Minimalstandard für die Sicherheit der Informations- und Kommunikations-technologie in der Lebensmittelversorgung

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Vorwort

Die zunehmende IT-Durchdringung und Vernetzung praktisch aller Lebensbereiche eröffnet Potenziale, auf die ein hochentwickeltes und industrialisiertes Land wie die Schweiz nicht verzichten kann. Gleichzeitig entstehen durch die Digitalisierung neue Risiken, welche adressiert werden müssen. Die Gefahr durch gezielte Cyber-Angriffe auf die IT-Infrastruktur betrifft staatliche Stellen ebenso wie Betreiber kritischer Infrastrukturen und andere Unternehmen, die mit besonders sensiblen Informationen umgehen.

Vorliegender «Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie in der Lebensmittelversorgung (IKT-Minimalstandard)» setzt dort an, wo sich eine moderne Gesellschaft Ausfälle am wenigsten leisten kann: bei den IKT-Systemen der kritischen Infrastrukturen. Dies gilt für die Lebensmittelversorgung ebenso wie beispielsweise die Energieversorgung oder das Gesundheitswesen. Der hier vorliegende IKT-Minimalstandard soll entsprechend Unternehmen aus der Lebensmittelbranche dabei unterstützen, IKT-Störungen zu vermeiden, bzw. diese rasch zu beheben.

Der IKT-Minimalstandard ist ein Branchendokument der Lebensmittelversorgung, welches anerkannte Richtlinien und Empfehlungen zur Verbesserung der IKT-Sicherheit beinhaltet. Diese wurden von Branchenexperten ausgearbeitet und werden künftig regelmässig aktualisiert. Die Empfehlungen werden von den Unternehmen der Branche im Sinne einer «Selbstregulierung» freiwillig umgesetzt. Der IKT-Minimalstandard richtet sich grundsätzlich an alle Unternehmen, die an Produktion, Verteilung, Import und Verarbeitung von Lebensmitteln beteiligt sind.

Anleitung zum Einsatz des IKT-Minimalstandards

Der IKT-Minimalstandard gliedert sich in mehrere Kapitel: Kapitel 1 und 2 bieten eine Einführung in die Lebensmittelversorgung. Kapitel 3 erläutert den Defense in Depth-Ansatz. Kapitel 4 und 5 beschreiben die umzusetzenden Massnahmen und stellen Hilfsmittel (insbesondere das Assessment Tool in Excel) zur Umsetzung vor.

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

Zusammenfassung

Die fortschreitende Digitalisierung und Zentralisierung in der Lebensmittelversorgung erhöhen gleichermassen die Effizienz der Verarbeiter und Detailhändler wie auch den Grad der Abhängigkeit von IKT-Systemen. So verwendet beispielsweise der Detailhändler für den gesamten Warenwirtschaftsfluss heute nur noch ein einziges System (Warenwirtschaftssystem), und auch die Kassen können nur noch mit Hilfe des digitalen Kassensystems bedient werden. Weiter stützen sich die Verarbeiter auch auf SCADA-Systeme (Supervisory Control and Data Acquisition), um ihre Produktion zu steuern und somit ihre Produkte herzustellen. Ein klares Verständnis der aktuellen Sicherheitsherausforderungen sowie der verfügbaren Gegenmassnahmen ist notwendig.

Der vorliegende IKT-Minimalstandard basiert auf dem NIST Framework Core[1] sowie den Erkenntnissen der Risiko- und Verwundbarkeitsanalyse der Lebensmittelversorgung des Bundesamtes für wirtschaftliche Landesversorgung.[2]

[1] Das NIST Framework Core 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.

[2] Risiko- und Verwundbarkeitsanalyse der Lebensmittelversorgung. Bundesamt für wirtschaftliche Landesversorgung, Bern 2016.

Inhaltsverzeichnis

Hintergrund und Überblick

Die wirtschaftliche Landesversorgung (WL), beziehungsweise das Bundesamt für wirtschaftliche Landesversorgung (BWL) überprüfte im Rahmen der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) die Lebensmittelversorgung auf IKT-Verwundbarkeiten. Die IKT-Verwundbarkeitsanalyse wurde gemeinsam von Bund und Privatwirtschaft erarbeitet und verifiziert. Den Kern der Analyse bilden die versorgungsrelevanten Prozesse der Lebensmittelbranche. In den Phasen Verarbeitung, Verteilung und Verkauf von Lebensmitteln bestehen Abhängigkeiten insbesondere von folgenden Systemen:

- **Enterprise Ressource Planning Systeme** (ERP): diese Systeme werden für die Erfassung sowie Bearbeitung unternehmensrelevanter Daten (Kapital, Personal, Betriebsmittel, Material, Informations- und Kommunikationstechnik usw.) verwendet. ERP-Systeme beinhalten je nach Bedürfnis des Unternehmens eines oder mehrere der folgenden Subsysteme.
- **Warenwirtschaftssysteme:** dies betrifft insbesondere die Systeme der Detailhändler, welche für den Bestellfluss und Nachschub eines grossen Teils der Lebensmittel notwendig sind.
- **Kassensysteme:** diese sind notwendig, damit die Lebensmittel in den Filialen verkauft und im Warenwirtschaftssystem erfasst werden können.
- **Prozesssteuerungssysteme** (SCADA): diese steuern sowohl die Produktion der Lebensmittel als auch die Kommissionierung in den Verteilzentren.
- **Tourenplanungssysteme:** diese Systeme werden verwendet, um die Transportmittel mit den richtigen Waren zu beladen und die entsprechenden Kunden effizient zu beliefern.
- **Finanztransaktionssysteme:** diese Systeme sind notwendig, um Finanztransaktionen durchzuführen und buchhalterisch festzuhalten.
- **Zollsysteme**
- **Lagerbewirtschaftungssysteme**
- **Kommunikationssysteme** (Telefon, E-Mail etc.)

Ergänzend sei darauf hingewiesen, dass auch die landwirtschaftliche Produktion zunehmend auf IKT-Systeme setzt. IKT-gesteuerte Melkroboter oder automatisierte Bewässerungs-, Fütterungs- und Belüftungsanlagen gewinnen an Bedeutung. Gemäss IKT-Verwundbarkeitsanalyse ist deren Wichtigkeit für die Lebensmittelversorgung heute noch zu relativieren.

Der IKT-Minimalstandard bietet Empfehlungen zur Stärkung der Resilienz der obengenannten Systeme. Diese wurden gemeinsam mit der IG Detailhandel Schweiz sowie der Swiss Retail Federation als Branchenempfehlung abgefasst und werden im Sinn einer Selbstregulierung von den Akteuren der Branche freiwillig umgesetzt.

1 Ausgangslage und Zielsetzung

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

1.1 Abgrenzungen

Der vorliegende IKT-Minimalstandard wurde durch die wirtschaftliche Landesversorgung in Zusammenarbeit mit externen Experten erarbeitet. Es existieren heute bereits mehrere international anerkannte Standards zur IKT-Sicherheit, die meist deutlich über das vorliegende Dokument hinausgehen (siehe Tabelle 53). Der IKT-Minimalstandard versteht sich explizit nicht als Konkurrenz zu existierenden internationalen Standards, sondern ist mit diesen kompatibel, bei gleichzeitig reduziertem Umfang. Er soll einen einfacheren Einstieg in die Thematik ermöglichen und trotzdem ein hohes Schutzniveau gewährleisten.

Die Branchenempfehlung fokussiert auf jene Unternehmens-Prozesse, welche einen direkten Einfluss auf die Versorgung der Schweizer Bevölkerung mit Lebensmitteln haben.

2 Die Lebensmittelversorgung der Schweiz

2.1 Übersicht über die Lebensmittelversorgung

In der Schweiz wird die Lebensmittelversorgung durch ein heterogenes Feld von Akteuren sichergestellt. So stellen eine hohe Anzahl an kleinen und mittleren Betrieben, die landwirtschaftlichen Produkte her. Dies ist insbesondere dadurch bedingt, dass sich das hügelige und alpine Gelände der Schweiz besser für kleine und mittlere als für grosse landwirtschaftliche Betriebe eignet. Jedoch bleibt eine Vielzahl von Kleinbetrieben in Tal- und Bergzonen hinter der Strukturentwicklung und Produktivitätssteigerung grösserer Betriebe zurück. Durch diese grosse Anzahl Akteure bestehen bei der Produktion von landwirtschaftlichen Produkten Redundanzen und damit eher eine geringe Verwundbarkeit gegenüber Cyber-Risiken.

Auch die Verarbeitung der landwirtschaftlichen Rohstoffe zu Lebensmitteln durch die Industrie wird durch eine grössere Anzahl an Akteuren durchgeführt. In der Schweizer Lebensmittelindustrie gibt es keinen Monopolisten, dessen Ausfall die Versorgung der Schweiz gesamtheitlich gesehen in Frage stellen würde. So verarbeiten beispielsweise mehrere hundert Käsereien Milch zu Käse. Vier grosse industrielle Verarbeiter stellen die Versorgung mit Schweizer Milchprodukten sicher.[3] Auch bei der Verarbeitung von Fleisch und Mineralwasser (Abfüllen in Flaschen) besteht eine Vielzahl von Unternehmen. Die Verarbeitung von Getreide sowie Ölsaaten zur Herstellung von Ölen und Fetten erfolgt in wenigen Unternehmen. Damit besteht bei der Herstellung von pflanzlichen Ölen (durch die drei grossen Ölmühlen) und Fetten ein deutlich höheres Klumpenrisiko. Für die Vermahlung von Getreide sind vier grosse Mühlenunternehmen verantwortlich.

Der Detailhandel wird von zwei Akteuren dominiert. Coop und Migros stellen gemeinsam über drei Viertel der Versorgung mit Lebensmitteln sicher. Sie spielen bei der Versorgung der Schweiz eine zentrale Rolle. Ein Ausfall eines grossen Detailhändlers – beispielsweise durch einen gezielten Cyber-Angriff auf das Bestellsystem oder das Kassensystem – hat das Potential, die Versorgung mit Lebensmitteln gesamtschweizerisch negativ zu beeinflussen. Die Logistik der Detailhändler und insbesondere die Verteilzentren sind essentiell für die Verteilung der Lebensmittel in die Filialen.

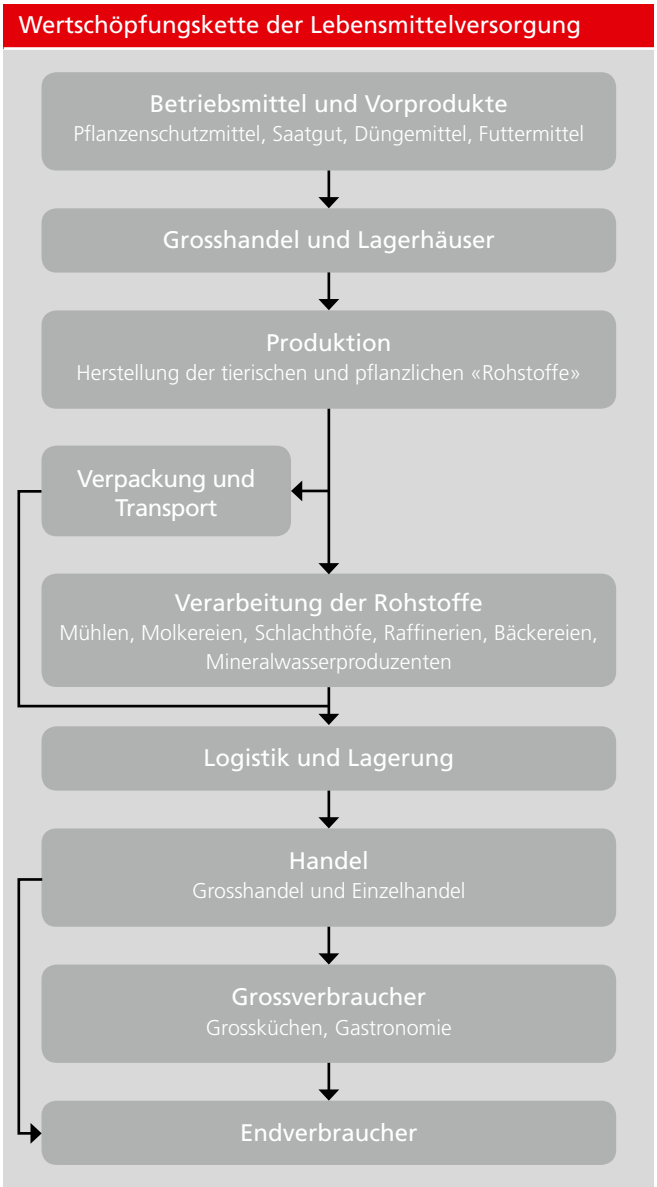

Abbildung 1: Wertschöpfungskette der Lebensmittelversorgung

[3] Emmi, Cremo, Hochdorf, Elsa. Daneben gibt es etwa 90 gewerbliche Molkereien.

