	Verordnung über die Personenbeförderung
WAN	Wide Area Network
WL	Wirtschaftliche Landesversorgung
WLAN	Wireless Local Area Network

Tabelle 55: Abkürzungsverzeichnis

6.5 Abbildungsverzeichnis

6.6 Tabellenverzeichnis

Autoren/innen und Fachexperten der Erstausgabe

Vorname, Name	Firma	Funktion
Hans-Peter Käser	BWL	Hauptautor/Projektleitung
Daniel Caduff	BWL	Co-Autor
Nathalie Gratzer	BWL	Co-Autorin
Marcus Griesser	WL/SBB	PL VöV/Co-Autor/Fachexperte
Patrick Favre	BAV	Fachexperte/Quality Assurance
Tobias Hubschmid	BAV	Fachexperte/Quality Assurance
Ulrich Schär	BAV	Fachexperte/Quality Assurance
Andreas Klopfenstein	BLS	Fachexperte/Quality Assurance
Daniel Noger	BLS	Fachexperte/Quality Assurance
Martin Wyss	BLS	Fachexperte/Quality Assurance
Stephan Berger	BLS	Fachexperte/Quality Assurance
Urs Hoerler	RhB	Fachexperte/Quality Assurance
Jean-Luc Nottaris	SBB	Fachexperte/Quality Assurance
Stefan Käser	SBB	Fachexperte/Quality Assurance
Olaf Zanger	SBB	Fachexperte/Quality Assurance
Peter Häberli	SOB	Fachexperte/Quality Assurance
Roland Kressbach	SOB	Fachexperte/Quality Assurance
Giorgio Anastopoulos	tl	Fachexperte/Quality Assurance
Marc Striffeler	TPF	Fachexperte/Quality Assurance
Marcel Gahler	VBZ	Fachexperte/Quality Assurance

Chronologie

Datum	Kurzbeschreibung
August 2019	Arbeitsaufnahme AG ICT-Security für kritische Infrastrukturen
September 2019 bis Juni 2020	Erarbeitung erster Entwurf des Dokumentes
Juni 2020	Freigabe Arbeitsgruppe
Juni bis Juli 2020	Konsultation VöV (Kommission Infrastruktur)
August 2020	Freigabe durch VöV

Haftungsausschluss

Das vorliegende Dokument mit Empfehlungen zur Verbesserung der Sicherheit von Informations- und Kommunikationssystemen des öffentlichen Verkehrs sowie die Systeme der Steuerung des öffentlichen Verkehrs wurde von den beteiligten Personen und Stellen nach bestem Wissen und Gewissen erstellt.

Das Bundesamt für wirtschaftliche Landesversorgung übernimmt keine Gewährleistung, weder ausdrücklich noch implizit. Dies trifft auch auf die involvierten Fachexperten, Unternehmen und Mitarbeitenden zu. Die Verantwortung für den sicheren Betrieb der IKT sowie die Haftung für mögliche Schäden liegt einzig bei dem/der Anwender/in.

Impressum und Kontakt

Herausgeber
Bundesamt für wirtschaftliche Landesversorgung BWL
Bernastrasse 28, CH-3003 Bern
info@bwl.admin.ch, www.bwl.admin.ch
Telefon +41 58 462 21 71

Konsultierter Verband
Verband öffentlicher Verkehr


Jeremias Gotthelf