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

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

VBSA
ASED
ASIR

Vorwort

Liebe Anwenderinnen und Anwender
des IKT Minimalstandard für Abfallverwertungsanlagen

Sie alle arbeiten in der systemrelevanten Abfallbranche. Systemrelevant bedeutet, dass der Ausfall unserer Anlagen, vor allem der Kehrichtverwertungsanlagen, die Gesellschaft empfindlich treffen würde. Doch welches Ereignis könnte einen Ausfall herbeiführen? Ganz oben auf der Liste der Risikofaktoren stehen Cyberattacken. In jüngster Zeit wurden Unternehmen, Behörden und andere staatsnahe Organisationen – darunter auch KVA – wiederholt Opfer von gezielten, hoch professionell durchgeführten Cyberattacken. Durch diese Angriffe werden nicht nur Daten blockiert oder gelöscht, auch physische Anlagenbestandteile wie die Waage oder Turbinen können sabotiert, manipuliert oder zerstört werden. Ziel der Cyberkriminellen ist meistens die Erpressung von Geld oder das Zerstören und Stilllegen von Anlagen.

Eine KVA hat viele sensible Punkte, die Schwachstellen für Cyberangriffe aufweisen können. Als Beispiele seien die Waage, der Kran, das Prozessleitsystem, die Turbine oder Sensoren für Emissionsmessungen genannt. Hinzu kommen Fernzugriffe von Lieferanten für Wartung aller Art. Der heikelste Punkt bleibt allerdings der Faktor Mensch und sein manchmal unbedarfter Umgang mit den Informations- und Kommunikationstechnologien (IKT). Ein nachhaltiger Informationsschutz kann nur erreicht werden, wenn er von der Geschäftsleitung getragen und vorgelebt wird und wenn alle Mitarbeitenden einbezogen und geschult werden.

Wo stehen wir heute als Branche? Bis anhin wurde die Informationssicherheit in jeder Anlage sehr unterschiedlich gehandhabt. Während einige KVA dafür eine eigene Stelle geschaffen haben, wird das Thema in anderen Betrieben stiefmütterlich behandelt. Der vorliegende IKT Minimalstandard dient dazu, die Abwehr von Cyberkriminalität zu professionalisieren und zu vereinheitlichen. Er wurde als Handbuch von Praktikern für Praktiker geschrieben, fokussiert auf konkret umsetzbare Schutzmassnahmen und erfüllt somit die Voraussetzungen, nicht als «Papiertiger» in der Schublade eines Sicherheitsbeauftragten zu verschwinden. Mit der Anwendung des Handbuchs setzen Sie den vom Bundesamt für wirtschaftliche Landesversorgung (BWL) empfohlenen «IKT-Minimalstandard» in Ihrem Unternehmen um und leisten einen wichtigen Beitrag zur Cyber-Resilienz Ihres Betriebs.

Auch der VBSA unterstützt die Bestrebungen für mehr Informationssicherheit in der Abfallbranche. Er empfiehlt all seinen Mitgliedern die Umsetzung des vorliegenden Standards, stellt Plattformen für den Austausch bereit und setzt sich für eine offene Kommunikation über Vorfälle ein.

Gelingt es uns, Cyberkriminelle auszusperren, sparen wir viel Geld und Nerven und stellen eine reibungslose Abfallverwertung sicher – im Auftrag der Gesellschaft und im Sinn der Umwelt.

Robin Quartier
Ariane Stäubli
Geschäftsstelle VBSA

Inhaltsverzeichnis

1 Management Summary

Der vorliegende IKT-Minimalstandard adressiert systemrelevante Betriebe der Abfallentsorgung und stellt eine Empfehlung dar, wie Cyber-Risiken zukunftsorientiert und wirtschaftlich auf ein akzeptables Mass reduziert werden können. Eine erfolgreich verankerte Sicherheitsstrategie schützt die Mittel einer Organisation, die zur Ausführung der kritischen Geschäftsprozesse notwendig sind. Diese Strategie sollte neben technischen Massnahmen auch die dazu erforderlichen Prozesse, Ausbildung und Schulung der Mitarbeitenden, sowie die Security-Governance umfassen. Wer seinen Betrieb mit Informationssicherheit widerstandsfähiger macht, erzielt zusätzlich Geschäftsvorteile.

Im Folgenden wird aufgezeigt, warum der Umsetzung des IKT-Minimalstandards eine hohe Bedeutung zukommt:

I. Generell nimmt die Bedrohung zu, weil Cyberkriminalität ein sehr lukratives Geschäftsmodell darstellt und auch gezielte Industrie-Sabotage zu beobachten ist.

II. Mit voranschreitender Digitalisierung steigt die Notwendigkeit, Daten innerhalb der Unternehmensgrenzen ohne Medienbrüche auszutauschen. Als Beispiel sei das Ablesen und Auswerten von Sensoren entlang der Rauchgasreinigung genannt. Immer öfter werden heute ebenfalls Ansprüche an den unternehmensübergreifenden Datenaustausch gestellt, beispielsweise bei Fernwartungsarbeiten an Anlageteilen.

III. Steigende Abhängigkeiten von IKT-gesteuerten Prozessen öffnen Schwachstellen. In Industriebetrieben wie einer KVA wird zwischen Information Technology (IT)- und Operation Technology (OT)-Systemen unterschieden. Während IT-Systeme die elektronische Datenverarbeitung, z. B. bei administrativen Prozessen umfassen, bezeichnen OT-Systeme die Hard- und Software-Infrastruktur für die direkte Überwachung und/oder Steuerung von Industrieanlagen und Prozessen. Auch OT-Systeme wie z. B. Turbinensteuerungen können manipuliert oder ausser Kraft gesetzt werden. Folglich ist es bereits heute von entscheidender Wichtigkeit, für OT-Infrastrukturen ebenfalls nachhaltige und resiliente Sicherheitskonzepte zu implementieren und zu betreiben.

IV. Kritische Infrastrukturen (SKI) hängen gegenseitig voneinander ab (Entsorgung Spitalabfälle, Umweltschutz etc.).

Bei der Umsetzung einer Cyber-Strategie darf nicht vergessen werden, dass zur Stärkung der IKT-Sicherheit neben neuen Prozessen und Sicherheitssystemen ebenfalls zusätzliche personelle Ressourcen erforderlich sind. Denn auch das beste Sicherheitssystem verfehlt seine Wirkung, wenn dessen Alarme niemand beachtet und die Ursachen nicht systematisch verfolgt und bearbeitet werden.

Insbesondere in industriellen Anlagen mit kritischen Prozessen für die Versorgungssicherheit, zu welchen die KVA ebenfalls zählen, ist es wichtig, dass folgende Schutzziele der Informationssicherheit jederzeit unversehrt bleiben:

- Verfügbarkeit, Zuverlässigkeit der IT-Nutzung
- Vertraulichkeit, Schutz vor unbefugtem Zugang
- Integrität, Schutz vor Löschen und Verfälschung der elektronischen Information

Während in der IT (Datenanalyse, Management, Administration etc.), Vertraulichkeit, Integrität und Verfügbarkeit von Informationen gleichermassen wichtig sind, ist bei der OT die Verfügbarkeit das prioritäre Schutzziel (siehe Abbildung 1).

Im nächsten Abschnitt wird die zunehmend enge Verflechtung von IT- und OT-Systemen illustriert. Eine IT/OT-Konvergenz ermöglicht beispielsweise ortsunabhängig, umfassende Kontrollen des Betriebszustands sowie eine einfachere Analyse von Daten aus komplexen Systemen. Dadurch kann in Not- und Störungsfällen die Erarbeitung von Lösungen verbessert und beschleunigt werden, da Lieferanten, Führungskräfte und Mitarbeiter Einblick in «Echtzeitdaten» der Systeme und Anlagen haben.

Folgende Punkte zeigen abschliessend die Vorteile der Umsetzung und Verankerung einer Cyberstrategie gemäss dem IKT-Minimalstandard auf:

- Weniger isolierte IT- und OT-Systeme (Silos), Synergien werden genutzt.
- Geringere Entwicklungs-, Betriebs- und Supportkosten sowie weniger ungeplante Ausfallzeiten aufgrund der vorausschauenden Wartung.
- Verbesserte Einhaltung gesetzlicher Vorschriften, da die Implementierung einer Cyberstrategie eine bessere Transparenz, Verwaltung und Prüfung ermöglicht, sowohl für IT- wie OT-Systeme.
- Verbesserte Automatisierung und Sichtbarkeit der dezentralen OT, Stichwort Lieferanten, da die Möglichkeit entsteht, Wartungsdaten in Echtzeit zu übermitteln und auszuwerten.
- Effizientere Energie- und Ressourcennutzung, da die OT-Systeme besser auf den tatsächlichen Produktbedarf abgestimmt werden können. Als Beispiel sei der optimierte Einsatz von Betriebsmitteln aufgrund der Auswertung von sensorerhobenen Daten genannt.
- Effizienteres Anlagenmanagement, da alle IT- und OT-Systeme nach einer gemeinsamen Methodik erfasst, verwaltet und übersichtlich dargestellt werden.

KVA, die zukünftig den IKT-Minimalstandard systematisch umsetzen und die dadurch entstehenden Chancen nutzen, werden erkennen, dass IKT-Sicherheit nicht als Kostenfaktor, sondern als echter Geschäftsvorteil im Hinblick auf die Versorgungssicherheit der Schweiz angesehen werden kann.

IT-Sicherheit vs OT-Sicherheit

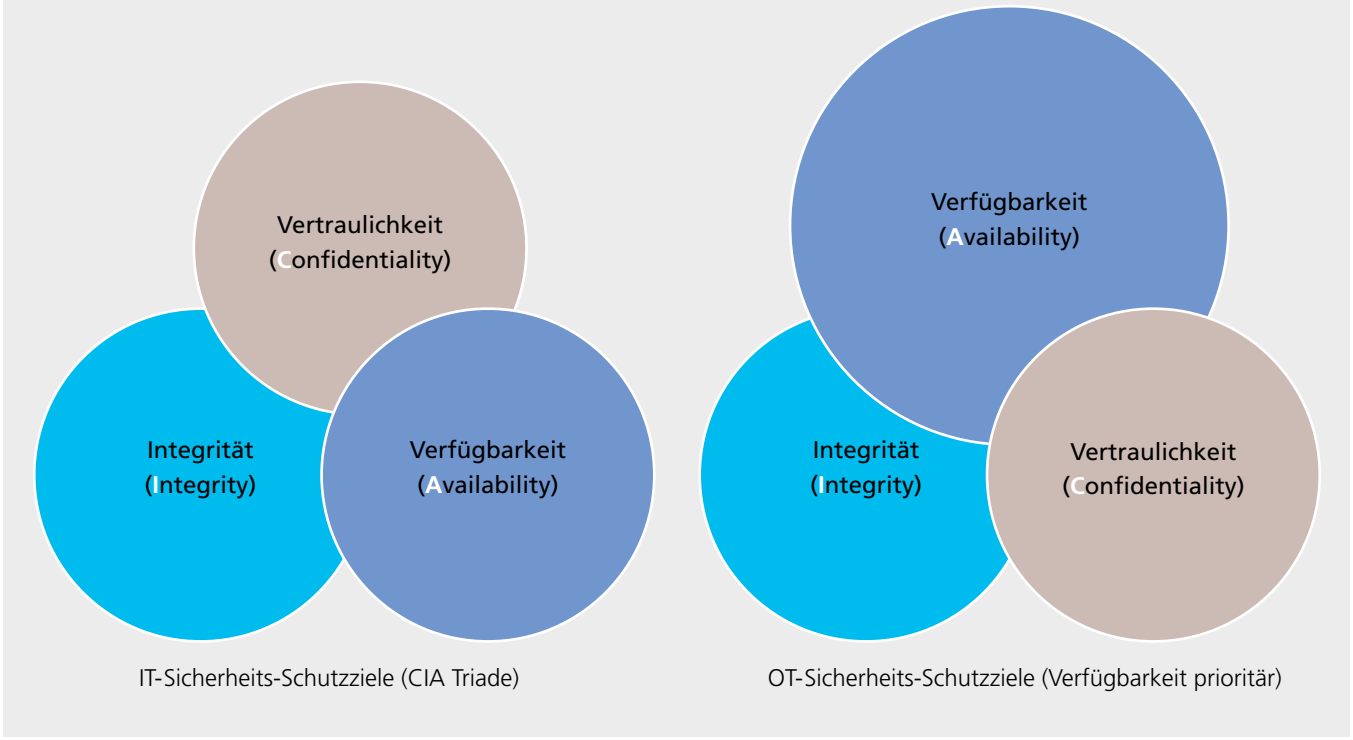

Abbildung 1: IT-Sicherheit vs OT-Sicherheit

2 Ausgangslage

In der Schweiz entstehen jährlich rund 80 bis 90 Millionen Tonnen Abfall. Den grössten Anteil machen unverschmutzte Aushub- und Ausbruchmaterialien sowie Rückbaumaterialien aus. Aufgrund des hohen Lebensstandards hat die Schweiz mit 716 kg Abfall pro Person eines der höchsten Siedlungsabfallaufkommen der Welt. Davon werden knapp 53 % rezykliert. Um den hohen Primärrohstoffverbrauch der Schweiz zu reduzieren, will der Bund sämtliche Material- und Stoffflüsse entlang der Wertschöpfungskette berücksichtigen – vom Rohstoffabbau über das Produktedesign bis zur Abfallbewirtschaftung.