2.2 Versorgungsleistung

Der Teilsektor Lebensmittelversorgung stellt die Versorgung der Schweizer Bevölkerung mit Lebensmitteln sicher. Jedem Unternehmen, welches dazu einen erheblichen Beitrag leistet, wird empfohlen, seine IKT-Systeme anhand des vorliegenden Standards zu sichern.

Der sechste Schweizerische Ernährungsbericht zeigt einen täglichen durchschnittlichen Energieverbrauch pro Person und Tag von 3'111 kcal auf.[4] Ein Blick auf die statistische Erhebung zeigt, dass vier Lebensmittelkategorien dazu einen wesentlichen Beitrag leisten (Abbildung 2). Zusätzlich wird die Versorgung mit Mineralwasser berücksichtigt, da Wasser elementarer Bestandteil der Lebensmittelversorgung ist:[5]

1. Getreide und Zucker (Kohlenhydrate)
2. Fleischprodukte (Fette und Proteine)
3. Milchprodukte[6] (Fette und Proteine)
4. Öle und Fette (Fette)
5. Mineralwasser

Der Schweizer Bürger verzehrt primär Lebensmittel aus diesen fünf Kategorien. Mit ihnen stillt er sein Bedürfnis nach den Makronährstoffen (Proteine, Fette und Kohlenhydrate). Die Verteilung der benötigten kcal auf Proteine, Fette und Kohlenhydrate ist essentiell für eine ausgewogene Ernährung. Die Versorgung mit Proteinen, Fetten und Kohlenhydraten erfolgt grösstenteils durch Getreide, Zucker, Fleisch, Milchprodukte sowie Öle und Fette (Tabelle 1). Diese Lebensmittelkategorien decken gemeinsam über 78% des Bedarfs an essentiellen Nährstoffen ab.[7]

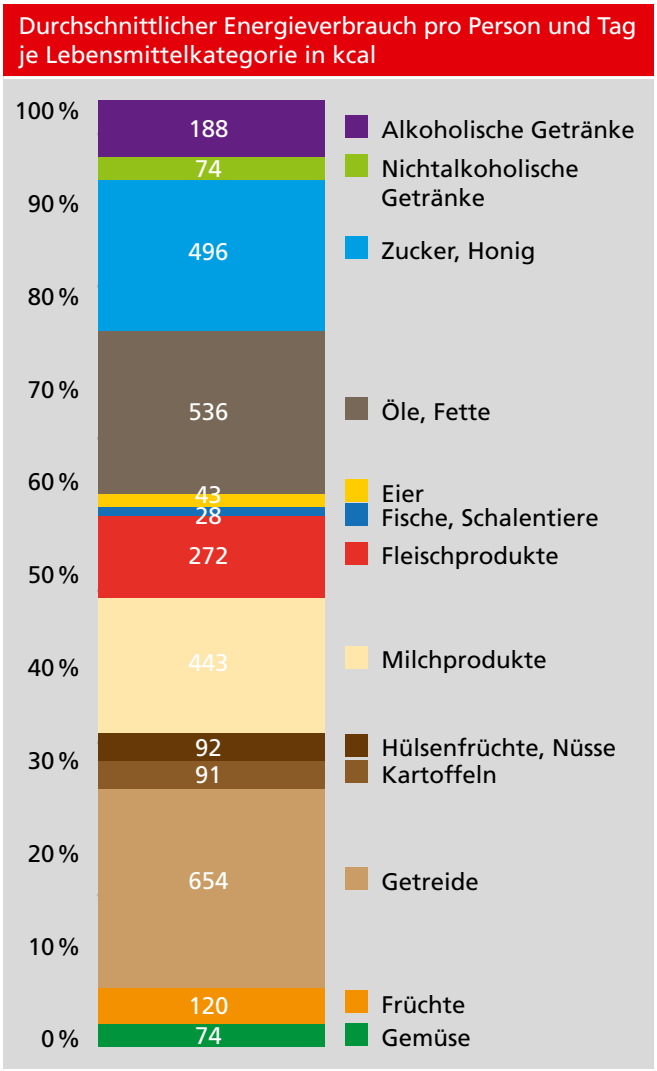

Abbildung 2: Durchschnittlicher täglicher Energieverbrauch pro Lebensmittelkategorie und Person in kcal

Proteine	%	Fette	%	Kohlenhydrate	%
Getreide	22,6 %	Fleisch	14,3 %	Getreide	38,6 %
Fleisch	27,9 %	Milchprodukte	22,9 %	Zucker	35,2 %
Milchprodukte	25,3 %	Öle und Fette	47,6 %		
Total	75,8 %	Total	84,8 %	Total	73,8 %

Tabelle 1: Qualitative Betrachtung der Lebensmittelversorgung

[4] Bundesamt für Gesundheit: Sechster Schweizerischer Ernährungsbericht, S. 82 ff.

[5] Für die Versorgung der Bevölkerung mit Trinkwasser, siehe IKT-Verwundbarkeitsanalyse Teilsektor Wasserversorgung; Bundesamt für wirtschaftliche Landesversorgung BWL; 2016

[6] Inklusive Butter.

[7] Bundesamt für Gesundheit: Sechster Schweizerischer Ernährungsbericht.

2.3 Übersicht der kritischen Prozesse

Der Lebensmittelsektor zeichnet sich insbesondere im Detailhandel und beim Verarbeiter der Lebensmittel durch eine durchgehend hohe Abhängigkeit von IKT-Systemen aus. In allen Prozessen der Detailhändler gelangen IKT-Systeme zum Einsatz, deren Ausfall die Versorgung mit Lebensmitteln erheblich negativ beeinflussen würde. Ganz ähnlich sieht es bei den Verarbeitern in der Lebensmittelindustrie aus. Ohne SCADA-Systeme zur Steuerung der Prozesse kann die industrielle Verarbeitung nicht aufrechterhalten werden. Im Gegensatz dazu ist die IKT-Abhängigkeit bei den landwirtschaftlichen Produktionsprozessen heute noch geringer. Eine Übersicht über die kritischen Prozesse, respektive Systeme findet sich in der untenstehenden Abbildung.

Abbildung 3: Kritische Prozesse der Lebensmittelversorgung

Kassensysteme (Erfassen)

Unter einem Kassensystem versteht man eine IKT-Lösung für eine elektronische Registrierkasse. Diese Kassensysteme werden auch genutzt, um die Gewohnheiten und Vorlieben einzelner Kunden zu erfassen, zum Beispiel mit Kundenkarten oder Bonusprogrammen. Die meisten verwendeten Kassensysteme tauschen Daten mit Warenwirtschafts- oder ERP-Systemen aus.

Warenbewirtschaftung

In einem Warenwirtschaftssystem wird die mengen- und wertmässige Steuerung der Warenflüsse abgebildet. Damit unterstützt es sämtliche Handelsprozesse eines Unternehmens, von der Beschaffung, über die Lagerwirtschaft, bis zum Verkauf.

Lagerbewirtschaftung

Unter der Lagerbewirtschaftung verstehen wir hier die IKT-gestützte Optimierung der Lagerhaltung.

Tourenplanung

Die Tourenplanung wird durch ein Tourenplanungssystem zur Einsatzplanung und Optimierung der Ressourcen unterstützt. Die Optimierung geschieht, indem der Transportbedarf einer Anzahl Kunden zu einer oder mehreren Touren zusammengefasst wird, sodass zeitliche Vorgaben der Kunden, Lasten und Kapazitäten der Fahrzeuge, Pausen- und Arbeitszeiten der Fahrer und Wartungszyklen der Fahrzeuge eingehalten und gleichzeitig die Transportkosten minimiert werden.

Finanztransaktion (Bezahlung)

Finanztransaktionssysteme sind Systeme für den bargeldlosen Zahlungsverkehr sowie die Verbuchung der Transaktionen und das Ausführen von Zahlungsaufträgen. Die Bedeutung des Angebots bargeldloser Zahlungsverfahren hat in den vergangenen Jahren weiter zugenommen.

Kommunikation

Hierunter wird jegliche für die Kommunikation verwendete IKT verstanden. Dazu gehören insbesondere die Sprachkommunikation über Voice over IP (VoIP), EDI (Electronic Data Interchange nach dem weltweiten GS1 Standard), der E-Mail-Verkehr und die mobile Kommunikation. Die Kommunikationssysteme sind essentieller Teil der Lebensmittelversorgung.

Produktionssteuerung (SCADA)

SCADA-Systeme werden für die Überwachung und Steuerung technischer Systeme (Geräte, Apparate, Maschinen, Anlagen und biologische Systeme) verwendet.[8] Die Produktionssteuerungssysteme (SCADA) steuern die Produktionsanlangen zur Herstellung von Lebensmitteln (z. B. in Ölmühlen, Zuckerraffinerien, Schlachthöfen, Getreidemühlen, Bäckereien, der Verarbeitung von Milch, der Abfüllung von Mineralwasser usw.).

Kommissionierung (SCADA)

Kommissioniert wird entweder vollautomatisch durch Pick by Voice-Systeme oder durch Scanning Systeme. Jegliche Art des Kommissionierens ist IKT-gestützt. Eine Kommissionierung mit ausgedruckten Streichlisten ist nur theoretisch denkbar, denn durch den enormen Zusatzaufwand ist dieser Ansatz ungeeignet. Die Kommissionierungssysteme werden von den meisten Verarbeitern und allen Detailhändlern verwendet und sind essentieller Teil der Lebensmittellogistik (z. B. in Verteilzentren).

Enterprise Ressource Planning

Ein ERP-System ist eine komplexe Anwendung oder eine Vielzahl miteinander kommunizierender IKT-Systeme, die zur Unterstützung der Ressourcenplanung des gesamten Unternehmens eingesetzt werden. Komplexe ERP-Systeme werden häufig in Teil-Systeme (Anwendungs-Module) aufgeteilt, die je nach Unternehmensbedarf miteinander kombiniert werden können.

Verzollung

Unter den Systemen zur Verzollung sind insbesondere das AEV14online, eDec und eVersteigerung zu verstehen. Diese Zollsysteme sind notwendig, um die Verzollung zeitgerecht und effizient abzuwickeln.

Bei vielen Produkten und Produktgruppen wie Fleisch, Wurstwaren, Eiern, Brotgetreide, Früchten, Gemüse, Kartoffeln und Milchprodukten gibt es Zollkontingente. Zur Ersteigerung dieser Kontingente wird die Anwendung eVersteigerung eingesetzt. Nicht vollständig ausgenützte Kontingente können bis zum Verfalldatum via AEV14online an einen Dritten übertragen werden. Bei der Ankunft der Ware am Zoll wird diese mit den Daten der Versteigerung verglichen und entsprechend verzollt. Dies erleichtert die Zollabwicklungen und erlaubt eine zeitsparende Administration.

[8] *Supervisory Control and Data Acquisition*

Defense in Depth

3 Elemente einer Defense in Depth-Strategie

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 einen Feind schwieriger ist, ein komplexes und mehrschichtiges Abwehrsystem zu überwinden als eine einzige Barriere. Gleichzeitig werden die Methoden und Vorgehensweisen der potenziellen Angreifer beobachtet, um darauf basierend entsprechende Abwehrdispositive vorzubereiten. Im IKT-Sicherheitsumfeld zielt 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 potenzieller Angreifer stellt erst dann eine Bedrohung für ein IKT-System dar, wenn es ihm gelingt, eine existierende Schwachstelle in einem dieser Elemente auszunutzen. Organisationen und Unternehmen sind gehalten, die Massnahmen laufend zu überwachen und wo nötig an neue Bedrohungen anzupassen.

3.2 Industrielle Kontrollsysteme (Industrial Control Systems, ICS)

Aufgrund der komplexen Architektur von ICS, resp. SCADA-Systemen[9] 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.

Grundsätzlich gilt, dass bezüglich der Implementierung von Defense in Depth-Konzepten wichtige Unterschiede zwischen der Büroautomation und einem SCADA bestehen. Tabelle 2 zeigt sicherheitsrelevante Themenfelder und ihre unterschiedliche Bedeutung für IKT und ICS.

[9] *In diesem Dokument werden die Begriffe ICS und SCADA synonym verwendet.*

Sicherheitsthema	IKT (z. B. Büroinformatik)	ICS/SCADA (z. B. Produktionssteuerung)
Antivirus	Weit verbreitet. Einfach zu verteilen und zu aktualisieren. Anwender haben die Möglichkeit zur Personalisierung. Antiviren-Schutz kann auf Geräte oder Unternehmensebene konfiguriert werden.	Der Speicherbedarf und die Verzögerung des Datenaustauschs durch den Scanvorgang der Antiviren-Software kann ein ICS-System negativ beeinflussen. Organisationen können ihre älteren ICS-Elemente meist nur mit Produkten aus dem Sekundärmarkt schützen. Antivirenlösungen verlangen zudem im ICS-Umfeld oft nach «Ausnahme»-Ordnern, um zu verhindern, dass geschäftskritische Dateien unter Quarantäne gestellt werden.
Sicherheits-aktualisierungen (Update Management)	Klar definiert, unternehmensweit ausgeführt, automatisiert über Fernzugriff.	Lange Vorlauf- und Planungszeit bis zur erfolgreichen Patch-Installation; immer Hersteller-spezifisch; kann das ICS (temporär) zum Erliegen bringen. Notwendigkeit, das diesbezüglich akzeptable Risiko zu definieren.
Technologielebens-zyklus (Technology Support Life Cycle)	2–3 Jahre, mehrere Anbieter, laufende Weiterentwicklung und Upgrades.	10–20 Jahre, typischerweise derselbe Lieferant/ Dienstleister über den gesamten Lebenszyklus; Ende des Lebenszyklus verursacht neue Sicherheitsgefährdungen.
Methoden zum Testen und 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.
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.

Tabelle 2: Unterschiede zwischen IKT und ICS

Sicherheitsthema	IKT (z. B. Büroinformatik)	ICS/SCADA (z. B. Produktionssteuerung)
Physische Sicherheit (Physical Security)	Variiert zwischen schwach (Büro-IT) bis stark (gehärtete Rechenzentren).	Typischerweise sehr gute physische Sicherheit.
Sichere Systement-wicklung (Secure Software Development)	Integraler Teil des Entwicklungsprozesses	ICS wurden historisch meist als physisch isolierte Systeme konzipiert. Sicherheit als integraler Teil der Systementwicklung war entsprechend wenig verbreitet. Anbieter von ICS haben diesbezüglich Fortschritte gemacht, jedoch langsamer als in der IKT-Welt. Kernelemente von ICS lassen oft keine nachträglichen Sicherheitslösungen zu, bzw. diese sind nicht verfügbar.
Sicherheitsvorgaben	Allgemeine regulatorische Vorgaben, abhängig vom Sektor (nicht alle Sektoren)	Spezifische regulatorische Richtlinien, abhängig vom Sektor (nicht alle Sektoren)

Tabelle 2: Unterschiede zwischen IKT und 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 zu ermöglichen, sowohl im IKT- als auch im ICS-Umfeld
- Notwendigkeit, der eigenen Zulieferkette (engl. Supply Chain) vertrauen zu müssen
- Zeitgemässe Möglichkeiten, ICS-spezifische Protokolle zu überwachen und zu schützen
- Die Möglichkeit, das Fachwissen über sich neu entwickelnde Bedrohungen gegenüber ICS stets aktuell zu halten

Der Defense in Depth-Ansatz erschwert direkte Angriffe auf IKT-Systeme und erhöht die Wahrscheinlichkeit, auffälliges oder unübliches Verhalten innerhalb des Systems frühzeitig zu entdecken. Dieser Ansatz ermöglicht auch die Schaffung von gesonderten Zonen für die Implementierung von Technologien, die ein Eindringen ins System erkennen können (Intrusion Detection Technology). Typische Elemente einer Defense in Depth-Strategie finden sich in Tabelle 3.

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
Netzwerkperimeter-Security	• Firewalls • Fernzugriff & Authentifizierung • Jump Servers/Hosts
Host Security	• Patch- & Schwachstellen-Management • Endgeräte • Virtuelle Geräte
Security Überwachung	• Intrusion Detection Systems • 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 3: Elemente einer Defense in Depth-Strategie

3.3 Risikomanagement

3.3.1 Risikomanagementprogramm

Voraussetzung zur Implementierung einer Defense in Depth-Strategie ist das Verständnis der Geschäftsrisiken einer Organisation, welche im Zusammenhang mit IKT-Bedrohungen stehen. Diese Risiken müssen in Abstimmung mit dem unternehmensweiten Risikoappetit bewirtschaftet werden. Die Verantwortlichen für Betrieb und Unterhalt von IKT-Systemen müssen 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 Grundsätze 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 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. Führen Sie diese Analysen nach strengen Vorgaben durch und verwenden Sie dabei einen strukturierten, systematischen Ansatz.

3.3.2 Risikomanagementframework

IKT-Risikoanalysen sollen in ein Risikomanagementframework eingebettet sein und regelmässig 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).

3.3.3 Risikoanalyse

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

3.4 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.

3.5 Massnahmen

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

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

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

3.6 Cybersecurity-Architektur

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

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

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

3.7 Physische Sicherheit

Physische Sicherheitsmassnahmen reduzieren das Risiko von versehentlichen oder vorsätzlichen Verlusten oder Schäden an IKT-Betriebsmitteln der Organisation oder deren Umfeld. Zu den zu schützenden Betriebsmitteln gehören unter anderem physische Vermögenswerte wie Werkzeuge und Anlagen, die Umwelt, das erweiterte Umfeld sowie das geistige Eigentum, einschliesslich proprietärer Daten wie Prozesseinstellungen und Kundeninformationen. Physische Sicherheitskontrollen müssen häufig spezifische Umwelt-, Sicherheits-, Regulierungs-, Rechts- und sonstige Anforderungen erfüllen. Organisationen sollen physische Sicherheitskontrollen wie technische Kontrollen dem Schutzbedarf anpassen. Um einen umfassenden Schutz zu gewährleisten, 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 Sie die Sicherheitseinstellungen konfigurieren, den Zugang beschränken, Sicherheitssoftware installieren und die Geräte zentral verwalten.

3.8 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.

3.9 Mobile Device Konfiguration

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

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

3.10 Industrielle Kontrollsysteme

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.

3.11 ICS-Netzwerk-Architektur

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 mindestens zwei Sicherheitszonen unterteilt wird. Die erste Sicherheitszone (Sicherheitszone der Organisation) beinhaltet IT-Systeme für die Planung und Ressourceneinteilung (z. B. ERP, Warenwirtschaftssystem). Die zweite Sicherheitszone (Sicherheitszone für die Produktion) beinhaltet Steuerungssysteme (SCADA-Systeme), die die Produktion von Lebensmitteln oder den Verkauf steuern.

Abbildung 4 ist eine schematische Darstellung der üblichen Kommunikationswege und Sicherheitszonen des Teilsektors Lebensmittelversorgung. Sie zeigt auf, wie die Trennung zwischen IT (Information Technology) und OT (Operational Technology) sowie die üblichen Kommunikationswege aussehen können.[10]

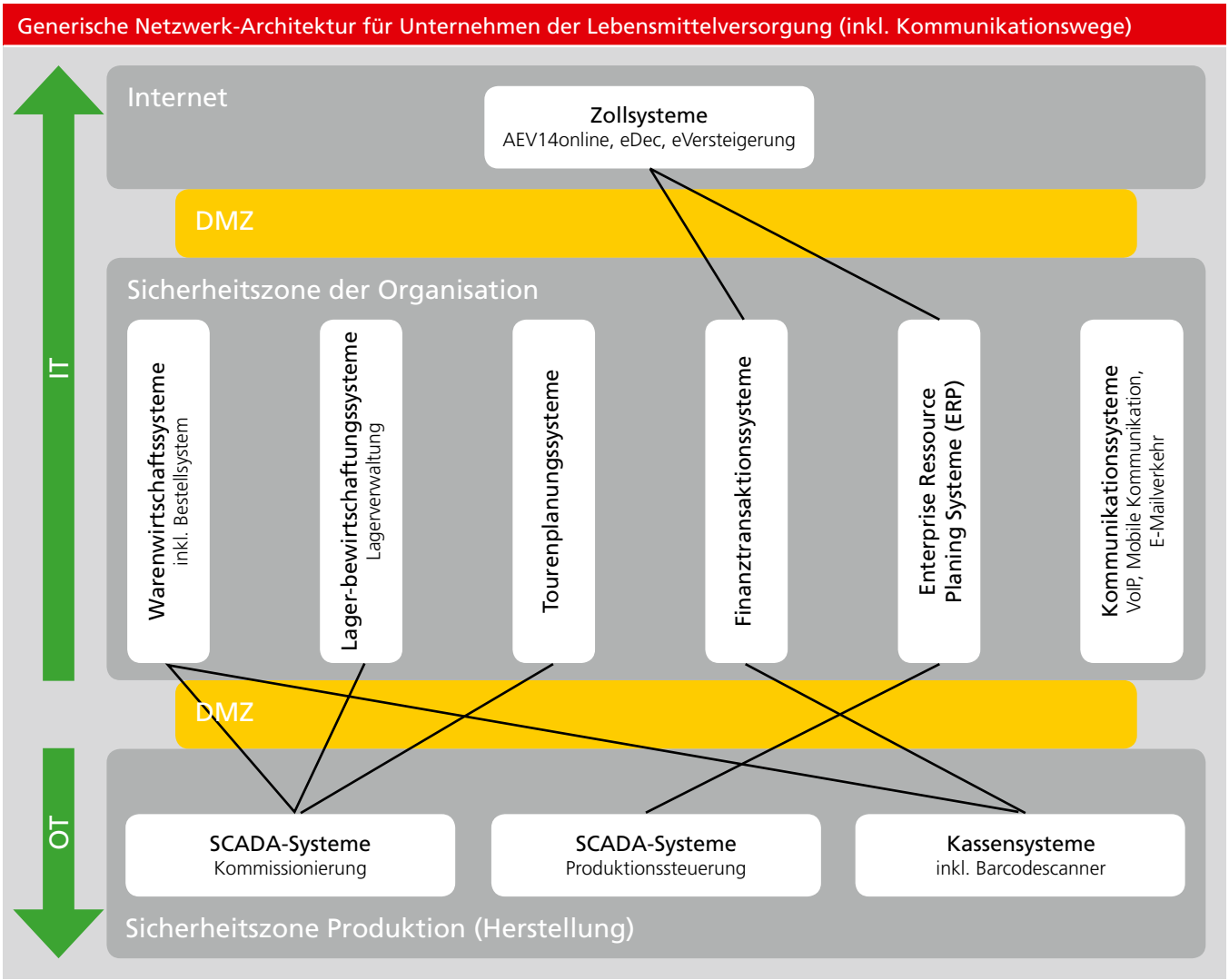

Abbildung 4: Generische Netzwerk-Architektur für Unternehmen der Lebensmittelversorgung (inkl. Kommunikationswege)

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

3.12 ICS/SCADA-Netzwerk-Perimeter-Security

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

3.13 Host Security

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

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

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

- Installation und Konfiguration einer host-basierten Firewall
- Bildschirmschoner mit kurzen Intervallen und Aufforderung zur Passworteingabe sollen 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, auch solche, welche nicht mehr benutzt werden
- Nicht sichere Services, wie Telnet, Remote Shell oder FTP, müssen durch sichere Alternativen wie sTelnet, SSH, sFTP usw. ersetzt werden
- Benutzer sollten nicht in der Lage sein, Services zu deaktivieren
- Backups von Systemen müssen gemacht und geprüft werden, besonders, wenn diese nicht zentral gesteuert werden
- Vom Betriebssystem bereitgestellte Sicherheitsmodule wie z. B. Sicherheitsscanner sollten aktiviert oder durch eine adäquate Software ersetzt werden
- Für Laptops und andere mobile Geräte, welche nicht durchgehend mit dem Firmennetz verbunden sind, gelten die gleichen Richtlinien. Bei mobilen Geräten soll die Harddisk zusätzlich verschlüsselt werden

3.14 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.

3.15 Informationssicherheitsstrategie

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.

3.16 Lieferantenmanagement

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

3.17 Das Element 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 ist. Auch die Bekämpfung von Aktivitäten mit bösartigen Absichten von Insidern stellt eine weitere Herausforderung dar. Im Umgang mit diesen Herausforderungen, sind Unternehmen gehalten, sich mit den nachfolgenden Themen zu befassen.

3.17.1 Beschäftigungszyklus von Mitarbeitenden

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

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

3.17.2 Weisungen/Richtlinien

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

3.17.3 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 Sicherheitsniveau geschult und es kann sichergestellt werden, dass alle erforderlichen Vorschriften und Standards bekannt sind. Der Prozess zur Erkennung eines Cyber-Vorfalles (Intrusion Detection) ist von besonderer Bedeutung. Im Umgang mit herstellerspezifischen Protokollen und Legacy-Systemen sind netzwerkbasierte Sicherheitsverfahren besonders wichtig.

3.17.4 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.

3.17.5 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. Jeder Einzelne soll in seinem persönlichen Zuständigkeitsbereich befähigt sein, risikobasierte Entscheidungen zu treffen.