Gemäss Umweltschutzgesetz lassen sich Abfälle wie folgt definieren[1]:

Abfälle sind bewegliche Sachen, deren sich der Inhaber entledigt oder deren Entsorgung im öffentlichen Interesse geboten ist.

Die Entsorgung der Abfälle umfasst ihre Verwertung oder Ablagerung sowie die Vorstufen Sammlung, Beförderung, Zwischenlagerung und Behandlung. Als Behandlung gilt jede physikalische, chemische oder biologische Veränderung der Abfälle.

Als Umgang gilt jede Tätigkeit im Zusammenhang mit Stoffen, Organismen oder Abfällen, insbesondere das Herstellen, Einführen, Ausführen, Inverkehrbringen, Verwenden, Lagern, Transportieren oder Entsorgen.

Die Gesamtheit aller Tätigkeiten und Aufgaben, die mit dem Vermeiden, Verringern, Verwerten und Ablagern von Abfällen zusammenhängen, wird als Abfallwirtschaft bezeichnet. Abfallwirtschaftliches Handeln kann öffentlich, privat oder in gemischten Formen organisiert sein.

Die Abfallwirtschaft beschäftigt sich mit:

- Strategischer Planung der Abfallbewirtschaftung auf lokaler, regionaler, kantonaler und nationaler Ebene
- Möglichkeiten der Abfallvermeidung und -verringerung, z. B. durch Abfallberatung
- Triage von Abfällen und Trennung von gemischt gesammelten Abfällen
- Verwertung und Recycling von Abfällen (z. B. Kompost, Ersatzbrennstoffe, Bauabfälle, Aushubmaterial, Metalle)
- Sammlung und Transport von Abfällen (Sammelstellen, Behältersysteme, Fahrzeuge, Umladestationen)
- Behandlung (mechanisch, chemisch, biologisch, thermisch) von Abfällen mit dem Ziel einer nachgeschalteten Verwertung (Recycling) bzw. der Ablagerung
- Ablagerung von Abfällen und Behandlungsrückständen auf Deponien (Standortsuche, Planung, Abfalleinbau, Deponiesickerwasser etc.)

Abfalltransport

Der Abfalltransport umfasst die verschiedenen Leistungen zur Sammlung bei den Verursachern/-innen und dem Transport der Abfälle von und zu den an der Verwertung und Ablagerung beteiligten Akteuren. Für den Transport sind Unternehmen zuständig, die Abfälle einsammeln und transportieren, Umschlagplätze betreiben, im Auftrag einer Gemeinde mobile Sammlungen von Sonderabfällen aus Haushalten durchführen und diese ohne Zwischenlagerung direkt an ein Entsorgungsunternehmen übergeben oder Saugwagenunternehmen, die Fahrzeuge ohne integrierte Abwasserbehandlung betreiben.

Eine grossflächige Störung in der Abfallentsorgung würde mittelfristig zu grossen Abfallbergen in den Städten und Gemeinden und vermutlich zur vielfachen, illegalen Entsorgung des Abfalls führen. In den Strassen würde es durch den gelagerten Müll zu gravierenden hygienischen Missständen mit einer möglichen Gefährdung der Gesundheit kommen. Bereits nach kurzer Zeit würden auch Betriebe und Unternehmungen unter dem Abfallaufkommen leiden: Kunden bleiben fern, die Produktion ist wegen fehlender Lagerkapazitäten nicht mehr möglich, unhygienische Zustände lassen eine normale Arbeit nicht zu, etc. Zudem besteht im Rahmen der Behandlung von Sonderabfällen die Gefahr einer Verschmutzung der Umwelt, der Verbreitung von Krankheiten oder gar des Ausbruchs von Seuchen.

[1] *Bundesgesetz über den Umweltschutz (USG), SR 814.01, Artikel 6*

Die folgende Darstellung zeigt den Aufbau der Branche und die Schnittstellen mit anderen kritischen Teilsektoren:

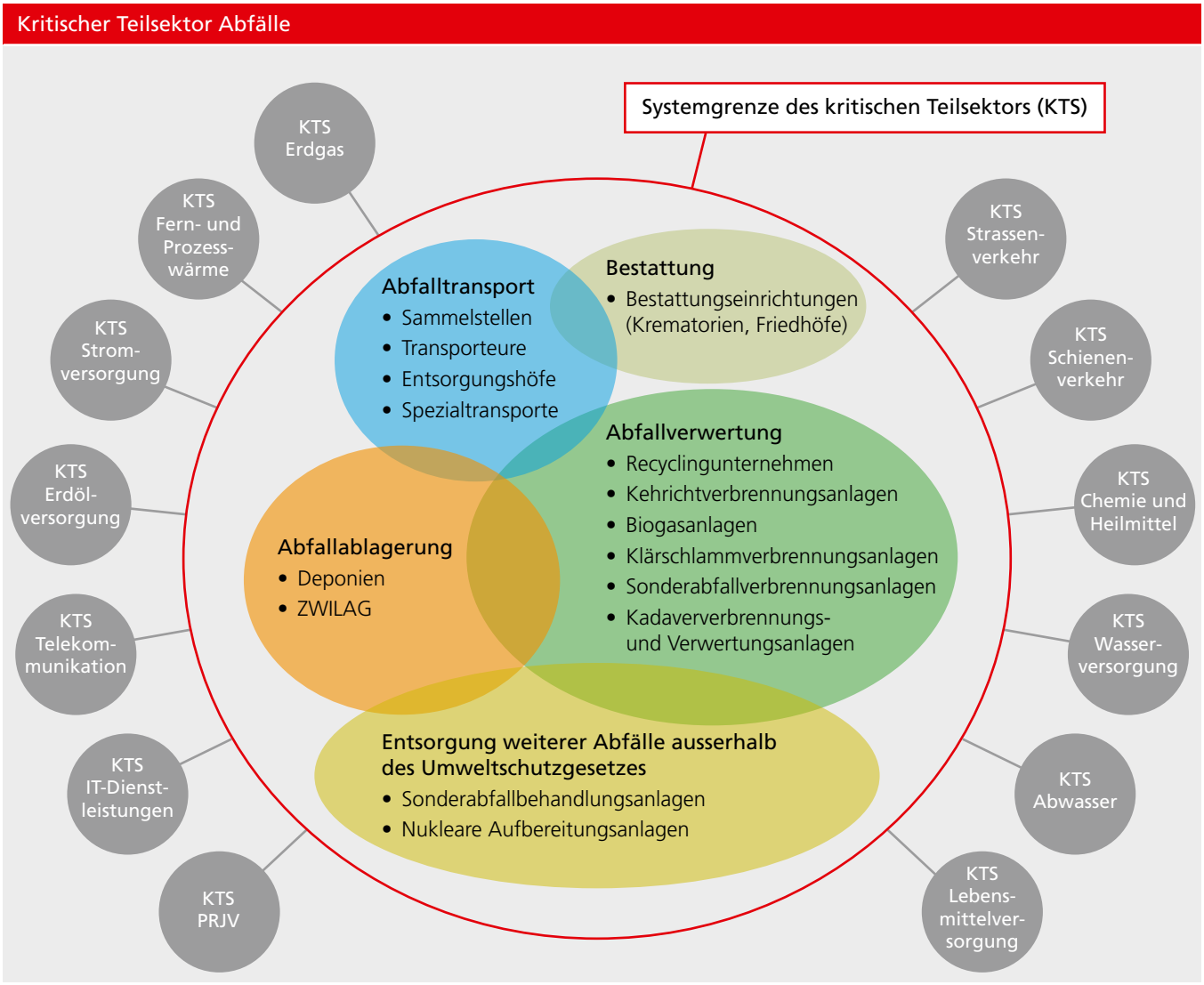

Abbildung 2: Kritischer Teilsektor Abfälle

Abfallverwertung

Im Rahmen der Abfallentsorgung werden verschiedenen Ziele wie Rückgewinnung von Rohstoffen (wo mit wirtschaftlich verhältnismässigen Massnahmen möglich), energetische Verwertung der Abfälle sowie Minimierung der langfristig zu deponierenden Abfallmenge verfolgt. Es werden dabei verschiedene Methoden zur thermischen sowie stofflichen Verwertung oder Kombinationen von beidem angewendet.

Die Schweizer KVA verbrannten im Jahr 2020 etwas mehr als 4 Millionen Tonnen Abfall und sind somit bei 100%iger Auslastung ihrer Kapazitäten. Der längere Ausfall einer Anlage würde die Entsorgungssituation in der Schweiz beträchtlich anspannen. Zusätzlich wird aus grenznahen ausländischen Gebieten Abfall angenommen, was ökologisch sinnvoll ist, da lange Abfalltransporte reduziert werden sollen. Zudem exportiert die Schweiz Hunderttausende von Tonnen von Abfällen, die nicht im Inland behandelt oder verwertet werden können (Sonderabfälle, getrennt gesammelte Kunststoffabfälle, etc.).

In der Schweiz gibt es derzeit 29 Kehrichtverwertungsanlagen (KVA) die sämtliche nicht anderweitig verwerteten Abfälle umweltschonend verbrennen. Die anfallende Wärme wird zu Heizzwecken und zur Stromerzeugung genutzt. Aus den verbleibenden Schlacken und Filterstäuben werden Metalle und andere Wertstoffe abgetrennt. Der Rest wird abgelagert.

Nebst den KVA gibt es andere thermische Anlagen wie z. B. Klärschlammverbrennungsanlagen oder Holzheizkraftwerke. So unterschiedlich diese Anlagen auch sind, sie haben als gemeinsamen Nenner die Entsorgung von Stoffen. Diese Abfälle mit teils hohem Heizwert eignen sich als Ersatzbrennstoffe für die Energie-Gewinnung oder zur Einsparung von Primärressourcen.

Biogene Abfälle werden vorteilshalber kompostiert oder vergärt, was gegenüber der Verbrennung in einer KVA deutliche ökologische Vorteile aufweist, weil die natürliche Substanz nach der Verwertung wieder in den natürlichen Kreislauf eingebracht wird.