Assessment Framework

4 NIST Framework

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

Überblick

Das NIST 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)*

Implementation Tiers

Das NIST Framework Core kennt vier Implementation Tiers (dt. «Stufen»). Diese beschreiben die Ausbaustufe (Schutzniveau), welche ein Unternehmen umgesetzt hat. Sie reichen von teilweise (Tier 1) bis dynamisch (Tier 4). Zur Festlegung des eigenen Schutzniveaus (Tier 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.

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 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 IKT-Minimalstandard mitgelieferte Assessment Tool verwendet werden. Die Resultate aus der Beantwortung der 106 Aufgaben werden entsprechend den 5 Funktionen des 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

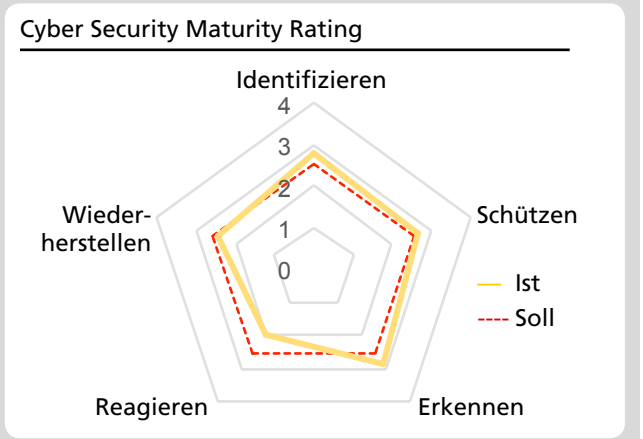

Abbildung 5: Beispiel Overall Cybersecurity Maturity Rating

4.1 Identifizieren (Identify)

Inventar Management (Assest Management)

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

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

Tabelle 4: Aufgaben ID.AM

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

Tabelle 5: Referenzen ID.AM

Geschäftsumfeld (Business Environment)

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

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

Tabelle 6: Aufgaben ID.BE

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

Tabelle 7: Referenzen ID.BE

Vorgaben (Governance)

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

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

Tabelle 8: Aufgaben ID.GV

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

Tabelle 9: Referenzen ID.GV

Risikomanagement (Risk Assessment)

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

Bezeichnung	Aufgabe
ID.RA-1	Identifizieren Sie die (technischen) Verwundbarkeiten Ihrer Betriebsmittel und dokumentieren Sie diese.
ID.RA-2	Tauschen Sie sich regelmässig in Foren und Gremien aus, um aktuelle Informationen über Cyber-Bedrohungen zu erhalten.
ID.RA-3	Identifizieren und dokumentieren Sie interne und externe Cyber-Bedrohungen.
ID.RA-4	Identifizieren Sie mögliche Auswirkungen 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 10: Aufgaben ID.RA

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

Tabelle 11: Referenzen ID.RA

Risikomanagement Strategie (Risk Management Strategy)

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

Bezeichnung	Aufgabe
ID.RM-1	Etablieren Sie Risikomanagementprozesse, bewirtschaften Sie diese aktiv und lassen Sie sich 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 12: Aufgaben ID.RM

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

Tabelle 13: Referenzen ID.RM

Lieferketten Risikomanagement (Supply Chain Riskmanagement)

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

Bezeichnung	Aufgabe
ID.SC-1	Etablieren Sie klare Prozesse zum Management der 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 14: Aufgaben ID.SC

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

Tabelle 15: Referenzen ID.SC

4.2 Schützen (Protect)

Zugriffsmanagement und -steuerung (Access Control)

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

Bezeichnung	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 Berechtigungsstufen und Zugangsdaten zugeordnet sind.

Tabelle 16: Aufgaben PR.AC

Standard	Referenz
COBIT 5	DSS05.04, DSS06.03, DSS01.04, DSS05.05, APO13.01, DSS01.04, DSS05.03, DSS05.04, DSS05.05, DSS05.07, DSS06.03, BAI08.03
ISA 62443-3:2013	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.13, SR 2.1, SR 2.6, SR 3.1, SR 3.8, SR 2.2, SR 2.3
ISO 27001:2013	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3, A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.6.1.2, A.7.1.1, A.9.1.2, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6, A.9.4.1, A.9.4.4
NIST-SP-800-53 Rev. 4	AC-2, IA Family, PE-2, PE-3, PE-4, PE-5, PE-6, PE-9, AC-17, AC-19, AC-20, AC-2, AC-3, AC-5, AC-6, AC-16, AC-24, IA-2, IA-4, IA-5, IA-8

Tabelle 17: Referenzen PR.AC

Sensibilisierung und Ausbildung (Awareness and Training)

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 18: Aufgaben PR.AT

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

Tabelle 19: Referenzen PR.AT

Datensicherheit (Data Security)

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

Bezeichnung	Aufgabe
PR.DS-1	Stellen Sie sicher, dass gespeicherte Daten geschützt sind (vor Verletzungen der Vertraulichkeit, Integrität und Verfügbarkeit).
PR.DS-2	Stellen Sie sicher, dass Daten während der Übertragung (vor Verletzungen der Vertraulichkeit, Integrität und Verfügbarkeit) geschützt sind.
PR.DS-3	Stellen Sie sicher, dass für Ihre 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 20: Aufgaben PR.DS

Standard	Referenz
COBIT 5	APO01.06, BAI02.01, BAI06.01, DSS06.06, BAI09.03, APO13.01, BAI07.04, BAI03.05.4
ISA 62443-3:2013	SR 3.4, SR 4.1, SR 3.1, SR 3.8, SR 4.1, SR 4.2, SR 7.1, SR 7.2, SR 5.2
ISO 27001:2013	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7, A.12.3.1, A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3
NIST-SP-800-53 Rev. 4	SC-28, SC-8, CM-8, MP-6, PE-16, AU-4, CP-2, SC-5, AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4, SI-7, CM-2, SA-10

Tabelle 21: Referenzen PR.DS

Informationsschutzrichtlinien (Information Protection Processes and Procedures)

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 22: Aufgaben PR.IP

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

Tabelle 23: Referenzen PR.IP

Unterhalt (Maintenance)

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 24: Aufgaben PR.MA

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

Tabelle 25: Referenzen PR.MA

Einsatz von Schutztechnologie (Protective Technology)

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 26: Aufgaben PR.PT

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

Tabelle 27: Referenzen PR.PT

4.3 Erkennen (Detect)

Auffälligkeiten und Vorfälle (Anomalies and Events)

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 28: Aufgaben DE.AE

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

Tabelle 29: Referenzen DE.AE

Überwachung (Security Continous Monitoring)

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

Bezeichnung	Aufgabe
DE.CM-1	Etablieren Sie ein kontinuierliches Netzwerkmonitoring, um potentielle Cybersecurity-Vorfälle zu entdecken.
DE.CM-2	Etablieren Sie ein kontinuierliches Monitoring/Überwachung aller physischen Betriebsmittel und Gebäude, um Cybersecurity-Vorfälle entdecken zu können.
DE.CM-3	Etablieren Sie ein Monitoring der 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 30: Aufgaben DE.CM

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

Tabelle 31: Referenzen DE.CM

Detektionsprozess (Detection Processes)

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

Bezeichnung	Aufgabe
DE.DP-1	Definieren Sie klare Rollen und Verantwortlichkeiten, so dass klar ist, wer wofür zuständig ist und wer welche Kompetenzen hat.
DE.DP-2	Stellen Sie sicher, dass die Detektionsprozesse 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 32: Aufgaben DE.DP

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

Tabelle 33: Referenzen DE.DP

4.4 Reagieren (Respond)

Reaktionsplanung (Response Planning)

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

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

Tabelle 34: Aufgaben RS.RP

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

Tabelle 35: Referenzen RS.RP

Kommunikation (Communications)

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

Bezeichnung	Aufgabe
RS.CO-1	Stellen Sie sicher, dass alle Personen ihre Aufgaben bezüglich der Reaktion und der Reihenfolge ihrer Handlungen auf eingetretene Cybersecurity-Vorfälle kennen.
RS.CO-2	Definieren Sie Kriterien für 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 36: Aufgaben RS.CO

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

Tabelle 37: Referenzen RS.CO

Analyse (Analysis)

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

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

Tabelle 38: Aufgaben RS.AN

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

Tabelle 39: Referenzen RS.AN

Schadensminderung (Mitigation)

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

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

Tabelle 40: Aufgaben RS.MI

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

Tabelle 41: Referenzen RS.MI

Verbesserungen (Improvements)

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

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

Tabelle 42: Aufgaben RS.IM

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

Tabelle 43: Referenzen RS.IM

4.5 Wiederherstellen (Recover)

Wiederherstellungsplanung (Recovery Planning)

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

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

Tabelle 44: Aufgaben RC.RP

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

Tabelle 45: Referenzen RC.RP

Verbesserungen (Improvements)

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

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

Tabelle 46: Aufgaben RC.IM

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

Tabelle 47: Referenzen RC.IM

Kommunikation (Communications)

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 48: Aufgaben RC.CO

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

Tabelle 49: 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. Dieser IKT-Minimalstandard bietet mit dem NIST Framework Core ein Werkzeug, mit welchem die Akteure der Lebensmittelversorgung 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, Verbänden und Bund werden sich die Chancen weiterer Anwendungsmöglichkeiten zeigen.

Neben dem hier vorliegenden IKT-Minimalstandard stellt die Wirtschaftliche Landesversorgung den Unternehmen der Lebensmittelbranche den Standard auch als Excel-basiertes Assessment Tool zur Verfügung.[11] Zur Einschätzung des Maturitätsniveaus des Unternehmens oder der Organisation ist insbesondere das Assessment Tool hilfreich. Der hier vorliegende Teil (IKT-Minimalstandard) ist als Begleitdokument zu verstehen, welches an das Thema heranführt und bei Fragen herangezogen werden kann.

Dieser Standard ist keine Vorgabe, sondern soll die Akteure der Lebensmittelversorgung zur eigenen Reflektion hinsichtlich Cybersecurity anregen. IKT-Sicherheit ist kein Zustand, sondern ein Prozess. Der IKT-Minimalstandard soll diesen Prozess anstossen und bei der Umsetzung helfen.

[11] *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. Grössere Organisationen mit entsprechenden Ressourcen und ausgebildeten Mitarbeitern (z. B. im Detailhandel) werden keine Schwierigkeiten haben, diese Empfehlung umzusetzen. Möglicherweise werden grössere Unternehmen bereits das in diesem Dokument vorgeschlagene Framework oder ein anderes umgesetzt haben. Die Lebensmittelversorgung besteht jedoch aus einer äusserst heterogenen Menge von Akteuren. Einige durchaus kritische Infrastrukturen sind in ihrer Grösse (Anzahl Mitarbeiter und Ressource für die Informationssicherheit) eher mit einem Klein-Unternehmen vergleichbar. Eine umfassende Umsetzung des Frameworks kann solche Unternehmen vor eine grosse Herausforderung stellen. Um dem gerecht zu werden und ein möglichst skalierbares Vorgehen zu ermöglichen wird empfohlen, dass Klein-Unternehmen mindestens die folgenden 21 Schritte (Kapitel 6.1.1) umsetzen:

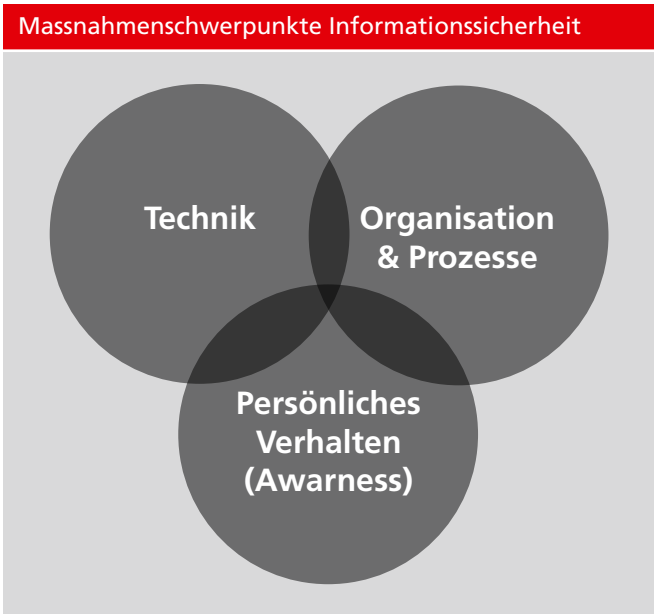

Abbildung 6: Massnahmenschwerpunkte Informationssicherheit

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.

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.