Ungefähr die Hälfte der Siedlungsabfälle wird getrennt gesammelt, nachsortiert und kann deshalb zum Grossteil wiederverwertet werden. Zu den wichtigsten Rohstoffen, die aus Abfällen in den Produktionskreislauf zurückgeführt werden, gehören Papier, Glas, Grüngut, Metall, Holz und Textilien. Auch ein grosser Teil der mineralischen Bauabfälle wie zum Beispiel Beton wird wiederaufbereitet und lässt sich als Recycling-Baustoff wieder einsetzen.

Ein wichtiger Aspekt in Bezug auf die Abfallverwertung ist die Kommunikation der Behörden zum Umgang mit Abfällen. Ohne eine ständige Sensibilisierung und Information lässt das Wissen in der Bevölkerung zur korrekten und umweltgerechten Entsorgung schnell nach.

Der Teilbereich Abfallverwertung hat eine erhebliche unmittelbare wirtschaftliche Bedeutung durch die Wertschöpfung der Entsorgungsindustrie selbst sowie für die Abnehmer der in der Abfallverwertung gewonnen wiederverwertbaren Produkte, Rohstoffe und freigesetzten Energie in Form von Wärme und Elektrizität.

Abfallablagerung

Im Teilbereich Abfallablagerung wird die Deponierung und Ablagerung von Abfällen behandelt.

Abfälle, die nicht weiter verwertet werden können, müssen so behandelt werden, dass sie bei ihrer Ablagerung in einer Deponie keine Umweltschäden auslösen können. Je nach seiner Zusammensetzung und Schadstoffkonzentration wird ein Abfall in einem der fünf Deponietypen (A, B, C, D, E) endgelagert. Die Kriterien für die Zuordnung und Deponierfähigkeit der abzulagernden Abfälle sind in der Abfallverordnung (VVEA) definiert.

Stark kontaminierte Abfälle wie Filteraschen oder Rückstände aus der Wäsche von Filteraschen werden teilweise ins Ausland exportiert und dort in einer Untertagdeponie abgelagert.

Ein grosser Teil des Abfalls kann als Rohstoff der Verwertung zugeführt werden. Unter Abfallverwertung werden die thermische und die stoffliche Verwertung von Abfällen verstanden. Die gebräuchlichen Entsorgungsverfahren in der Schweiz werden im Folgenden beschrieben.

2.1 Stoffliche Abfallverwertung

Recycling

Recycling beschreibt einerseits die unmittelbare Wiederverwendung ausgedienter Produkte (z. B. Gebrauchtkleider oder funktionstüchtige Teile aus Altfahrzeugen), andererseits die stoffliche Verwertung, also die Gewinnung von Rohstoffen aus Abfall (z. B. Produktion von neuem Glas aus Scherben, das Einschmelzen von Eisenschrott oder das Herstellen von Recycling-Baustoffen aus Bauabfällen). Downcycling bezeichnet die Umwandlung von Abfällen zu Materialien von minderer Qualität als das ursprünglich verwendete Material.

Verwertung von Aushubmaterial und Bauabfällen

Bei der stofflichen Verwertung machen Aushubmaterial und Bauabfälle aus dem Rückbau von Gebäuden und baulichen Infrastrukturen mengenmässig den grössten Teil aus. Das Material entsteht sowohl beim kontrollierten Abbruch kompletter Gebäude und Etagen als auch bei der Erstellung von An- und Umbauten. Im Gegensatz zum früheren unkontrollierten Abbrechen mit der Abrissbirne oder durch Sprengung erfolgt der Abriss von Gebäuden heute oft als planmässiger Rückbau mit weitgehender Trennung der einzelnen Abfallfraktionen unmittelbar vor Ort.

Kompostierung und Vergärung

Ein weiterer wichtiger Bestandteil der stofflichen Abfallverwertung ist die Kompostierung und Vergärung von biogenen bzw. organischen Abfällen. Als organische Abfälle werden Abfälle pflanzlicher, tierischer oder mikrobieller Herkunft bezeichnet. Diese stammen aus der Landwirtschaft, der Lebensmittelindustrie und dem privaten Konsum.

2.2 Chemisch-physikalische oder biologische Behandlung

Chemisch-physikalische oder biologische Behandlungen befreien die Abfälle von Schadstoffen oder ermöglichen eine sichere Ablagerung. Biologische Verfahren wandeln mit Hilfe von Mikroorganismen oder Pflanzen Schadstoffe in unbedenkliche Produkte um. Dies umfasst hauptsächlich folgende Verfahren:

- Wässrige Abfälle werden durch Filtration, Fällung oder andere Techniken wie den Abbau durch Mikroorganismen so weit von Schadstoffen befreit, dass das Wasser in die Kanalisation eingeleitet werden kann. Die abgetrennten Schadstoffe werden je nach Zusammensetzung verbrannt oder deponiert.
- Flüssige Stoffgemische werden mit physikalischen Verfahren in ihre Einzelkomponenten aufgetrennt, um Teile davon wieder zu verwerten.
- Schlammförmige Abfälle müssen oftmals entwässert werden, damit sie verbrannt oder deponiert werden können.
- Feste Abfälle mit hohen Schadstoffgehalten dürfen nicht ohne Vorbehandlung in Deponien abgelagert werden. Schadstoffe in verunreinigtem Aushub können durch Wäsche abgereichert werden. Organische Schadstoffe werden mittels thermischer Behandlung zerstört oder mittels Mikroorganismen oder Pflanzen in unschädliche Stoffe umgewandelt. Stark schwermetallhaltige Abfälle wie Filterasche aus Abfallverwertungsanlagen werden vor der Deponierung sauer gewaschen, wobei eine Entfrachtung der Schwermetalle aus den Aschen stattfindet.

Deponien

Rückstände aus der Abfallverbrennung oder Abfälle, die sich nicht für eine stoffliche oder thermische Verwertung eignen, werden in gesetzeskonformen Deponien abgelagert. Erfüllen sie die Anforderungen an die Ablagerung nicht, müssen sie vorbehandelt werden.

2.3 Thermische Abfallverwertung

Die Verbrennung von Abfällen wird in der Schweiz zur Reduktion der zu deponierenden Abfallmenge und zur Sterilisierung der Abfälle genutzt. Die dabei freigesetzte Energie wird zurückgewonnen und weiterverwertet. Thermisch verwertet werden brennbare, stofflich nicht wiederverwertbare Abfälle. Diese werden in Kehrichtverbrennungsanlagen (KVA) oder in Zementwerken und sonstigen Industrieanlagen verbrannt. Alle Schweizer KVA nutzen die Verbrennungswärme zur Stromerzeugung oder zur Belieferung von Fernwärmenetzen und Industrieanlagen. Zudem werden Eisen, Aluminium, Kupfer und weitere Metalle aus der Schlacke zurückgewonnen.

In Zementwerken und sonstigen Industrieanlagen dienen Abfälle als Energielieferanten zur Erzeugung von Prozesswärme, die zur Herstellung bzw. Bearbeitung von Produkten (wie Zement) genutzt wird.

Bei der Verbrennung der Abfälle entstehen Luftschadstoffe, die durch eine mehrstufige Rauchgasreinigung und Entstickung weitgehend zurückgehalten werden, so dass nur noch geringe Mengen von Schadstoffen in die Umwelt gelangen.

Die folgende Grafik zeigt den Aufbau einer Kehrrichtverbrennungsanlage. Im vorliegenden Dokument wird der Teil Abfallentsorgung behandelt. Für den Bereich Fernwärmeteil, Stromversorgung und Abwasserbereich ist ein separater IKT-Minimalstandard erstellt worden (obschon die Anlagen meist alle Teile beinhalten).

Aufbau einer Kehrichtverbrennungsanlage

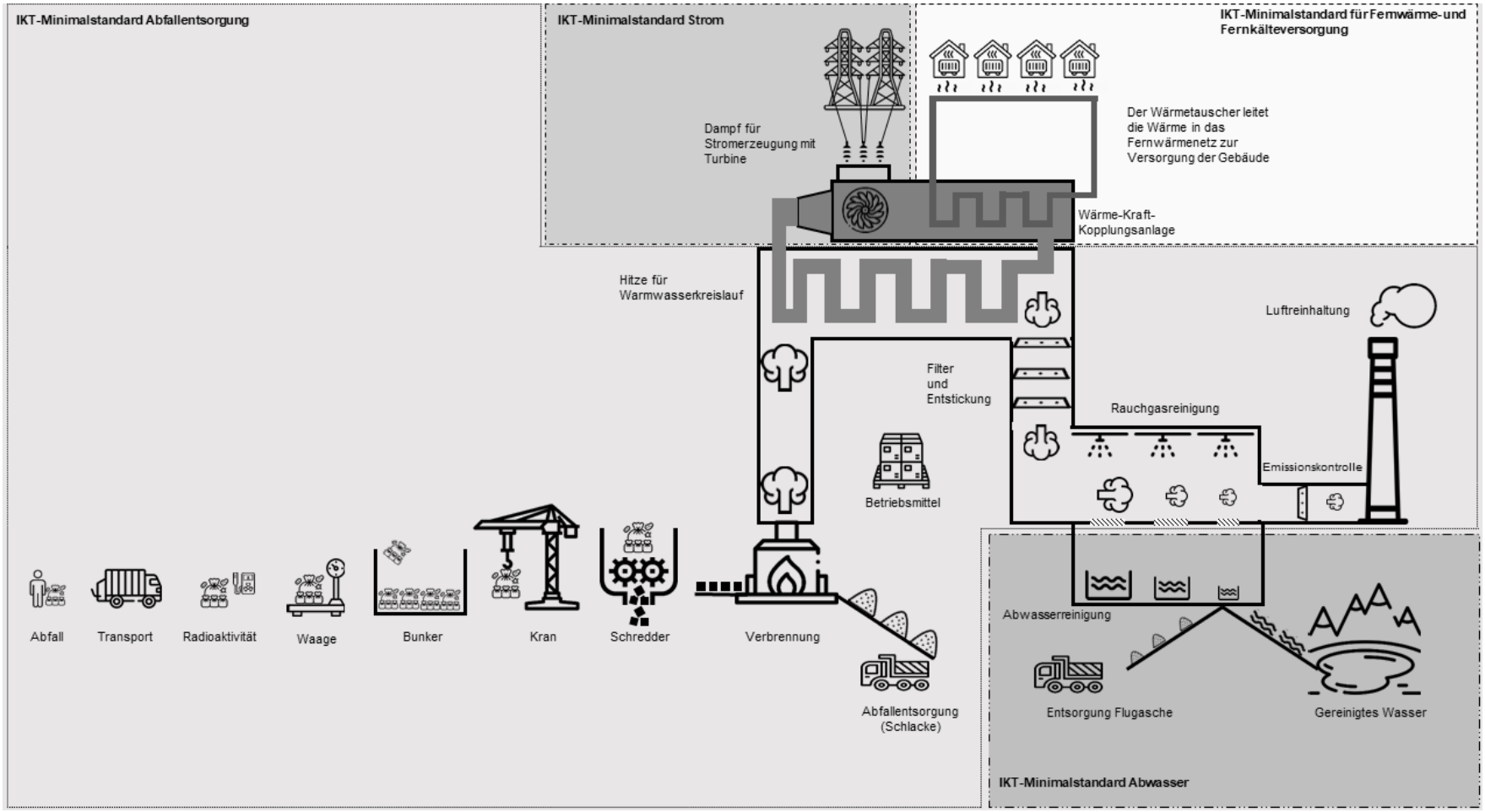

Abbildung 3: Aufbau einer Kehrichtverbrennungsanlage

3 Ziele des Minimalstandards

Das vorliegende Dokument adressiert Betriebe der Abfallentsorgung in der Schweiz und stellt eine Empfehlung dar, wie Informationsschutz-Risiken auf ein akzeptables Mass reduziert werden können. Dabei wird der «Risikobasierte Ansatz» sowie die «Defense in Depth-Strategie» angewendet.

Nebst der primären Aufgabe, Abfälle umweltschonend und gesetzeskonform zu entsorgen, entsteht bei der thermischen Abfallentsorgung nutzbare Energie. Zudem werden Metalle aus der Schlacke zurückgewonnen. Übrig bleiben kontaminierte Verbrennungs-Restprodukte, die in Deponien abgelagert werden müssen. Die Aufbereitung und anschliessende Deponierung verursachen zusätzliche Stoffströme, deren Behinderung oder Unterbrechung erheblich negativen Einfluss auf die Primäraufgabe, der thermischen Abfallverwertung, haben können. Diese exemplarische Betrachtung verdeutlicht, dass eine Kehrichtverbrennungsanlage selbst viele ungeahnte Angriffsvektoren liefert, die nicht unterschätzt werden dürfen.

Warum Informationsschutz betreiben:

- Generell nimmt die Bedrohung zu, weil Cyberkriminalität einerseits ein sehr lukratives Geschäftsmodell darstellt. Andererseits ist auch gezielte Industrie-Sabotage zu beobachten.
- Steigende Abhängigkeiten von Informations- und Steuerungssystemen öffnen Schwachstellen.
- Kritische Infrastrukturen hängen gegenseitig voneinander ab (Entsorgung Spitalabfälle, Umweltschutz etc.).
- Wer seinen Betrieb mit einer resilienten Informationssicherheit widerstandsfähiger macht, erzielt zusätzlich Geschäftsvorteile.

Die Umsetzung der Informationssicherheit nach diesem Standard erfolgt nach dem **risikobasierten Ansatz** Damit ist gemeint, dass die Prozesse nach Risiken bewertet und deren Auswirkung als Kritikalität quantifiziert wird. (Siehe Tabelle 3: Kritische Prozesse in den Kehrichtverbrennungsanlagen)

Als weitere Methode wird die Defense-in-Depth-Strategie angewendet:

Die Defense-in-Depth-Strategie leitet sich aus dem militärischen Prinzip ab, dass ein komplexes, mehrschichtiges Verteidigungssystem schwerer zu durchbrechen ist als eine einzelne Barriere. Ziel dieser Strategie ist es daher, mehrere Sicherheitsmassnahmen auf unterschiedlichen Schutzebenen anzuwenden und so den Angreifer zu zwingen, eine Vielzahl von komplexen Sicherheitsbarrieren zu überwinden.

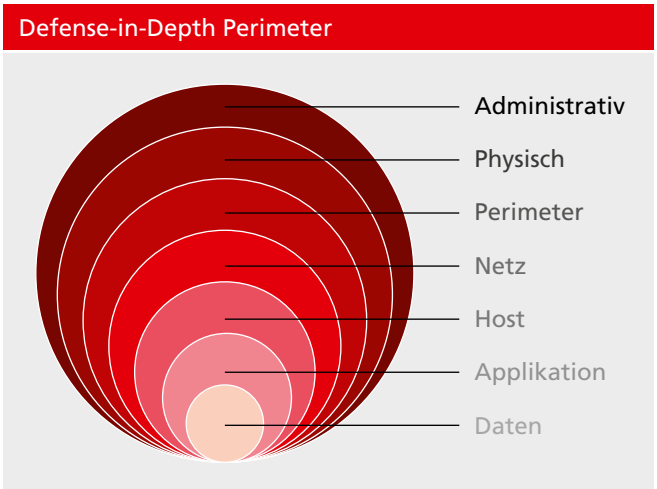

Abbildung 4: Defense-in-Depth Perimeter

4 Kritische Prozesse/Aktivitäten

In nachfolgender Grafik werden die möglichen Angriffsziele einer KVA aufgezeigt:

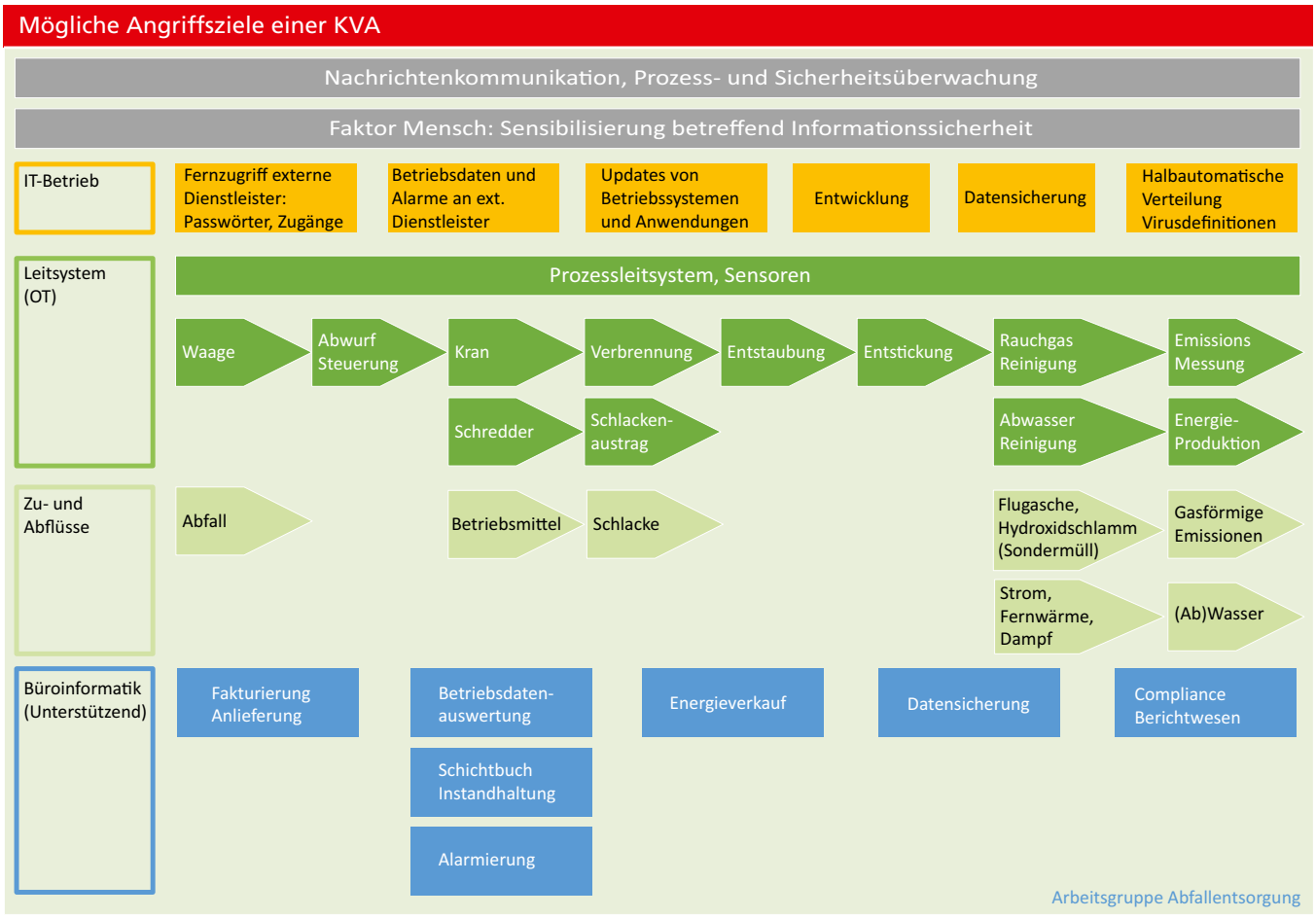

Abbildung 5: Mögliche Angriffsziele KVA

In Bezug auf die Verwundbarkeitsanalyse werden nachfolgend die Themenfelder mit Lösungsvorschlägen aufgeführt.

4.1 Kommunikation

Zuverlässig funktionierende Kommunikationssysteme für Wort und Schrift sind in der heutigen Zeit unerlässlich. Sei es als wichtiger Bestandteil eines reibungslosen Prozessablaufes oder zur Sicherstellung der Erreichbarkeit aller Personen im Betrieb in Notfallsituationen.

Nicht zu vernachlässigen ist insbesondere die Notkommunikation mit externen Stellen, damit in einer Krisensituation mit Behörden oder Blaulichtorganisationen kommuniziert werden kann. Die Definition der Kommunikationsmittel & -kanäle sollten im Vorfeld erfolgen und nicht erst in einer Krisensituation. Ebenfalls sollten Apps und Anwendungen (Messenger) definiert sein, welche für die mobile Kommunikation eingesetzt werden. Wichtig ist, dass nur Anwendungen eingesetzt werden, bei welchen die Übertragungssicherheit (z. B. durch Verschlüsselung) sichergestellt ist. Ebenfalls zu beachten ist, dass beim Einsatz von Apps auf mobilen Geräten keine Daten ungewollt synchronisiert werden und somit an Dritte abfliessen.

Um einen Systemausfall zu überbrücken, sollten wichtige Telefonnummern und Notfallpläne ausgedruckt und in einem Notfallordner abgelegt werden.

Interne Kommunikationsmittel	Externe Kommunikationsmittel
• IP-Telefonie • Funk, Betriebsfunk • DECT und WLAN-Telefone, Betreiber Schnurlostelefonie • Ausrufanlage/Evakuationsanlage • Betreiber GSM Anlage, GSM Telefone (Mobile Devices/Handy)	• Notleitung zur Quartiertelefonzentrale (Swisscom etc.) welche die interne Zentrale umgehen • Polycom Funkstation/Hand Funkgerät • GSM Telefone (Handy) • sichere Messenger • E-Mail-Ausfallsystem bereithalten

Tabelle 1: Interne und externe Kommunikation

Wie des Öfteren in der Technik gibt es auch in der Kommunikationstechnologie nicht eine Lösung zur Abdeckung des gesamten Spektrums von Anforderungen, sondern es ist eine Mischung von mehreren Lösungen notwendig, um die gewünschte Verfügbarkeit zu erlangen.

Beispielsweise sind GSM Systeme (Natel) weniger für die Kommunikation in abgeschirmten Gebäuden wie Stahlbauten oder in Kellergeschossen geeignet, da ohne aufwändige interne Antennenanlagen die Empfangsleistung der Geräte stark eingeschränkt ist. Dasselbe gilt für herkömmlichen Betriebsfunk im 4 m, 2 m, und 70 cm Bandbereich und DECT-Telefonieanlagen. Auch diese benötigen Antennen und Relaisstationen zur einwandfreien Kommunikation in Untergeschossen und Räumen mit starker elektromagnetischer Abschirmung.

Beim Einsatz von Messengerdiensten sollte darauf geachtet werden, dass keine Daten, insbesondere Kontaktdaten vom Gerät zum Lösungsanbieter kopiert werden. Ebenfalls sollte der Dienst eine «End to End»-Verschlüsselung der Sprach- und Textnachrichten anbieten, damit eine gesicherte Kommunikation bis auf Stufe «Vertraulich» gemacht werden kann.