6.1.1 21 Schritte zu besserer Informationssicherheit

Risikobasiertes Vorgehen

Das Risikobasierte Vorgehen erlaubt jedem Unternehmen (egal ob Grossunternehmen oder KMU) das Risiko selbständig zu erheben und die eigene Risikobereitschaft festzulegen. Je nach Grösse des Unternehmens können bei der Risikobereitschaft deutliche Unterschiede bestehen. Während beispielsweise bei einem Grossunternehmen der Ausfall des Warenwirtschaftssystems sowohl einen enormen finanziellen Verlust als auch einen Reputationsschaden verursachen könnte, würde ein gleicher Ausfall bei einem kleineren Verarbeiter geringe oder keine Auswirkungen aufweisen (da Bestellungen und Warenfluss des täglichen Geschäfts bekannt sind oder einfache Resilienzmassnahmen bestehen). Dieses Risikobasierte Vorgehen ermöglicht es Unternehmen jeder Grösse ein Vorgehen zur Verbesserung der Informationssicherheit zu wählen, welches im Rahmen ihrer Möglichkeiten bleibt (Mitarbeiter, Wissen, Finanzen etc.).

Hilfestellung Empfehlungen

Die folgende Hilfestellung ist insbesondere (aber nicht nur) an kleinere und mittelgrosse Unternehmen gerichtet, bei denen ein ganzheitliches Umsetzen des NIST Framework Core (siehe Kapitel 6) nicht möglich ist. Es ersetzt jedoch nicht die Risikoeinschätzung sowie die Definition der eigenen Risikobereitschaft entsprechend dem Framework. Es wird empfohlen, die dort identifizierten Risiken entsprechend den NIST-Controls (siehe Kapitel 6) zu verringern. Die folgenden Empfehlungen gelten als Hilfestellungen und dürfen nicht als Ersatz für das NIST Framework Core verstanden werden.

Die folgende Hilfestellung basiert auf dem erweiterten 10-Punkte Programm des Vereins Infosurance:[12]

Massnahmen für einen wirkungsvollen Grundschutz			
1.	**Sichern Sie Ihre Daten regelmässig mit Backups**		
	Datenverluste entstehen auf verschiedene Arten: Daten werden versehentlich überschrieben, Informationen auf einer Harddisk werden durch einen Defekt unlesbar oder ein Brand beziehungsweise ein Wasserschaden zerstört Ihre Daten. Solche Verluste können Sie mit regelmässigen Datensicherungen (Backups) vermeiden. • Grundsätzlich sind alle Daten mit geschäftsrelevantem Inhalt zu sichern. Softwarekonfigurationen sollten ebenfalls gesichert werden. • Die Häufigkeit der Datensicherung richtet sich nach Tätigkeit und Grösse Ihres Unternehmens. Mindestens einmal pro Woche sollte jedes KMU seine Daten sichern. • Regeln Sie schriftlich, wer für Datensicherungen zuständig ist und führen Sie eine Kontrollliste über die erfolgreiche Sicherung der Daten. • Sichern Sie die Daten immer auf mobilen Medien (Bandlaufwerk, auswechselbarer Datenträger). • Es lohnt sich, von wichtigen Daten, die nur in Papierform vorliegen (z. B. von Verträgen, Urkunden), Kopien anzufertigen und diese ebenfalls ausser Haus aufzubewahren. • Beachten Sie, dass die Bilanz, die Erfolgsrechnung, die Geschäftsbücher, die Inventare, die Buchungsbelege und die buchungswirksame Geschäftskorrespondenz während 10 Jahren aufbewahrt werden müssen. • Überprüfen Sie periodisch, ob sich die Daten von den Sicherungsmedien zurückspielen lassen. Jede Sicherung ist nutzlos, wenn die Daten nicht korrekt auf das Backup-Medium übertragen wurden.		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
2.	**Halten Sie Ihr Antivirus-Programm aktuell**		
	Schädliche Programme, wie zum Beispiel Viren und Würmer, können Ihre IT-Infrastruktur lahmlegen und damit die wirtschaftliche Existenz Ihres Unternehmens gefährden. • Computerviren können Daten und Programme verändern, manipulieren oder sogar vollständig zerstören. Bösartige Computerprogramme werden via E-Mail-Anhänge (Attachments) und Instant Messengers usw. übertragen. Im Internet sind Viren oft als nützliche oder unterhaltende Gratisprogramme getarnt und werden durch einen einfachen Mausklick aktiviert. • Unzureichend geschützte Computersysteme werden häufig zur Verbreitung von Viren und für gezielte Attacken gegen ein drittes Unternehmen missbraucht. Wer als Geschäftsleiterin oder Geschäftsleiter ungenügende Vorkehrungen zum Schutz seiner Computersysteme trifft, handelt fahrlässig und muss allenfalls mit Strafverfolgung rechnen. • Schutz vor bekannten Viren und Würmern bietet ein Antivirus-Programm. Es identifiziert Eindringlinge und macht sie unschädlich. • Installieren Sie ein Antivirus-Programm auf sämtlichen Servern, Arbeitsstationen sowie auf Ihren Notebooks. • Da Hacker laufend neue Viren programmieren, muss das Antivirus-Programm immer wieder aktualisiert werden. Die Aktualisierung sollte auf jeden Fall täglich durchgeführt werden. • Fordern Sie die Mitarbeitenden auf, Warnmeldungen über Viren unverzüglich dem IT-Verantwortlichen zu melden.		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:

[12] *Download unter: http://www.kmu.admin.ch/dam/kmu/de/dokumente/savoir-pratique/Informatique-et-IT/InfoSurance_10_Points_Programme_FR.pdf.download.pdf/InfoSurance_10_Points_Programme_FR.pdf*

Massnahmen für einen wirkungsvollen Grundschutz			
3.	**Schützen Sie Ihren Internetzugang**		
	Gibt es in Ihrem Betrieb Firewalls? Ja? Dann achten Sie bestimmt darauf, dass die Ports auch stets geschlossen werden. In der Welt des Internets und des elektronischen Datenaustauschs erfüllt die Firewall diese Sicherheitsaufgabe. • Ohne eine Firewall können Unbefugte auf Ihren Computersystemen Schaden anrichten. Sie können darauf unbemerkt Befehle ausführen oder Ihre Rechner zu illegalen Attacken auf Dritte missbrauchen. Zudem gelangen sie an Geschäftsdaten, die eventuell dem Datenschutzgesetz unterstehen. • Im Handel sind Produkte erhältlich, die gleichzeitig eine Firewall und einen Virenschutz bieten. Gerade für kleinere Betriebe sind kombinierte Produkte sehr zu empfehlen. • Manche Betriebssysteme haben eine eigene Firewall eingebaut. Nutzen Sie auf jeden Fall auch diese Möglichkeit und aktivieren Sie diese Firewalls. • Wenn Sie in Ihrem Betrieb Wireless-LAN für Ihre Computer einsetzen, sorgen Sie dafür, dass diese richtig und sicher funktionieren. • Sämtliche Netzwerkübergänge müssen mit einer Firewall gesichert werden. • Wickeln Sie den gesamten Internetverkehr über die Firewall ab. Erlauben Sie keine anderen Zugänge zum Internet (z. B. via Modem). • Setzen Sie keine privaten Laptops und Wireless-LAN-Geräte im Unternehmen ohne entsprechenden Schutz und schriftliche Einwilligung des IT-Verantwortlichen ein. • Schützen Sie die Konfiguration Ihrer Firewall mit einem starken Passwort.		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
4.	**Aktualisieren Sie Ihre Software regelmässig**		
	So wie Sie Ihr Auto regelmässig warten, müssen auch Computerprogramme in einem Unternehmen gepflegt und auf den neuesten Stand gebracht werden. • Heutige Software beinhaltet oft Millionen von Zeilen Code. Dabei schleichen sich trotz Kontrollen Fehler ein. Für den Hersteller ist es nahezu unmöglich, Anwendungen in jeder denkbaren Umgebung und möglichen Konfiguration zu testen. Die Hersteller bieten regelmässig sogenannte «Patches», also «Software-Flicken» an. Sie beheben die bekannten Fehler. • Wenn Sie Ihre Software nicht oder nur selten aktualisieren, können Angreifer bekannte Fehler ausnützen, um Daten zu manipulieren oder um Ihre Infrastruktur für bösartige Zwecke zu missbrauchen. • Minimieren Sie Ihre «Angriffsfläche», indem Sie nur Software installieren, die Sie tatsächlich benötigen und unnötige Dienste, Netzwerkfreigaben und Protokolle deaktivieren. • Installieren Sie die neuesten «Patches» für Betriebssysteme und Anwendungsprogramme. • Installieren Sie verfügbare «Sicherheits-Updates» so schnell wie möglich. • Installieren Sie «Patches» auf sämtlichen Computern, d. h. auch auf Notebooks und Geräten von externen Mitarbeitenden.		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:

Massnahmen für einen wirkungsvollen Grundschutz			
5.	**Verwenden Sie starke Passwörter**		
	Wer den Benutzernamen und das Passwort eines Anwenders kennt, kann sich in einem System anmelden und übernimmt damit die (Computer-)Identität des entsprechenden Anwenders mit allen Zugriffsberechtigungen! Durch Passwortdiebstahl können somit Unbefugte ohne grossen Aufwand an vertrauliche Geschäftsformationen gelangen. Verhindern Sie, dass in Ihrem Betrieb der Identitätsdiebstahl möglich ist. • Werkseitige Passworteinstellungen bei Geräten, Betriebssystemen und Anwendungsprogrammen müssen vom IT-Verantwortlichen sofort geändert werden. • Halten Sie Ihre Mitarbeitenden dazu an, nur starke Passwörter einzusetzen, die regelmässig geändert werden. Machen Sie allen bewusst, dass sie für Handlungen verantwortlich sind, die unter ihrem Benutzernamen ausgeführt werden. • Starke Passwörter sind mindestens 8 Zeichen lang, enthalten Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen. • Verwenden Sie keine Passwörter, die Namen, AHV- und Passnummern und Geburtsdatum aus dem Familienumfeld enthalten. • Verwenden Sie ebenfalls auch keine Passwörter, die in Wörterbüchern (alle Sprachen) zu finden sind. • Schreiben Sie Passwörter niemals auf, ohne die Notiz sicher z. B. im Tresor zu verwalten. • Geben Sie Ihr Passwort niemals an Dritte weiter.		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
6.	**Schützen Sie Ihre mobilen Geräte**		
	Mobiltelefone und Notebooks mit Wireless-LAN sind ausgesprochen praktisch und vielseitig. Falsch eingesetzt, stellen diese Geräte aber ein Sicherheitsrisiko dar. Wer aus geschäftlichen Gründen gezwungen ist, sensible Daten auf mobilen Geräten zu speichern, muss spezielle Vorkehrungen treffen. • Sämtliche mobilen Geräte müssen mit einem starken Passwort geschützt werden (siehe Punkt 5) und die Daten müssen verschlüsselt gespeichert werden. Beim Verlust des Geräts oder im Fall eines Diebstahls haben Unbefugte sonst ein leichtes Spiel, an Ihre Geschäftsdaten zu gelangen. • Auf mobilen Geräten sollten nur diejenigen Daten gespeichert sein, die tatsächlich benötigt werden. • Auch mobile Geräte müssen regelmässig auf Viren geprüft werden, weil sie z. B. via E-Mail-Funktionen mit Ihren übrigen Computern synchronisiert werden. • Durch falsch konfigurierte Wireless-LAN-Geräte können Hacker innerhalb weniger Minuten aus Distanzen von über einem Kilometer in Ihr Firmennetzwerk eindringen! Die Nutzung von externen und öffentlichen Access Points (HotSpots) muss speziell geregelt werden. • Aktivieren Sie Bluetooth bei Ihren Geräten (Handy, Notebooks) nur bei Bedarf und nicht erkennbar. Ihr Gerät reagiert sonst ohne Ihr Wissen auf Anfragen fremder Geräte (im Umkreis von bis zu 100 Metern). • Aktivieren Sie die Verschlüsselung der kabellosen Datenübermittlung (WPA2). • Übermitteln Sie vertrauliche Daten nur über Verbindungen, welche zusätzlich mit einem Virtual Privat Network (VPN) geschützt sind.		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:

Massnahmen für einen wirkungsvollen Grundschutz			
7.	**Machen Sie Ihre IT-Benutzerrichtlinien bekannt**		
	Ohne verbindliche und verständliche IT-Benutzerrichtlinien können Ihre Mitarbeitenden nicht wissen, welche Handlungen erlaubt und welche verboten sind. Regeln werden nur ernst genommen, wenn sich auch Vorgesetzte daranhalten. Handeln Sie in allen Sicherheitsaspekten als Vorbild. • Definieren Sie als Bestandteil zu den Anstellungsbedingungen schriftliche IT-Benutzerrichtlinien und informieren Sie die Mitarbeitenden. • Machen Sie Sicherheit in Ihrem Unternehmen immer wieder und auf unterschiedliche Weise zum Thema. • Führen Sie ein bis zwei Mal pro Jahr Sensibilisierungsaktionen durch. Diese lassen sich auch mit einfachen Mitteln realisieren: z. B. durch E-Mails an alle Mitarbeitenden, Rundschreiben in der internen Post, Plakate in der Kantine, Beiträge in der Firmenzeitung usw. • Organisieren Sie eine Basisausbildung für alle Mitarbeitenden (z. B. auf der Basis dieser Broschüre). Die wichtigsten Lernziele sind: – Nutzen der IT-Sicherheit – Bestimmen starker Passwörter – sicherer Umgang mit Internet, E-Mail und dem Virenschutz – Ablagestruktur von Dokumenten • Regeln Sie – die Installation und den Einsatz von eigenen Programmen und Hardware (Spiele, USB-Memory Sticks, private Notebooks etc.) – den Gebrauch des Internets (was ist erlaubt, was nicht) – den Gebrauch von E-Mail (Vertraulichkeit, Weiterleiten, private E-Mail-Adressen, Kettenbriefe etc.) – den Umgang mit vertraulichen Informationen – das Verhalten bei sicherheitsrelevanten Vorkommnissen • Kündigen Sie Sanktionen bei einem Verstoss gegen die Benutzerrichtlinien an und setzen Sie diese nötigenfalls auch um.		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:

Massnahmen für einen wirkungsvollen Grundschutz			
8.	**Schützen Sie die Umgebung Ihrer IT-Infrastruktur**		
	Wissen Sie, wer in Ihrem Unternehmen tagsüber ein- und ausgeht? Einige wenige Vorkehrrungen verhindern bereits, dass Unbefugte an wichtige Geschäftsinformationen gelangen. Gelebte, sichtbare Sicherheit ist heute ein Qualitätskriterium und schafft Vertrauen bei Kunden und Lieferanten. Was nützt die beste Firewall, wenn sich Fremde in die Büroräume einschleichen können? • Alle Zugänge zum Gebäude resp. Firmenareal sind abzuschliessen oder zu überwachen. Falls dies nicht möglich ist, müssen zumindest die Büroräumlichkeiten geschützt werden. • Lassen Sie Besucher, Kunden und Bekannte nicht unbeaufsichtigt in Ihrem Betrieb umhergehen. • Alle Drittpersonen werden am Empfang abgeholt, während ihres Aufenthaltes dauernd begleitet und beim Verlassen des Gebäudes am Ausgang wieder verabschiedet. • Wenn Sie nicht über einen Empfang verfügen, der den Eingangsbereich überblickt, sollten Sie die Eingangstüre schliessen und ein Schild «Bitte läuten!» anbringen. • Stellen Sie sicher, dass sämtliche Einstiegsmöglichkeiten (Fenster, Türen usw.) über einen ausreichenden Einbruchschutz verfügen. • Schlüssel und Badges müssen korrekt verwaltet und die entsprechenden Listen aktualisiert werden. Schlüssel mit Passepartout-Funktion sind restriktiv zu verteilen. Die entsprechenden Berechtigungen müssen mindestens jährlich auf ihre Notwendigkeit geprüft werden. • Mitarbeitende, welche aus dem Unternehmen austreten, geben ihre Schlüssel, Badges und andere Zugangsberechtigungen beim Austritt ab. • Stellen Sie Server in abschliessbare, klimatisierte Räume. Ist kein entsprechender Raum verfügbar, schliessen Sie die Server in einen Computerschrank (Rack). • Lagern Sie brennbare Materialien wie Papier etc. nicht im oder unmittelbar vor dem Serverraum. • Stellen Sie Netzwerkdrucker nicht in öffentlich zugängliche Räume, da Unbefugte Einblick in Dokumente erhalten können. • Schliessen Sie Netzwerkkabel, die durch öffentliche Räume führen, sowie Modems, Hubs, Router und Switches ein.		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:

Massnahmen für mehr Vertraulichkeit			
9.	**Regeln Sie den Zugriffschutz auf Daten**		
	Durch unbefugten Zugriff können Informationen missbraucht werden. Schützen Sie deshalb den Datenzugriff entsprechend, sodass nur berechtigte Personen Zugang haben. • Wer unbefugten Zugriff zu Informationen hat, kann diese einsehen, kopieren, verändern oder löschen. • Legen Sie fest, wer Zugriff auf bestimmte IT-Anwendungen oder Informationen hat. Dabei sollten die Zugriffsrechte rollenbasiert vergeben werden, z. B. Sekretariat, Verkauf, Buchhaltung, Personalwesen, Systemadministrator. • Es sind nur so viele Zugriffsrechte zu vergeben, wie sie zur Durchführung einer Aufgabe benötigt werden («Need-to-know-Prinzip»). Die Zugriffsrechte werden von der jeweils verantwortlichen Person festgelegt. • Die Rechteverwaltung muss dokumentiert werden. Festgehalten wird, welche Person welche Funktion wahrnimmt und welche Person Zugriff auf welche Applikationen und Daten hat. Überprüfen Sie diese Rechte regelmässig und passen Sie sie entsprechend an. • Beim Austritt von Mitarbeitenden aus dem Unternehmen oder bei internem Wechsel sind deren Benutzerkonten und die Zugriffsrechte sofort zu sperren bzw. anzupassen. • Besonders zu beachten sind die Systembetreuer und die Administratoren. Sie verfügen in der Regel über sehr weitgehende Rechte.		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
10.	**Verschlüsseln Sie mobile Datenträger und Übermittlung**		
	Vertrauliche Daten können bei ungeschützter Übermittlung (z. B. E-Mail) von Dritten eingesehen werden. Mobile Geräte können verloren gehen und Ihre Daten geraten in falsche Hände. Um die Vertraulichkeit zu gewährleisten, ist eine Verschlüsselung der Daten auf den Geräten sowie der Übermittlung notwendig. • E-Mails können von Dritten gelesen werden. E-Mails mit vertraulichem Inhalt sollten Sie deshalb verschlüsseln. • Mobile Geräte wie Notebooks sind generell zu verschlüsseln. • Übermitteln Sie vertrauliche Daten nur über Verbindungen, welche zusätzlich mit einem Virtual Private Network (VPN) geschützt sind (siehe auch Punkt 6).		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:

Massnahmen für mehr Vertraulichkeit			
11.	**Sensibilisieren Sie ihre Mitarbeitenden**		
	Nur sensibilisierte Mitarbeitende setzen Sicherheitsmassnahmen um. Erläutern Sie Ihren Mitarbeitenden die Notwendigkeit der Massnahmen und den korrekten Umgang mit vertraulichen Daten. Schliessen Sie mit ihren Mitarbeitenden und externen Partnern eine Vertraulichkeitsvereinbarung ab. • Eigene und externe Mitarbeitende bearbeiten oft vertrauliche Daten. Diesen Personen muss bewusst sein, dass sie entsprechende Massnahmen ergreifen müssen, um die Vertraulichkeit zu gewährleisten. • Fügen Sie eine Vertraulichkeitsklausel in den Arbeitsvertrag ein. Dies gilt auch für externe Mitarbeitende oder Partner. Diese Vertraulichkeitsvereinbarung definiert, wie mit vertraulichen Informationen umgegangen werden muss. • Sensibilisieren Sie die neuen Mitarbeitenden bereits bei deren Einstellung für die Belange der IT-Sicherheit. • Kündigen Sie Sanktionen bei einem Verstoss gegen die Richtlinien an und setzen Sie diese nötigenfalls auch um.		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
12.	**Regeln Sie die Entsorgung von Informationen und Informationsträgern**		
	Vertrauliche Informationen können bei unsachgemässer Entsorgung in falsche Hände geraten. Erklären Sie Ihren Mitarbeitenden, wie Informationen und Informationsträger (Papier, elektronische Informationsträger) sicher und umweltgerecht entsorgt werden. • Regeln Sie die Entsorgung: – von Altpapier (Zeitungen, Werbungen und andere öffentliche Dokumente) – alle übrigen internen und vertraulichen Dokumente – Karton – elektronische Datenträger wie USB-Sticks, CDs und externe Festplatten • Legen Sie fest, wie das Archiv entsorgt werden soll. • Kündigen Sie Sanktionen bei einem Verstoss gegen die Richtlinien an und setzen Sie diese nötigenfalls auch um.		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:

Massnahmen für mehr Verfügbarkeit

13. Überprüfen Sie Ihre Systeme

Das reibungslose Funktionieren der IT-Systeme muss jederzeit gewährleistet sein. Deshalb müssen IT-Systeme überprüft und regelmässig gewartet werden. Eine korrekte Wartung vermindert Störungen und verhindert Schäden an der Informationstechnologie.

- Prüfen Sie regelmässig die Funktionstüchtigkeit Ihrer IT-Systeme:
  – Funktioniert das Backup-System?
  – Sind die Backup-Daten tatsächlich lesbar?
  – Funktioniert die unterbrechungsfreie Stromversorgung (USV)?
  – Enthalten die automatischen Systemprotokoll-Dateien Fehlermeldungen?
- Beachten Sie auch organisatorische Aspekte:
  – Werden gesetzliche und andere Richtlinien eingehalten?
  – Ist die Notfallvorsorge überprüft worden?
- Überwachung und Wartungsarbeiten müssen in regelmässigen Abständen durchgeführt werden.
- Erstellen Sie eine Wartungsliste:
  – Was muss wann durch wen geprüft und gewartet werden?
  – Stellen Sie die Kontrolle und die Nachvollziehbarkeit der Wartung sicher.
- Lassen Sie die externen Wartungstechniker eine Vertraulichkeitsvereinbarung unterzeichnen (siehe Punkt 11).

Umsetzungsstand

Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:

14. Schützen Sie den Zugang in Ihr Firmennetz durch eine Zwei-Faktor-Authentifizierung

Ein Zugriff von Extern in das Firmennetz setzt aus Sicherheitsgründen eine Zwei-Faktor-Authentifizierung voraus. Diese bietet einen angemessenen Schutz und gilt als üblicher Industriestandard.

- Definieren Sie mögliche Zugriffsvarianten wie:
  – Applikationsbasierter Zugriff
  – Netzwerkbasierter Zugriff
  – Site-to-Site VPN-Zugriff
- Definieren Sie Kategorien (interne und externe Mitarbeitende, Kunden, Lieferanten, Gäste) und legen Sie fest, wem welche Zugriffsvariante mit welchem Service zugeordnet wird.

Umsetzungsstand

Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:

Massnahmen für mehr Verfügbarkeit

15. Sorgen Sie für eine unterbruchsfreie Stromversorgung

Wenn Sie auf eine hohe Verfügbarkeit Ihrer Daten und Systeme angewiesen sind, können Sie sich keinen Ausfall leisten. Eine unterbruchsfreie Stromversorgung (USV) schützt Ihre Systeme vor einem Stromausfall und Spannungsspitzen (z. B. Blitzeinschlag) und verhindert Datenverluste.

- Die unterbruchsfreie Stromversorgung (USV) wird zwischen der normalen Stromversorgung und den zu schützenden Geräten geschaltet.
- Bei einem Stromausfall versorgt die Batterie der USV die Komponenten so lange mit Strom, dass sie geregelt abgeschaltet werden können.
- Zusätzlich kann eine USV als Filter wirken und Ihre Systeme vor Spannungsschwankungen schützen.
- Neben dem Server müssen auch weitere wichtige Peripherie-Geräte an der USV angeschlossen werden. Dazu gehören beispielsweise wichtige Rechner im Netzwerk, Router, Backup-Systeme usw.
- Erstellen Sie eine Liste mit den Komponenten, die an die USV angeschlossen werden müssen. Aus dieser Zusammenstellung wird die benötigte Leistungsfähigkeit der USV bestimmt.
- Kontrollieren Sie regelmässig die Leistungsfähigkeit der Batterien der USV und ersetzen Sie schwache Batterien sofort (siehe Punkt 13).

Umsetzungsstand

Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:

16. Halten Sie wichtige Elemente redundant

Ein Ausfall eines kritischen Elements in Ihrem Netzwerk wie beispielsweise eines Servers kann viel Geld kosten und stört den Betrieb. Viele Unternehmen sind sich nicht bewusst, wie abhängig sie von kritischen Systemen sind. Um nach einem Ausfall möglichst schnell wieder den Betrieb aufzunehmen, empfiehlt es sich, kritische IT-Systeme (z. B. Harddisk, Netzteile, Netzwerkkomponenten oder ganze Server) redundant zu halten.