4.2 Faktor Mensch – Mitarbeiterschulung und Sensibilisierung

Die grosse Mehrheit aller Cyberangriffe beginnt mit einem Mitarbeiter, welcher einen Fehler macht. Awareness-Schulungen und Sensibilisierungen sollen der «Schwachstelle Mensch» entgegenwirken. Eine Beschreibung zum Thema Awareness ist im Kapitel 6.6 beschrieben. Für die folgenden Themen sollten Mitarbeiter sensibilisiert werden:

Angriffsmöglichkeit	Bedrohung
Spam- und Phishing-Mails	Bösartige E-Mails stellen eine immer wiederkehrende Bedrohung für die Informationssicherheit eines Unternehmens dar. Als Spam- oder Junk-Mails werden unerwünschte, auf elektronischem Weg massenhaft übertragene Nachrichten bezeichnet, die dem Empfänger unverlangt zugestellt werden, ihn oft belästigen und auch häufig werbenden Inhalt enthalten. Spam-Mail können den E-Mail-Server des Unternehmens «überfluten» und so verlangsamen oder gar lahmlegen. Eine weitaus bedrohlichere Gefahr stellen die Phishing-Mails dar. Phishing ist der Versand gefälschter E-Mails, die den Nutzer dazu verleiten sollen, auf einen Betrug hereinzufallen. Phishing-Mails zielen häufig darauf ab, dass die Nutzer Finanzinformationen, Zugangsdaten oder andere sensible Informationen preisgeben.
Malware	«Malicious Software» oder kurz «Malware» sind Programme, die den Systemen oder Benutzern schaden und sich oftmals selbständig weiterverbreiten. Der Schaden kann z. B. entstehen, indem der Angreifer Daten ausspioniert (Tastatur, Festplatte) oder verschlüsselt sowie Zugriffe von Administratoren erlangt. Bekannte Formen von Malware sind z. B. Viren, Trojaner, Spy- oder Ransomware.
Social Engineering	Beim Social Engineering geht es um die zwischenmenschliche Beeinflussung einer Person. Dabei versucht der Hacker das Vertrauen des Opfers zu gewinnen und ihn so zum Beispiel zur Preisgabe von vertraulichen Informationen oder zur Freigabe von Kreditkartendaten und Passwörtern zu bewegen. Social Engineering findet gleichermassen physisch, per E-Mail, am Telefon oder in den sozialen Medien statt.

Tabelle 2: Angriffsmöglichkeit und Bedrohung

Wie eingangs des Kapitels bereits erwähnt, sind die obenerwähnten menschlichen Verwundbarkeiten die grössten Einfallstore für erfolgreiche Cyberangriffe. Aus diesem Grund sollten Mitarbeiter in einem fortlaufenden Awareness Programm regelmässig 2–3-mal jährlich zum Thema der Informationssicherheit geschult werden. Die angestrebte Wahrnehmung der Informationssicherheit sollte so sein, dass sich die Mitarbeiter intuitiv richtig verhalten, was in der Kompetenzstufenentwicklung als «unbewusste Kompetenz» bezeichnet wird.

Angestrebte Awareness-Entwicklung der Mitarbeiter

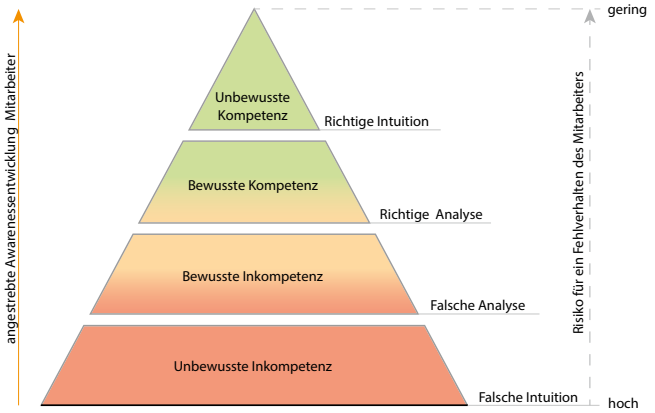

Abbildung 6: Angestrebte Awareness-Entwicklung der Mitarbeiter

4.3 Videosystem

Das Videosystem stellt ein weiteres unverzichtbares Glied in der physischen Sicherheitskette dar, welches jedoch ohne qualifizierte Einführung und geregelten Betrieb einige Risiken mit sich bringt. Eines der wichtigen Themen ist hierbei die Einhaltung des Datenschutzgesetzes (DSG). Um dies sicherzustellen, bedarf es eines Betriebskonzepts welche u. a. beschreibt was, wo und wann aufgezeichnet wird, welche Benutzer Zugang zum Bildmaterial haben, wie lange Bilder aufbewahrt werden und wer eine Auswertung in welchen Fällen anordnen darf. Ein besonderes Augenmerk gilt hier auch der Datensicherung, denn da muss ebenfalls sichergestellt werden, dass die Bilder nach der Aufbewahrungsfrist gelöscht werden.

Einsatzbeispiele von Videoüberwachung sind:

- Zutrittsüberwachung an der Perimetergrenze (Haupt-/Seiten eingänge)
- Prozessüberwachungen (Bunker, Abwurfsystem, Waage etc.)
- Überwachung von sensiblen Räumlichkeiten (Serverräume)
- Heutige Videosysteme sind in der Lage, Aufzeichnungen ereignisbasiert zu starten. Diese Möglichkeit erlauben es, Livebilder bei einem Vorfall direkt in der Leitzentrale anzuzeigen und so das Risiko eines Prozessausfalls zu minimieren.

4.4 IT-Betrieb

4.4.1 Fernwartung durch externe Dienstleister

Systeme, insbesondere solche welche für die Sicherstellung des gesetzlichen Entsorgungs- oder Versorgungsauftrages wichtig sind, sollen **nie permanent** per Fernwartungszugang für die Dienstleister zugänglich sein.

Zugänge von extern sollten:

a) netzwerktechnisch bei Nichtgebrauch geschlossen werden.
b) nur über vorangemeldete und zeitlich begrenzte Wartungszugänge und über sichere Verbindungen (z. B. VPN) zugänglich sein.
c) die Anzahl der zugreifenden Benutzer des Dienstleisters auf das notwendige Minimum reduziert, namentlich bekannt und mit eigenem Account ausgestattet sein.
d) die Wartungszugänge idealerweise über ein zentral verwaltetes Privileged Access Management System (PAM) mit einer Multifaktor Authentifizierung (MFA) und Aufzeichnungs- oder Logfunktionalität (Audit Trail) erfolgen. Die Zugriffe sollten nach einer einheitlichen Governance erfolgen. Sind zwingende Ausnahmen notwendig, sollten diese dokumentiert und überwacht werden.

Passwörter für den Systemzugriff sollten durch den Systemadministrator in regelmässigen Abständen erneuert werden, um sicher zu stellen, dass ausgetretenes Personal vom Dienstleister keinen Systemzugriff mehr hat.

4.4.2 Betriebsdaten an externe Dienstleister

Betriebsdaten, welche von externen Dienstleistern und Lieferanten benötigt werden sind in der Regel keine online-Prozessdaten. Dadurch können diese automatisiert vom Prozessleitsystem auf ein Verzeichnis ausserhalb der Prozessnetzwerkes geschrieben werden. So kann der Dienstleister seine Daten bei Bedarf beziehen, ohne dass ihm Zugriff auf das Leitsystem gewährt werden muss.

Das direkte Kopieren von Informationen während einer Fernwartungssitzung sollte unterbunden werden. Alternativ sollte dem Benutzer jedoch ein Transferlaufwerk zur Verfügung gestellt werden.

Sehr empfehlenswert ist es, in den Verträgen oder einem Service-Level-Agreement (SLA), eine Dienstleistungs-Vereinbarung mit dem externen Lieferanten/Dienstleister festzulegen, welche Daten zu welchem Zweck übergeben, über welche gesicherten Wege zum Lieferanten übermittelt und wie lange sie dort aufbewahrt werden.

4.4.3 Alarme

Unter Alarmsystemen verstehen wir Brandmeldeanlagen, manuelles oder workflowbasiertes Aufbieten von Blaulicht-Organisationen bei Personenschaden und schweren Havarien sowie das automatisierte Aufbieten von weiterem Personal und Unterstützungseinheiten. Evakuierungsalarme gehören ebenfalls dazu.

4.4.4 Updates von Betriebssystemen und Programmen

Vollständig automatisierte Updates in OT-Netzwerken sind sehr risikobehaftet und deshalb nicht empfehlenswert. Updates in industriellen Anlagen sollten vom Hersteller validiert, freigegeben und idealerweise auch installiert werden. Diese Leistungen müssen in einem SLA definiert und abgegrenzt werden. Die Anzahl an geplanten Updatezyklen pro Jahr, sowie die Reaktionszeit bis zur Verfügbarkeit von wichtigen Sicherheitsupdates zwischen den geplanten Zyklen ist ebenfalls in dem SLA festzulegen.

Als OT-Netzwerke noch vollständig autark und vom Internet getrennt waren, reichte es aus, die Systeme 1–2-mal jährlich zu aktualisieren und Sicherheitslücken zu schliessen. Jedoch mit der zunehmenden Vernetzung und Verschmelzung von IT und OT nehmen auch die Anforderungen an regelmässige System-Updates laufend zu. Systeme, bei welchen ein regelmässiges Software-Update nicht oder nicht mehr möglich ist, sollten vollständig isoliert oder nur mit sehr restriktiven Zugangsbeschränkungen von weniger vertrauenswürdigen Zonen her erreichbar sein.

Der Prozess des Software-Updates sollte für interne Anwendung in einer Richtlinie und extern in einem SLA beschrieben und vereinbart sein. Die Einhaltung der SLA-Leistungen inkl. deren Dokumentation sollte mindestens 1 x jährlich mit dem Leistungserbringer besprochen und überprüft werden.

4.4.5 Entwicklung

Sollen eigene Softwareentwicklungen oder -anpassungen gemacht werden, ist es beinahe unumgänglich ein Test- und Integrationssystem, welches dem Produktivsystem entspricht, aufzubauen. Da das Betreiben von einer, zwei oder gar drei Systemlandschaften hinsichtlich personeller und finanzieller Ressourcen sehr aufwändig ist, ist hier der «Make or buy»-Entscheid besonders wichtig, d. h. welcher Nutzen resp. welche Kosten und Risiken entstehen dem Unternehmen durch den eigenen Softwareentwicklungsprozess und die dafür notwendige Infrastruktur, gegenüber der kompletten Auslagerung zu einem Leistungserbringer.

4.4.6 Backup und Sicherungen

Um das Risiko und die Folgen eines Datenverlusts zu reduzieren (z. B. durch unbeabsichtigte Änderungen der Daten, Hardwaredefekte), sollte möglichst von allen IT-Systemen in regelmässigen Abständen Datensicherungen durchgeführt werden. Die Backup-Strategie sollte verschiedene Örtlichkeiten für die Datensicherung vorsehen. Daher ist es zu empfehlen, für den schnellen Zugriff eine Datensicherung lokal auf den IT-Systemen vorzuhalten und zusätzlich eine Datensicherung auf einem zentralen System anzulegen. Um auch der Gefahr eines Ransomware-Angriffs vorzubeugen, sollte eine weitere Kopie der Datensicherung auf einem logisch und physisch getrennten System («Air Gap») gespeichert werden.

Die 3-2-1 Datensicherungsstrategie

Datensicherungen von entfernten Cloud-Systemen sollten mit geeigneter Technologie ebenfalls in denselben Infrastrukturen wie die lokalen Systeme gesichert werden, um einen Zugriff in Krisensituationen sicherzustellen. Ist dies nicht möglich, sollte mit dem Leistungserbringer entsprechende Business Continuity Management (BCM) Verfahren u. a. bezüglich Verfügbarkeit, Zugriff, Datentransport, Datenübergabe definiert werden.

Quelle: computerweekly.de

Abbildung 7: Datensicherungsstrategie

Die Datensicherung sollte folgende Informationen und Daten beinhalten:

- Betriebssysteme und Firmware
- Konfigurationen (z. B. Router, Switches, Anwendungen Firewall Regelwerk)
- Anwendungen
- Datenbanken
- Produktionsdaten
- sonstige Daten (z. B. Protokolldaten)

4.4.7 Verteilung von Virusdefinitionen

Eine automatisierte und direkte Verteilung von Malwaredefinitionen ohne vorgelagerte Testszenarien ist in einer OT-Infrastruktur nicht empfehlenswert und risikobehaftet. Eine beschädigte oder fehlerhafte Datei könnte eines oder mehrere Systeme beeinträchtigen oder gar zum Ausfall bringen.