- Redundanz heisst, dass mindestens ein identisches Ersatzgerät oder -system vorhanden ist, welches das beschädigte Gerät oder System bei einem Ausfall ersetzt.
- Um den Ausfall einer Festplatte zu verhindern, kann eine sogenannte Festplattenspiegelung benützt werden. Falls eine Festplatte ausfällt, übernehmen automatisch andere Festplatten deren Aufgabe, ohne dass der Betrieb unterbrochen wird.
- Schliessen Sie mit Ihren Lieferanten Serviceverträge für Hard- und Software Interventionen (Reaktionszeiten, Lieferfristen usw.) ab.
- Erarbeiten Sie eventuell mit Ihrem Lieferanten Notfallpläne für Ausfallszenarien (siehe Punkt 17).
- Benutzen Sie nur Komponenten von namhaften Herstellern. Diese sind in der Regel von guter Qualität und wurden intensiv getestet.
- Denken Sie nicht nur an redundante IT-Systeme, sondern auch an eine redundante Internet-Anbindung.
- Wichtig ist, dass die Ersatzgeräte identisch sind und bereits vorkonfiguriert sind, damit sie im Ereignis sofort eingesetzt werden können.

Umsetzungsstand

Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:

Massnahmen für mehr Verfügbarkeit

17. Planen Sie die Notfallvorsorge

Ein existenzbedrohender Notfall tritt meistens plötzlich ein. Besonders höherer Gewalt ist man schutzlos ausgeliefert. Durch das richtige Verhalten kann in einer Notfallsituation der Schaden in Grenzen gehalten werden. Es muss deshalb im Voraus festgelegt werden, wie man sich bei einem Notfall verhält und welche Aktionen auszulösen sind.

- Überlegen Sie sich, welche Notfallsituationen in Ihrem Unternehmen eintreten können und wie darauf reagiert werden soll. Setzen Sie sich mit folgenden Ausfallszenarien auseinander: Ausfall der IT, Ausfall von Personal, Ausfall der Arbeitsplätze oder des Gebäudes und Ausfall externer Partner und Dienstleistungen.
- Bei einem Notfall muss schnell alarmiert und gehandelt werden. Jede Person muss genau wissen, wer alarmiert werden muss und wer verantwortlich ist. Erstellen Sie dazu einen Alarmierungsplan und eine Verantwortlichkeitsregelung.
- Erstellen Sie einen Notfallvorsorgeplan. Dazu gehören Sofortmassnahmen zur Einleitung des Notfallbetriebs, Regelungen für den Ablauf des Notfallbetriebs und Massnahmen zur schnellen Wiederherstellung des Normalbetriebes.
- Instruieren Sie die Mitarbeitenden, wie sie sich in Notfallsituationen zu verhalten haben und welche Sofortmassnahmen eingeleitet werden müssen.
- In Stress-Situationen handelt der Mensch oft intuitiv. Das richtige Verhalten im Ereignisfall muss deshalb geübt werden.
- Dokumentieren Sie alle IT-Komponenten ordnungsgemäss. Bewahren Sie diese Dokumentation extern auf.
- Zu einer Dokumentation gehören beispielsweise eine Liste der Benutzer, Gruppen und Rechte (siehe Punkt 9), das Netzwerklayout, die Konfigurationen der Systeme, Installationsbeschreibung, Konzepte, Arbeitsabläufe und Stellenbeschreibungen für sicherheitsrelevante Stellen. Führen Sie diese Dokumentationen regelmässig nach.
- Organisieren Sie Ausweichmöglichkeiten für die IT-Systeme mit der höchsten Verfügbarkeitsanforderung, damit schnell ein Weiterbetrieb gewährleistet werden kann.
- Überprüfen Sie die Reaktionszeit des Supports mit Ihren Verfügbarkeitsanforderungen. Kann z. B. ein Serverausfall wirklich in der benötigten Zeit behoben werden?

Umsetzungsstand

Vollständig umgesetzt.	Teilweise umgesetzt.	Nicht umgesetzt.
Kommentar:	Kommentar:	Kommentar:

18. Verteilen Sie das Know-how

Gerade in kleineren KMU steckt das entscheidende Wissen über die IT-Systeme oft nur bei einer Person. Fällt sie aus oder verlässt sie das Unternehmen, gerät es in Schwierigkeiten.

- Das Schlüsselwissen steckt in der Konfiguration, im Betrieb und im Unterhalt der IT-Systeme des Unternehmens. Versuchen Sie das Schlüssel-Wissen von Personen zu verteilen und zu dokumentieren.
- Krankheit, Unfall, Todesfall oder der Austritt aus dem Unternehmen können zum Verlust des Schlüsselwissens führen.
- Damit das Wissen bei einem Ausfall nicht verloren geht, sollten wichtige Systeme und Prozesse dokumentiert werden. Das erleichtert auch den Nachfolgern und neuen Mitarbeitenden, sich schnell zurechtzufinden (siehe Punkt 17).
- Bewahren Sie wichtige Passwörter im Doppel in einem Safe auf.
- Sichern Sie die geschäftsrelevanten Daten von ausgeschieden Mitarbeitern.

Umsetzungsstand

Vollständig umgesetzt.	Teilweise umgesetzt.	Nicht umgesetzt.
Kommentar:	Kommentar:	Kommentar:

Massnahmen im Umfeld der Ernährung			
19.	**Redundante Anbindung der WAN/Cloud**		
	Ein Ausfall des WAN/Cloud kann die Verbindung zu zentralen, dezentralen und Kundensysteme unterbrechen. • Redundante Anbindung ins WAN für alle für die Lebensmittelversorgung relevanten Systeme.		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
20.	**Verwenden Sie autonome Produktions- und Logistikplattformen**		
	Ein Ausfall des WAN/Cloud kann die Verbindung zu Ihren zentralen sowie dezentralen Systemen und Kundensystemen unterbrechen. Verkaufs-, Produktions- und Logistiksysteme stehen dann nicht mehr zur Verfügung. • Netzwerk segmentieren in: – übergreifendes Office-Netzwerk für alle zentral geführten Systeme – lokale Produktions-Netzwerke an den diversen Produktions- und Logistikstandorte • Sicherstellen, dass ICS/SCADA-Systeme unabhängig vom WAN autonom betrieben werden können: – Steuerung der Produktions- und Lagersysteme – Hausleit- und Überwachungssysteme – Logistik- und Kommissioniersysteme – Kassensysteme		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
21.	**Verwenden eines Kommunikationsstandards (z. B. EDI Electronic Data Interchange)**		
	GS1 Schweiz ist der Fachverband für nachhaltige Wertschöpfungsnetzwerke und ist Mitglied von GS1, dem weltweiten Netz von über hundert nationalen Organisationen, die ihren Mitgliedern hochstehende, auf gemeinsame Standards ausgerichtete Dienstleistungen anbieten. Sie verstehen sich als Kompetenzplattform für eine ganzheitliche Optimierung in Logistik, Supply Chain und Demand Management in der Schweiz und Lichtenstein. Wir empfehlen Ihnen: – sich an die internationalen Standards von GS1 zu halten – die empfohlenen Prozessmodelle zu verwenden – die praxisorientierte Weiterbildung zu nutzen		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:

Tabelle 50: 21 Schritte zu besserem Informationsschutz

6.1.2 Fünf Sicherheitsmassnahmen für industrielle Kontrollsysteme

Hier sind fünf wichtige Massnahmen, die Organisationen in ihrer ICS/SCADA-Umgebungen nutzen können. Die Anwendung dieser Schritte wird den Weg zu einer robusteren Sicherheitsumgebung ebnen und das Risiko für betriebliche Systeme erheblich reduzieren.

Fünf Sicherheitsmassnahmen für SCADA
1. Identifizieren, minimieren und sichern Sie alle Netzwerkverbindungen zur SCADA-Umgebung.
2. Härten Sie das SCADA und die unterstützenden Systeme, indem Sie unnötige Dienste, Ports und Protokolle deaktivieren, verfügbare Sicherheitsfunktionen aktivieren und robuste Konfigurationsmanagementpraktiken implementieren.
3. Überwachen und bewerten Sie die Sicherheit von SCADA-Systemen, den Netzwerken und insbesondere deren Zusammenschaltungen kontinuierlich.
4. Implementieren Sie einen risikobasierten und verteidigungsintegrierten Ansatz zur Sicherung von SCADA-Systemen und -Netzwerken.
5. Managen Sie die «menschlichen» Anforderungen der SCADA-Systeme, indem Sie die Erwartungen für die Leistung festlegen, die Einzelpersonen für ihre Leistungen verantwortlich machen, Richtlinien festlegen und SCADA-Sicherheits-training für alle Betreiber und Administratoren anbieten.

Tabelle 51: Fünf Sicherheitsmassnahmen für SCADA-Systeme

6.2 Grundlagen, Dokumente und Standards

Vorliegender IKT-Minimalstandard für die Lebensmittelversorgung 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 (SCADA-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 Lebensmittelversorgung	2016	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 im kritischen Teilsektor «Lebensmittelversorgung».
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 (u. a. Lebensmittelversorgung) 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)	2012	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 wie Lebensmittelversorgung – siehe weiter oben).

Titel	Jahr	Herausgeber & Beschreibung
Bundesgesetz über die wirtschaftliche Landesversorgung (Landesversorgungs-gesetz, LVG)	Stand 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 Versorgungs-systeme und Infrastrukturen beitragen. Eine dieser Massnahmen bildet der vorliegende IKT-Minimalstandard für die Lebensmittelversorgung.
Bundesgesetz über Lebensmittel und Gebrauchsgegenstände (Lebensmittelgesetz, LMG)	Stand 2013	Hrsg.: **Die Bundesversammlung der Schweizerischen Eidgenossenschaft** Dieses Gesetz bezweckt die Konsumenten vor Lebensmitteln und Gebrauchsgegen-ständen zu schützen, welche die Gesundheit gefährden können, den hygienischen Umgang mit Lebensmitteln sicherzustellen sowie die Konsumenten im Zusammenhang mit Lebensmitteln vor Täuschungen zu schützen.
KRITIS-Sekorstudie «Ernährung und Wasser»	Stand 2015	Hrsg.: **Bundesamt für Sicherheit in der Informationstechnik** Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist eine der zentralen Stellen Deutschlands unter den zuständigen Behörden zum Schutz von Kritischen Infrastrukturen. Mit unterschiedlichen Aktivitäten wie der Organisation von Branchen-gesprächen, der Bereitstellung von Standards und Leitfäden zu wichtigen IT Sicherheits-themen und nationalen Projekten sowie der Koordination des UP KRITIS verfolgt das BSI die Umsetzung der Nationalen Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) und der nationalen Cyber-Sicherheitsstrategie. In seinen Arbeiten ist das BSI auf genaue Kenntnisse zu den Funktionen kritischer Dienstleistungen und der damit verbundenen Bedeutung wichtiger Anlagen und Einrichtungen (KRITIS) angewiesen.
Risiko- und Krisen-management für die Ernährungsvorsorge in Österreich (EV-A)	Stand 2015	Hrsg.: **JOANNEUM RESEARCH, Agrarmarkt Austria** Der Bericht umfasst die Ergebnisse des Projekts Risiko- und Krisenmanagement für die Ernährungsvorsorge in Österreich (EV-A), das im Rahmen des österreichischen Sicherheitsforschungsförderprogramms KIRAS vom Bundesministerium für Verkehr, Innovation und Technologie finanziert wurde.

Tabelle 52: Dokumente der Schweizer Eidgenossenschaft und anderen Verwaltungen sowie Verbänden, die in der Lebensmittelversorgung von Bedeutung und anwendbar sind.

Tabelle 53 zeigt eine weiterführende Auswahl an internationalen Standards die teilweise in das vorliegende Dokument eingeflossen sind.

Titel	Jahr	Herausgeber & Beschreibung
ISO 27001:2013 Information technology – Security techniques – Information security management systems – Requirements **ISO 27002:2013 Information technology – Security techniques – Code of practice for information security controls**	2013	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: • 27000:2016 Übersicht und Vokabular (:2016 indiziert Jahr der Herausgabe) • 27001:2013 Anforderungen: Grundlagen mit Kontrollen und Kontrollzielen im Anhang • 27002:2013 Leitfaden für Kontrollen • 27003:2010 Anleitung zur Implementation • 27005:2011 Risiko Management Die ISO 27000 Security Standards sind mittlerweile die am meisten verbreiteten und dürften sich in den kommenden Jahren als die massgebenden erweisen. Schon heute liegt durchaus richtig, wer ISO Security Standards befolgt. Im Gegensatz zu anderen Standards, wie IT Grundschutz, ANSI/ISA oder NIST, sind sie nicht so sehr detailliert, dementsprechend flexibel anwendbar und können über eine längere Zeitspanne kontinuierlich verbessert und erweitert werden.
Guide to Industrial Control Systems (ICS) Security SP 800-82 Rev.2	2015	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.
ISA 62443 Industrial communication networks – Network and system security	2009 ff	Hrsg: **International Society of Automation (ISA)** Serie von insgesamt 13 *Industrial Automation and Control System (IACS)* Security Standards und technischen Berichten. Diese Normen sind allgemein anwendbar im Bereich industrieller Automation und nicht stromversorgungsspezifisch. Sie basieren auf den ISO 27000 Standards und erweitern diese mit Unterschieden und Spezifika industrieller Automation. Speziell zu erwähnen ist die Behandlung von Netzwerk- und Zonenarchitektur, die sich in anderen Standards kaum oder nicht so detailliert findet.
Recommended Practice: Improving Industrial Control System Cybersecurity with Defense in Depth Strategies	2016	Hrsg.: **Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)** Eine erweiterte und erneuerte Ausgabe einer früheren Veröffentlichung aus dem Jahre 2006. Umfassende Einführung in die Defense in Depth-Sicherheitsstrategie für industrielle Kontrollsysteme.

Tabelle 53: Nationale und internationale Standards zur IKT-Sicherheit

Titel	Jahr	Herausgeber & Beschreibung
BSI IT-Grundschutz-Kataloge 15. Ergänzung 2016 **BSI-Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz (V1.2 2014)** **BSI Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz**	2016	Hrsg.: **Bundesamt für Sicherheit in der Informationstechnik (BSI)** Der IT-Grundschutz beschreibt mit Hilfe der BSI-Standards 100-1 bis 100-4 eine Vorgehensweise zum Aufbau und zur Aufrechterhaltung eines Informations-Sicherheits-Management-Systems (ISMS). Die IT-Grundschutz-Kataloge beschreiben die Umsetzung der damit einhergehenden Massnahmen und Ziele. Das damit aufgebaute ISMS erfüllt die Anforderungen von ISO 27001 und verfügt über ein Äquivalent zu den Handlungsempfehlungen von ISO 27002. Sicherheit kann nach den vom BSI entwickelten Vorgehensweisen des IT-Grundschutzes, aber auch nach Standards der ISO 27000-Familie eingeführt und kontrolliert werden. Beide Möglichkeiten sind von ihrem Ansatz her kompatibel. Mit beiden wird ein ISMS aufgebaut und betrieben, mit dem Risiken im Bereich der Informationssicherheit ermittelt und durch geeignete Massnahmen auf ein akzeptables Mass reduziert werden. Ein wesentlicher Bestandteil eines ISMS nach ISO 27001 ist die Risikoanalyse und -bewertung, wohingegen eine Risikoanalyse beim BSI-Grundschutz nur in besonderen Fällen erforderlich ist. In den BSI-Grundschutzkatalogen wird die detaillierte Vorgehensweise zur Minimierung von Risiken beschrieben. Demnach lassen die ISO-Standards mehr Interpretation offen und sind flexibler, geben aber auch entsprechend weniger detailliert Anleitung und Unterstützung. Für den IT-Grundschutz-Ansatz gilt demnach entsprechend das Gegenteil und bietet, wie der Name sagt, einen «Grundschutz». Der Aufwand für eine ISO-basierte Zertifizierung ist geringer.
BSI ICS Security-Kompendium	2013	Hrsg.: **Bundesamt für Sicherheit in der Informationstechnik (BSI)** Das Kompendium stellt ein Grundlagenwerk dar und soll einen einfachen Zugang zur SCADA IT Security ermöglichen. Erläutert werden die notwendigen SCADA-Grundlagen, Abläufe, relevante Standards und ein konkreter Zusammenhang zum IT-Grundschutz, wobei auch Unterschiede und Lücken etablierter Standards und insbesondere des IT-Grundschutzes im Bereich SCADA-Security aufgezeigt werden.
BSI-Standard 100-1 Managementsysteme für Informations-sicherheit (ISMS)	2008	Hrsg.: **Bundesamt für Sicherheit in der Informationstechnik (BSI)** Der Standard beschreibt ISMS-relevante Methoden, Aufgaben und Aktivitäten, welche ein erfolgreiches ISMS ausmachen und welche Aufgaben auf die Führungsebene zukommen. Bei der Umsetzung der Empfehlungen hilft die Methodik des IT-Grundschutzes, die eine Schritt-für-Schritt-Anleitung für die Entwicklung eines ISMS in der Praxis gibt und konkrete Maßnahmen für alle Aspekte der Informationssicherheit nennt. Der Standard 100-1 richtet sich an Verantwortliche für den IT-Betrieb, Sicherheitsbeauftragte, -experten und -berater, welche mit dem Management für Informationssicherheit betraut sind.
BSI-Standard 100-2 IT-Grundschutz Vorgehensweise	2008	Hrsg.: **Bundesamt für Sicherheit in der Informationstechnik (BSI)** Die IT-Grundschutz-Vorgehensweise beschreibt Schritt für Schritt, wie ein Management-system für Informationssicherheit in der Praxis und mit Hilfe der Grundschutzkataloge aufgebaut und betrieben werden kann. Es wird sehr ausführlich darauf eingegangen, wie ein Sicherheitskonzept in der Praxis erstellt wird, wie angemessene Sicherheits-massnahmen ausgewählt werden und was bei der Umsetzung zu beachten ist.

Titel	Jahr	Herausgeber & Beschreibung
BSI-Standard 100-3 Risikoanalyse	2008	Hrsg.: **Bundesamt für Sicherheit in der Informationstechnik (BSI)** Dieses Dokument beschreibt eine Methodik zur Durchführung von Risikoanalysen, die ein bestehendes IT-Grundschutz-Sicherheitskonzept ergänzen. Dabei werden die in den IT-Grundschutz-Katalogen beschriebenen Gefährdungen als Hilfsmittel verwendet. Ein wesentlicher Unterschied zu den meisten anderen Risikoanalysemethoden ist das gänzliche Weglassen von Eintrittswahrscheinlichkeiten von Schadensereignissen.
BSI-Standard 100-4 Notfallorganisation	2008	Hrsg.: **Bundesamt für Sicherheit in der Informationstechnik (BSI)** Dieses Dokument beschreibt eine Methodik zur Etablierung eines Notfallmanagements, welche auf die in Standard 100-2 beschriebenen Vorgehensweisen aufsetzt und ergänzt. Beschrieben werden sämtliche Prozesse innerhalb einer Notfallorganisation von Business Impact-Analyse über Krisenmanagement bis hin zu Rückführung und kontinuierlichen Prozesstätigkeiten ausserhalb von Krisensituationen.
ISA 95/ISO 62264 Enterprise Control System Integration	2010 ff	Hrsg.: **International Society of Automation (ISA)** Eine Normenreihe von insgesamt 5 Standards zur Integration von Unternehmens-IT und Kontroll- und Leitsystemen.
Framework for Improving Critical Infrastructure Cybersecurity	2014	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.
Communication network dependencies for ICS/SCADA Systems	2016	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 cyber-physische 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.

Tabelle 53: Nationale und internationale Standards zur IKT-Sicherheit

6.3 Glossar

Abkürzung	Beschreibung
BABS	Bundesamt für Bevölkerungsschutz
BSI	Bundesamt für Sicherheit in der Informationstechnik (Deutschland)
BWL	Bundesamt für wirtschaftliche Landesversorgung
Detailhändler	Unternehmen zuständig für Verteilung und Verkauf von Lebensmitteln.
DMZ	Demilitarized Zone, Computernetz mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten (wird oft benutzt um eine logische Trennung zwischen zwei Netzwerkzonen sicherzustellen)
DNS	Domain Name System
eDec	Elektronische Datendeklaration. System der eidgenössischen Zollverwaltung für Importzollanmeldungen
EDV	Elektronische Datenverarbeitung
ENISA	European Union Agency for Network and Information Security
ERP	Enterprise Ressource Planning-System
Facility Control	Gebäudetechnik, Steuerung und Überwachung von Anlagen
Field	Feldebene
FINMA	Eidgenössische Finanzmarktaufsicht
HIDS	Host Intrusion Detection System
HMI	Human Maschine Interface, Stelle oder Handlung, mit der ein Mensch mit einer Maschine in Kontakt tritt
IaaS	Infrastructure as a Service
ICS	Wird synonym zum Begriff «SCADA» verwendet.
IDS	Intrusion Detection System
IKT	Informations- und Kommunikationstechnologie (dt. elektronische Datenverarbeitung EDV)
IP	Internet Protocol
IPS	Intrusion Prevention System
ISA	International Society of Automation
ISO	Internationale Organisation für Normung
ISB	Informatiksteuerungsorgan des Bundes
ISMS	Informationssicherheitsmanagementsystem
IT	Informationstechnologie, hier insbesondere Office-IT/Büroautomation. Alles was nicht OT/SCADA betrifft.
Kommunikations-netzwerk	Netzwerk des zur internen Daten- und Sprachkommunikation.
Leittechnik	Netz-, Stations- und Kraftwerksleittechnik
MELANI	Melde- und Analysestelle Informationssicherung (Informatiksteuerungsorgan des Bundes)

Abkürzung	Beschreibung
NIST	National Institute of Standards and Technology
MOU/MOA	Memorandum of Understanding/Agreement
MPLS	Multiprotokoll Label Switching, im Datenkommunikationsverkehr verwendete Technologie
MPLS-TP	Multiprotokoll Label Switching Transport Profile
NAC	Network Access Control
OT	Operational Technology (insbesondere SCADA-Systeme)
PaaS	Platform as a Service
PC	Personal Computer
PDH	Plesiochronous Digital Hierarchy, eine im Sprach- und Datenkommunikationsverkehr verwendete Technologie
Produktionssteuerung	Siehe SCADA
Produzent	Der Produzent ist verantwortlich für die Herstellung der Ressourcen (Getreide, Vieh, Zuckerrüben etc.). Ugs. Landwirt.
PRTG Network Monitor	PRTG Network Monitor ist eine umfassende Netzwerk-Monitoring-Lösung zur Überwachung von Up-/Downtime, Traffic und Nutzung.
SaaS	Software as a Service
SCADA	Supervisory Control and Data Acquisition, Überwachen und Steuern technischer Prozesse. Zum SCADA-System gehören neben der Steuerung und Überwachung auch die Sensoren, Leitungen, Computer und Leitstelle des (Produktions-)Systems. Gemeint sind insbesondere Kommissioniersysteme, Produktionssteuerungssysteme der Verarbeiter, sowie Kassensysteme der Detailhändler. Der Begriff «SCADA» wird hier synonym zum Begriff «ICS» verwendet.
SDH	Synchronous Digital Hierarchy, eine im Sprach- und Datenkommunikationsverkehr verwendete Technologie
SIEM	Security Incident and Event Management
SLA	Service Level Agreement, Dienstleistungsvereinbarung
Verarbeiter	Verarbeiter/Lebensmittelverarbeiter verwenden Rohstoffe (Getreide, Zucker, Fleisch, Öl etc.) um diese zu Produkten weiterzuverarbeiten. Der Verarbeiter ist Teil der Lebensmittelindustrie.
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network

Tabelle 54: Abkürzungsverzeichnis

6.4 Abbildungsverzeichnis

6.5 Tabellenverzeichnis

Autoren und Fachexperten der Erstausgabe

Vorname, Name	Firma	Funktion
Dario Walder	BWL	Hauptautor/Projektleitung
Daniel Caduff	BWL	Co-Autor
Walter Stadelmann	WL	Co-Autor/Fachexperte
Maximilian Müller	Emmi	Fachexperte/Quality Assurance
Ralf Kraekel	Migros	Fachexperte/Quality Assurance
Philippe Gehring	Cremo	Fachexperte/Quality Assurance
Franz Leugger	Coop	Fachexperte/Quality Assurance
Fabian Heiz	Coop	Fachexperte/Quality Assurance

Chronologie

Datum	Kurzbeschreibung
September 2016	Arbeitsaufnahme AG IKT-Ernährung der wirtschaftlichen Landesversorgung
Oktober 2017	Erarbeitung erster Entwurf des Dokumentes
Dezember 2017	Besprechung Entwurf 0.1 AG IKT-Ernährung WL
Februar 2018	Besprechung Entwurf 0.2 AG IKT-Ernährung WL
April 2018	Besprechung Entwurf 0.3 AG IKT-Ernährung WL
Juni-November 2018	Konsultation der Branchenverbände
Oktober 2018	Vernehmlassung in der wirtschaftlichen Landesversorgung

Haftungsausschluss

Das vorliegende Dokument mit Empfehlungen zur Verbesserung der Sicherheit von Informations- und Kommunikationssystemen der Lebensmittelversorgung sowie Systemen zur industriellen Steuerung der Lebensmittelverarbeitung 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 beim Anwender.

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

Konsultierte Verbände
IG Detailhandel Schweiz
Swiss Retail Federation