Aus diesem Grund ist es empfehlenswert, die Malware Definitionspakete vor der Verteilung auf einer Testinstallation eingehend zu prüfen. Ebenfalls sollte dabei, wenn möglich die Unversehrtheit der Datei durch eine Prüfsumme (MD5 Hash) verifiziert werden. Ist dies durch die fehlende Infrastruktur nicht möglich, stellt eine sequenzielle Verteilung eine gute Lösungsvariante dar. Zwischen den einzelnen Verteilschritten sollte zur Risikominderung sichergestellt werden, dass die bereits aktualisierten Systeme fehlerfrei und stabil laufen. Eine sequenzielle Verteilung sollte sich jedoch auch nicht über Wochen hinausziehen, da sonst das Risiko einer unerkannten Malware im System droht.

4.5 OT-Prozesse

4.5.1 Waage

Mit der Waage werden sämtliche Fahrzeuge vor resp. nach dem Abladen von Müll, Klärschlamm, Verbrauchsgütern (Betriebsmittel) o. ä. gewogen. Damit werden die angelieferten Mengen genau erfasst und überprüft, schliesslich wird auch anhand dieser Mengen abgerechnet.

Für den reibungslosen Betrieb der Verbrennungslinien ist es unerlässlich, sämtliche Massenströme und deren Zusammensetzung möglichst genau zu kennen. Daraus wird einerseits ermittelt, wie viel Müll/Klärschlamm entsorgt wird oder gebunkert werden soll, um die Ofenlinien über die ganze Laufzeit optimal zu betreiben, anderseits lässt sich aus diesen Zahlen auch ableiten, wie viel Verbrauchsgüter (Betriebsmittel) über die Zeit benötigt werden und wie gut der Verbrennungsprozess abläuft.

Die Waage besteht im Wesentlichen aus einem Wäge-System, einer Anzeige, Barrieren und/oder Ampeln und einer Schnittstelle zu einem oder mehreren Fremdsystemen (Betriebsdaten, Büro, Fakturierung), an welche die Daten weitergeleitet werden. Oft wird dafür ein Komplett-System mit einer speicherprogrammierbaren Steuerung (SPS) verwendet.

Die Waage als solche ist ein nicht hoch-kritischer Prozess und die Wägung kann in einem Notfall auch händisch erfolgen, allerdings wird oft unterschätzt, was die Folgen eines solchen Ausfalls für einen Betrieb sein können.

4.5.2 Abwurfsystem, Abkippstelle

Die Anlieferung des Mülls erfolgt in der Regel mit Lastwagen, Zügen oder in seltenen Fällen auch mit Schiffen. Je nach Anlagesituation wird der Müll entweder direkt in den Bunker gekippt oder wird mit Hilfe einer Abwurfeinrichtung in den Bunker befördert. Dies wird auf verschiedene Arten umgesetzt, z. B. wird der Müll auf einen Abwurftisch gekippt, und erst anschliessend wird der ganze Müll auf dem Tisch über eine Kippvorrichtung (Abwurf) in den Bunker befördert. In der Regel wird eine solche Anlage über eine SPS gesteuert. Diese SPS kann autonom (über ein Bedienfeld), über eine Hardware-Schnittstelle zum Leitsystem oder direkt im Leitsystem integriert und betrieben werden. Eine KVA verfügt in der Regel über mehrere Abwurflinien. Je nach Anlagesituation muss die Steuerung so ausgelegt sein, dass

ein Ausfall einer solchen Steuerung die Anlieferung durch Müll resp. dessen Abwurf nicht komplett verhindert, da dies zu Nachschub-Problemen resp. zu einem Abfall-Stau bei der Anlieferung führen kann. Das Risiko eines Komplettausfalls kann durch unabhängige oder redundante Steuerungskonzepte verhindert resp. minimiert werden.

4.5.3 Kran (und Abwurf)

Mithilfe des Krans wird der angelieferte Müll im Bunker vermischt, angehäuft und schliesslich in den Einfüllschacht des Ofens geführt. Der Kranführer bedient diesen in der Regel aus dem Kontrollraum heraus, von wo aus auch der ganze Verbrennungsprozess überwacht wird.

Der Automationsgrad dieser Kräne ist bereits sehr hoch, sodass die Beschickung des Ofens häufig voll automatisiert ist. In der Konsequenz besitzen diese Systeme oft eine Schnittstelle zum Leitsystem, wo die benötigte Menge an Kehricht angefordert wird. Die Kräne verfügen entsprechend über ein eigenes Wägesystem, so wird die angeforderte Menge resp. die gelieferte Menge stets gemessen und protokolliert.

Die Kran-Steuerung wird üblicherweise ebenfalls mit einer SPS umgesetzt, je nach Automationsgrad sind Schnittstellen zu Fremdsystemen vorhanden. Der Kranführer bedient den Kran in der Regel über Joysticks und wird dabei durch Kamerasysteme und/oder einer Anzeige unterstützt. Aufgrund der nötigen hohen Verfügbarkeit wird der Kran oft redundant betrieben, d. h. ein zweiter Kran steht zur Verfügung, sollte ein Defekt auftreten.

4.5.4 Schredder

Der Schredder wird dafür verwendet, Sperrgut oder Ähnliches zu zerkleinern. Üblicherweise wird das zu schreddernde Material separat vom Hausmüll angeliefert.

Je nach Anlage wird das zu schreddernde Material separat gebunkert oder es wird direkt nach der Anlieferung geschreddert und erst danach dem Hausmüll beigemischt.

Oft aber wird der Sperrmüll nur in einem Bunker gelagert, dann entscheidet der Kranführer direkt bei dessen Anlieferung, ob dieser Müll geschreddert werden muss, bevor er mit dem restlichen Müll im Bunker vermengt wird. Hier gibt es sehr viele verschiedene Anwendungen resp. Prozesse, somit muss das Ausfallrisiko jedes Schredders für jede Anlage spezifisch beurteilt werden. Wenn der Sperrmüll aufgrund eines Ausfalls des Schredders nicht mehr zerkleinert werden kann und keine andere Möglichkeit besteht, diesen Müll gesondert zu zerkleinern oder zu lagern, kann dies sehr schnell zu einem Engpass im Prozess führen. So kann sich z. B. die Brenneigenschaft des Mülls sehr rasch ändern, und der Ofen lässt sich in der Folge schlechter regeln.

Auch die Schreddersteuerung wird oft mit einer SPS umgesetzt. Je nach Anlage können mehrere Schredder (unabhängig) voneinander vorhanden sein, welche auch individuell beschickt werden. Oft wir ein Schredder mit Hilfe des Krans mit Sperrgut beliefert. Die Schreddersteuerung hat in der Regel weniger Schnittstellen zu Fremdsystemen, da üblicherweise der Kranführer entscheidet, welches Material vor dem Vermischen im Bunker noch geschreddert werden sollte. Ein Schredder ist normalerweise mit einem Brand-Früherkennungssystem ausgerüstet, da durch das Schreddern Funken entstehen können und sich das Material entzünden kann.

4.5.5 Verbrennung

Der Prozess Verbrennung ist der Zentrale Prozess, um die Kernaufgabe der Abfallentsorgung zu erfüllen. Unter Zugabe von Luft als Oxidationsmittel, wird eine Redoxreaktion ausgelöst, bei der Energie in Form von Wärme und Licht entsteht. Ein Feuer-Leistungsregler (FLR), steuert exakt die Brennstoffzufuhr und das Verbrennungsluftsystem, teils mit- oder ohne Rauchgasrezirkulation, um mit möglichst wenig Luftüberschuss Emissionskonform die geforderte thermische Leistung zu erbringen. Je nach Ausführung, kann eine Kompromittierung der FLR einen Totalschaden am Kessel verursachen. Der FLR ist dabei in der Ebene 1 – Siehe Kap. 7.1 Netzwerkzonierung – unterzubringen.

4.5.6 Schlackeaustrag

Der Schlackeaustrag ist stofflich gesehen dem Prozess Verbrennung direkt nachgelagert. Asche und unbrennbare Verbrennungsrückstände müssen abgekühlt und bis zum Weitertransport auf eine Deponie, in ein Zwischenlager (Schlackenbunker) befördert werden. Ist die Beförderung zum Schlackenbunker nicht mehr möglich, muss die Verbrennung gestoppt werden.

4.5.7 Entstaubung

Die im Feuerraum entstehenden leichten Ascherückstände, welche mit der Verbrennungsluft durch den Kessel mitgerissen werden, nennt man Flugasche. Diese muss elektrostatisch oder mechanisch entfernt werden, damit die nachgelagerten Systeme im Rauchgasweg (Katalysator, Wäscher etc.) ihre Funktion weiter erfüllen können. Fällt die Entstaubung aus, bedeutet dies meist die Abschaltung der Verbrennung und damit der Stillstand der Anlage.

4.5.8 Entstickung

Wird durch Verfahren entstickt, welche nach der eigentlichen Verbrennung angewendet werden, Spricht man von Sekundären Massnahmen. Diese reduzieren zu einem Grossteil für Mensch und Umwelt schädliche Stickoxide aus dem Rauchgas. Bei Ausfall der Entstickungsanlage, droht der temporäre Entzug der Betriebsbewilligung.

4.5.9 Rauchgasreinigung

Die Rauchgasreinigung ist in der Regel der letzte aktive Prozess, bevor das Rauchgas in die Atmosphäre entlassen wird. Dabei werden noch enthaltene Schadstoffe entfernt mit dem Zweck, Umweltauflagen zu erfüllen. Bei Ausfall der Rauchgasreinigung droht der temporäre Entzug der Betriebsbewilligung.

4.5.10 Emissionsmessung

Nach der Rauchgasreinigung, also bevor das Rauchgas in die Atmosphäre entlassen wird, muss das Rauchgas auf Schadstoffe gemessen werden. Damit wird auch letztinstanzlich die korrekte Funktion der vorgelagerten Prozesse kontrolliert. Werden Anomalien festgestellt, hat das direkten Einfluss auf den FLR. Dabei wird entweder automatisch oder manuell in die Regelung eingegriffen. Ein Ausfall der Messungen oder Manipulation der Emissionswerte, kann den temporären Entzug der Betriebsbewilligung zur Folge haben.

4.5.11 Abwasserreinigung

Je nach Ausführung der Gesamtanlage, können bei den vorgelagerten Prozessen, grössere Mengen kontaminierten Abwassers entstehen. Fallen solche Abwässer an, müssen diese vor der Einleitung in öffentliche Gewässer, entsprechend gereinigt werden. Dabei kann die Reinigung entweder Inhouse oder durch Dritte in Auftrag erfolgen. Bei Ausfall der Abwasserreinigung droht der temporäre Entzug der Betriebsbewilligung.

4.5.12 Energieproduktion

Als Nebenprodukt der Verbrennung, fällt Energie in Form von Wärme und Licht an. Durch die Wärme wird in separaten Kreisläufen Dampf, Strom und Fernwärme erzeugt. Kann die Energie nicht mehr abgeführt werden, hat das einen Verbrennungsstopp zur Folge. Aus diesem Grund ist der Sicherstellung der Energieabführung grossen Stellenwert beizumessen.

4.6 IT-Büroinformatik

Aufgrund der unterschiedlichen Schutzbedarfsanforderungen sollten OT und Büroinformatik strikt getrennt werden. Die Trennung erfolgt über die Netzwerksegmentierung. «Best Practice» ist, die Büroinformatik in den oberen Ebenen (Ebene 5/6) des Netzwerkzonenmodells anzusiedeln und durch eine Demilitarisierte Zone (DMZ) von der OT abzutrennen (Siehe Kapitel 7.1). Direkte Zugriffe ohne Protokollbruch aus den Zonen der Büro IT auf Systeme der OT sind zu vermeiden. Derartige Zugriffe sind mindesten über einen Jump Host in der ICS-DMZ, idealerweise aber über ein Privileged Access Management System (PAM) zu terminieren. Die Vorteile eines Zugriffs über ein PAM System sind u. a. die lückenlose Protokollierung der Zugriffe, sowie die sichere Verwaltung von hoch privilegierten Anmeldeinformationen.

5 Abhängigkeit, Kritikalität und Maturität

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

Die Kriterien zur Einstufung beziehen sich im sehr engen Sinn nur auf die Abhängigkeit des einzelnen Prozesses von der OT/IT und berücksichtigt mögliche Alternativen.

- Autonom = keine Abhängigkeit von steuerbaren OT/IT-Systemen
- Tief = ein Ausfall kann ohne OT/IT auch manuell bewältigt werden
- Mittel = ein Ausfall hat direkte Auswirkungen auf den Betrieb, der nur noch eingeschränkt möglich ist, Alternativen sind teilweise verfügbar
- Hoch = ein Ausfall verunmöglicht den Betrieb, es ist keine Alternative verfügbar

Dieser Vorschlag ist aufgrund der in den Unternehmen konkret durchgeführten Business Impact Analysen (BIA, siehe Beschreibung im Anhang dieses Dokumentes) und Schnittstellenanalysen individuell anpassbar. Das Maturitätslevel sollte das Level 2 allerdings sinnvollerweise nicht unterschreiten (Minimalanforderung bezüglich Informationssicherheit, siehe unten stehende Abbildung).

Die Kritikalität des Unterprozesses in der unteren Tabelle 3, soll ungeachtet der Anlagengrösse Auskunft über die Auswirkung auf die Durchführbarkeit des «Kernprozesses Abfall Entsorgen (KPE)» geben. Wenn z. B. der Müllkran ausfällt, ist in den meisten Fällen auch keine Verbrennung und damit Entsorgung mehr möglich, somit bedeutet das einen Totalausfall des KPE. Fällt z. B. die Rauchgasreinigung aus, hat dies dramatische Folgen für die Umwelt. KPE wird je nach Anlage behindert oder falls ein Bypass vorhanden ist, kann die Anlage weiter betrieben werden. Dem KPE nachgelagerte Prozesse wie thermische- oder elektrische Versorgung Dritter, ungeachtet, ob sie zur kritischen Infrastruktur gehören, finden in dieser Tabelle KEINE Berücksichtigung!

4 = Totalausfall des «Kernprozesses Abfall Entsorgen (KPE)»
3 = nur leichte Beeinflussung des KPE, starke Beeinflussung der Umsysteme
2 = keine direkte Beeinflussung des KPE, Funktion der Umsysteme mit anderen Mitteln provisorisch ersetzbar
1 = keine direkte Beeinflussung des KPE aber langfristige anderweitige Folgen

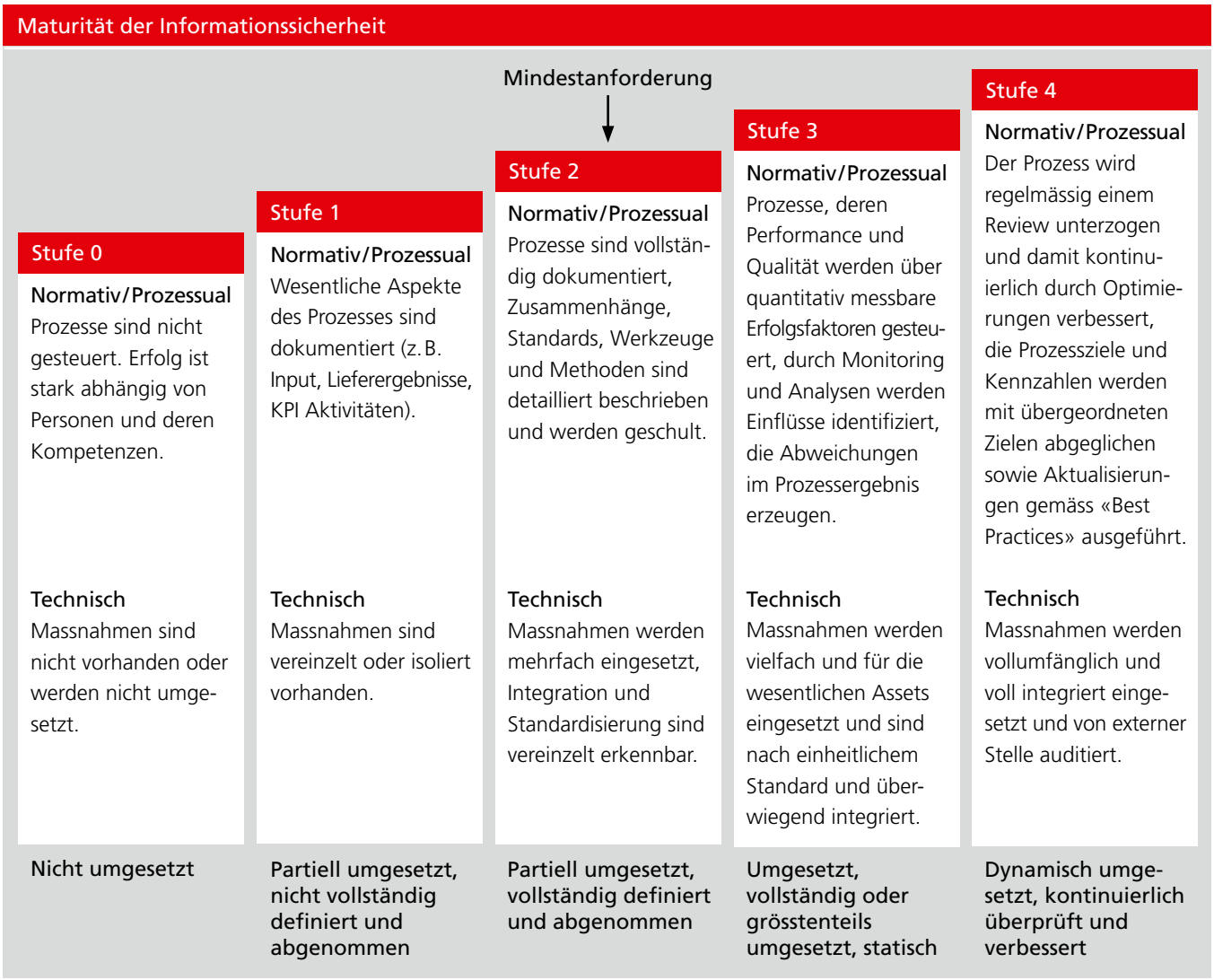

Abbildung 8: Maturität der Informationssicherheit

Die empfohlene Maturität für Kehrichtverbrennungsanlagen richtet sich nach der nachfolgenden Tabelle 3:

n/a = Prozess nicht vorhanden
0 = Nicht umgesetzt
1 = Partiell umgesetzt, nicht vollständig definiert und abgenommen
2 = Partiell umgesetzt, vollständig definiert und abgenommen
3 = Umgesetzt, vollständig oder grösstenteils umgesetzt, statisch (keine kontinuierliche Prozessverbesserung)
4 = Dynamisch, umgesetzt, kontinuierlich überprüft, verbessert

Bemerkungen zu n/a:
Grundsätzlich sollen Bewertungen von 0–4 gemacht werden. n/a darf nur angewendet werden, wenn der Prozess im Unternehmen nicht existiert.

5.1 Empfohlene minimale Maturität

Der folgenden Tabelle können die empfohlenen minimalen Maturitäten für jeden einzelnen kritischen Prozess der Kehrichtverbrennung entnommen werden.

Die Empfehlung basiert auf der Risikoeinschätzung bezüglich Erfüllung des Kernauftrags bei Prozessausfall sowie der Abhängigkeit des Prozesses von IT-Unterstützung.

Kritische Prozesse in den Kehrichtverbrennungsanlagen			
	Grad der IKT Abhängigkeit	Risiko für Auftragserfüllung	Empfohlene Maturität der Informations-sicherheit
Nachrichtenkommunikation	Mittel	Mittel	2–3
Faktor Mensch	Hoch	Hoch	2–3
Fernzugriff externe Dienstleister	Hoch	Mittel	4
Betriebsdatenauswertung	Hoch	Tief	2–3
Updates Betriebssysteme und Software	Mittel	Tief	2–3
Entwicklung	Hoch	Tief	2–3
Datensicherung OT	Hoch	Tief	3–4
Halbautomatische Verteilung Virendefinitionen	Mittel	Tief	2–3
Waage	Mittel	Mittel	2–3
Abwurfsteuerung	Mittel	Tief	2–3
Kran	Hoch	Hoch	4
Verbrennung und Kessel	Hoch	Hoch	4
Entstaubung	Autonom	Mittel bis Hoch	3
Entstickung	Mittel	Mittel	3
Rauchgasreinigung	Hoch	Mittel bis Hoch	4
Emissionsmessung	Hoch	Mittel	3–4
Schredder	Mittel	Tief	2
Schlackenaustrag	Hoch	Hoch	3–4
Abwasserreinigung	Hoch	Mittel	3–4
Betriebsmittel	Mittel	Mittel bis Hoch	3
Radioaktivitätsmessung	Tief	Tief	2–3
Schlacke (Abtransport)	Tief	Tief	2–3
Turbine	Mittel	Tief	3
Flugasche	Mittel	Mittel bis Hoch	2–3
Fernwärme, Strom, Dampf	Mittel	Hoch	3–4
Druckluft	Tief	Hoch	3–4
Rohwassergewinnung	Mittel	Hoch	3–4
Wasseraufbereitung	Hoch	Hoch	4
Zutritt und Autorisierung	Mittel	Tief	3–4
Sicherheitsüberwachung	Tief	Tief	2–3
Netzwerkkomponente OT-IT	Tief	Tief	2–3
Fakturierung, Anlieferung	Hoch	Tief	2–3
Betriebsdatenauswertung	Hoch	Tief	2–3
Energieverkauf	Mittel	Tief	2–3
Datensicherung IT	Hoch	Tief	3–4
Compliance und Berichtwesen	Hoch	Tief	2–3
Schichtbuch	Tief	Tief	2–3
Alarmierung (Blaulicht, Behörden, Personal)	Mittel	Tief	2

Tabelle 3: Kritische Prozesse in den Kehrichtverbrennungsanlagen

Die Abbildung 9 veranschaulicht die starke Abhängigkeit der Hauptprozesse Infrastruktur, Entsorgung und Unternehmensführung von den als kritisch definierten Systemen bzw. Unterprozessen. Wir wollen damit aufzeigen, dass sich der Ausfall eines Unterprozesses meistens nicht nur auf einen Hauptprozess, sondern gleich auf mehrere auswirkt.

Die Systemabhängigkeit zeigt die Auswirkung der Unterprozesse auf die Hauptprozesse in der Tabelle auf Seite 23:

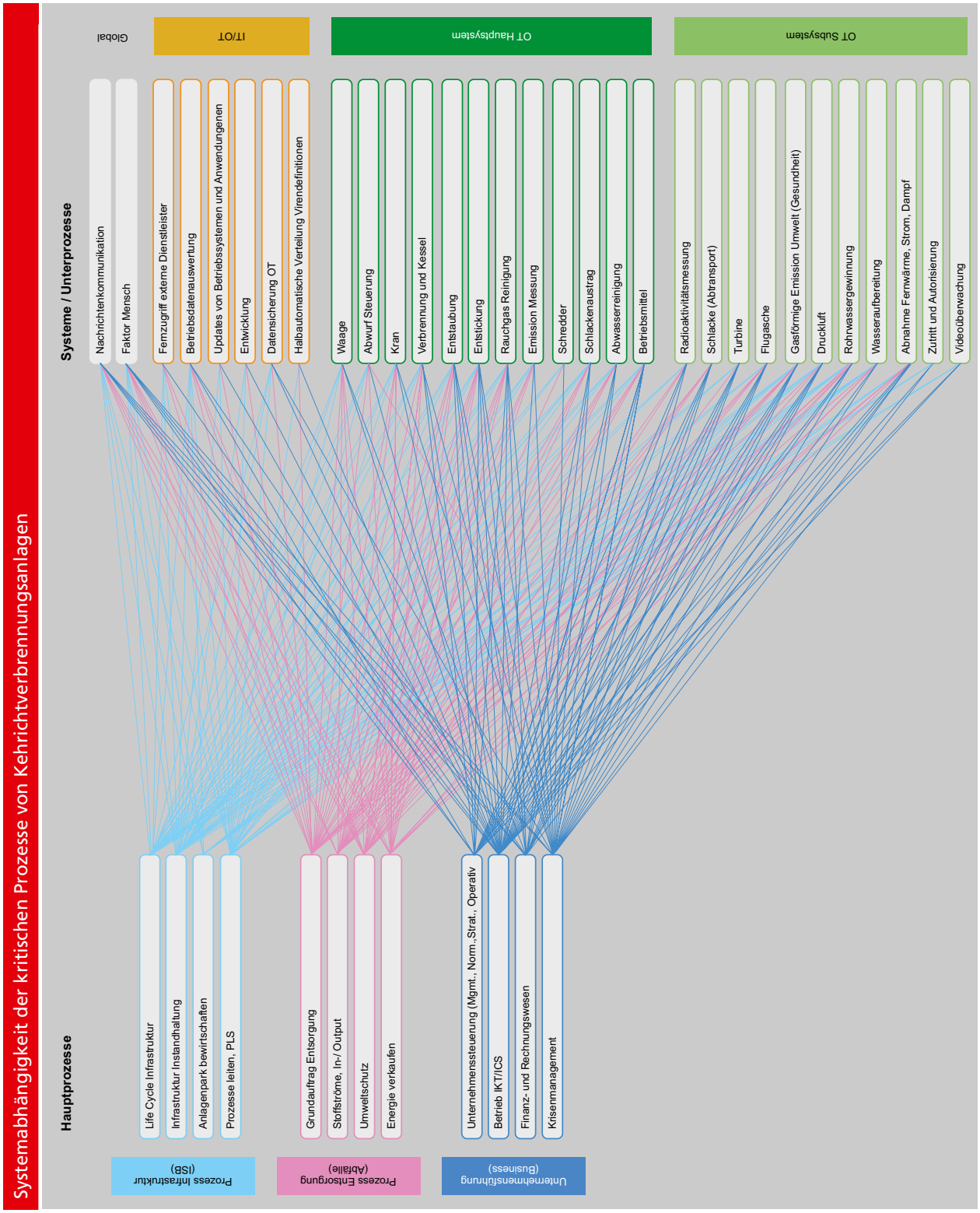

Abbildung 9: Systemabhängigkeit der kritischen Prozesse von Kehrichtverbrennungsanlagen

IT/OT-Systemabhängigkeit der kritischen Prozesse von Kehrichtverbrennungsanlagen															
Rubrik	Systeme/Unterprozesse	Hauptprozesse													
		Prozess Infrastruktur (ISB)				Prozess Entsorgung (Abfälle)				Unternehmens-führung (Business)					
		Life Cycle Intrastruktur	Infrastruktur Instand halten	Anlagenpark bewirtschaften	Prozesse leiten, PLS	Grundauftrag Entsorgung	Stoffströme In-/Output	Umweltschutz	Energie liefern	Unternehmenssteuerung (Mgmt., Norm., Strat., Operativ)	Betrieb IKT/ICS	Finanz- und Rechnungswesen	Krisenmanagement		
Global	Nachrichtenkommunikation	x	x	x	x	x	x	x	x	x	x	x	x		
	Faktor Mensch	x	x	x	x	x	x	x	x	x	x	x	x		
IT-Betrieb	Fernwartung externe Dienstleister	x	x		x	x		x			x				
	Betriebsdaten	x	x	x	x	x	x	x	x	x		x			
	Updates von Betriebssystemen und Anwendungen		x		x	x					x				
	Entwicklung		x		x	x					x				
	Datensicherung OT	x	x		x	x					x		x		
	Halbautomatischer Versand Virendefinitionen				x	x					x				
OT-Hauptsystem	Waage/Eingangskontrolle	x	x		x	x	x	x			x	x			
	Abwurf Steuerung	x	x		x	x	x		x		x				
	Kran	x	x		x	x	x		x		x		x		
	Verbrennung, inklusive Kessel	x	x		x	x		x	x	x	x		x		
	Entstaubung	x	x		x	x	x	x	x	x	x	x	x		
	Entstickung	x	x		x	x	x	x	x	x	x	x	x		
	Rauchgas-Reinigung	x	x		x	x	x	x	x	x	x	x	x		
	Emission Messung	x	x		x	x	x	x			x		x		
	Schredder	x	x				x						x		
	Schlackenaustrag	x	x		x	x	x	x		x	x	x	x		
	Abwasserreinigung	x	x		x	x	x	x		x	x	x	x		
	Betriebsmittel	x	x		x	x	x	x		x	x	x	x		
OT-Subsystem	Radioaktivitätsmessung	x	x		x		x	x		x	x		x		
	Schlacke (Abtransport)					x	x	x		x	x	x	x		
	Turbine	x	x		x			x		x	x	x	x		
	Flugasche	x	x		x	x	x	x		x	x	x	x		
	Gasförmige Emission, Umwelt, Gesundheit	x	x	x	x	x	x	x		x	x	x	x		
	Abnahme Fernwärme, Strom, Dampf			x	x	x	x		x	x	x	x	x		
	Druckluft	x	x	x	x	x			x		x		x		
	Rohwassergewinnung	x	x	x	x	x	x	x	x	x	x		x		
	Wasseraufbereitung	x	x	x	x	x			x		x		x		
	Zutritt und Autorisierung	x	x							x	x		x		
	Videoüberwachung	x	x							x	x				

Tabelle 4: IT/OT-Systemabhängigkeit der kritischen Prozesse von Kehrichtverbrennungsanlage

In der folgenden Tabelle werden die Angriffsmöglichkeiten der Prozesse und deren Auswirkungen beschrieben:

Prozess	Angriffsmöglichkeit	Auswirkung
Waage	Blockierung	Stillstand des Betriebs, weil keine Annahme mehr erfolgen kann. Ist für einen Notbetrieb eine manuelle Erfassung von Typ, Kunde, Gewicht möglich?
Abwurfsteuerung	Blockierung	Stillstand des Betriebs, weil keine Annahme mehr erfolgen kann.
Schredder	Blockierung	Minderung der Effizienz, ein Teil des Abfalls (Sperrgut) kann nicht mehr verwertet werden.
Kran	Blockierung oder Manipulierung	Stillstand des Betriebs, weil die Ofenlinie nicht mehr beschickt werden kann.
Verbrennung und Kessel	Manipulation Feuer-Leistungs-regelung (FLR), Kesselwasser-versorgung	Stillstand des Betriebs, weil keine Verbrennung mehr möglich, schlechter Ausbrand, dadurch keine Deponierung mehr möglich. Drohender Totalschaden des Kessels durch Überhitzung der Mauerung, Kesselrohre und Rost.
Schlackenaustrag	Störung von Ausbringen und Aufbereitung	Stillstand des Betriebs, wenn keine Schlackenausbringung mehr möglich oder durch Austrag von unverbranntem Material.
Staubabscheidung	Blockierung	Emittieren von Staub resp. Flugasche, dadurch Totalausfall des nachgeschalteten Katalysators.
Entstickung	Blockierung Ammoniakeindüsung oder Temperaturregulierung Kat (Brenner/Dampf)	Nichteinhalten der Luftreinhalte Verordnung (LRV), dadurch Abschalten der Anlage. Totalausfall der Anlage, wenn Katalysator durch Manipulation vorangeschalteter Prozesse unbrauchbar wird. Umfahrung des Katalysators nur für kurze Zeit erlaubt.
Rauchgasreinigung	Manipulation oder Blockierung des RG-Wäschers	Zerstörung des Rauchgaswäschers durch Überhitzung, dadurch Abschaltung der Verbrennungslinie.
Betriebsmittelversor-gung (Druckluft, Kühl-wasser, Chemikalien)	Manipulation oder Blockierung diverser prozessrelevanter Unter-systeme	Regelventile gehen ohne Druckluft in Sicherheitspositionen, etc. Abschaltung der Verbrennungslinien.

Tabelle 5: Prozesse – Angriffsmöglichkeiten – Auswirkungen

In der folgenden Tabelle werden die Angriffsmöglichkeiten der Produkte/Outputs und deren Auswirkungen beschrieben:

Produkte und Outputs	Angriffsmöglichkeit	Auswirkung
Asche, Schlacke, Filterkuchen	Störung des Prozesses der Entsorgung	Unerwünschte Lagerbildung auf dem Areal, Lieferverträge mit Deponien können nicht eingehalten werden (z. B. Deponie oder Untertags-Deponie [UTD] für Flugaschen).
Abwasser	Prozess stören	Gewässerverschmutzung, Abschaltung aller vorgelagerten Prozesse und dadurch Abschaltung der gesamten Anlage. Verlust der Betriebsbewilligung.
Strom und Wärme	• Manipulation Wärmeauskopplung • Manipulation der Turbine	• Destabilisierung des Fernwärmenetzes. • Gefährdung von kritischer Infrastruktur wie Spitäler oder Regierungsgebäude. • Mechanische Zerstörung durch Überdrehzahl, dadurch Totalausfall des Standortes.
Gasförmige Emissionen	Keine oder falsche Messung	Drohender Verlust der Betriebsbewilligung, Reputationsschaden. Haftung im Fall von unerwünschten, gesundheitsschädigenden Emissionen.

Tabelle 6: Produkte Outputs Angriffsmöglichkeiten und Auswirkungen

Bei den meisten Prozessen ist eine Blockierung oder eine Manipulation die grösste Gefahr. Alle Vorfälle haben Betriebsausfälle und damit hohe bis sehr hohe Kosten zur Folge.

6 Informationsschutz

6.1 Informationsschutz

Der Informationsschutz zielt auf den angemessenen Schutz von Informationen und der IKT-Infrastruktur in Bezug auf die festgelegten Schutzziele, wie Vertraulichkeit, Integrität und Verfügbarkeit ab. Ein unbefugter Zugriff auf Systeme oder die Manipulation von Daten soll verhindert und entstehende Risiken so weit als möglich gesenkt werden, um daraus resultierende wirtschaftliche Schäden zu verhindern.

Bei den Daten ist es unerheblich, ob diese einen Personenbezug haben oder nicht. Informationen können sowohl auf Papier als auch in IKT-Systemen vorliegen.

Im Arbeitsalltag werden oft die Begriffe «Informationsschutz», «Datenschutz» und «IT-Sicherheit» verwechselt oder in einem falschen Kontext benützt.

Wie in der unterstehenden Grafik ersichtlich, sind der Datenschutz und die IT-Sicherheit Teil des Informationsschutzes welcher wiederum ein wichtiger Bestandteil des Unternehmensrisikos-Managements und des Business Continuity Managements (BCM) ist.

6.2 Informationsschutzstrategie

Eine erfolgreiche Informationsschutzstrategie schützt die Mittel einer Organisation, die zur Ausführung der (kritischen) Geschäftsprozesse notwendig sind. Dabei gibt es keine allgemein gültige Definition von Anforderungen oder Lösungen.

Um die Sicherheitsrisiken im Bereich der kritischen Informations- und Kommunikationssysteme ganzheitlich identifizieren und behandeln zu können ist eine mehrschichtige Informationsschutzstrategie, welche dem «Defense-in-Depth[1]»-Ansatz folgt, unerlässlich.

Diese Strategie sollte neben **technischen Massnahmen** auch die dazu benötigten **Prozesse, Ausbildung und Schulung** der Mitarbeitenden, sowie die benötigte **Security-Governance** umfassen, um Informationssicherheit nachhaltig und erfolgreich umzusetzen und betreiben zu können.

[1] *Siehe Kapitel 3 Ziele des Minimalstandards*

Abbildung 10: Unternehmenssicherheit

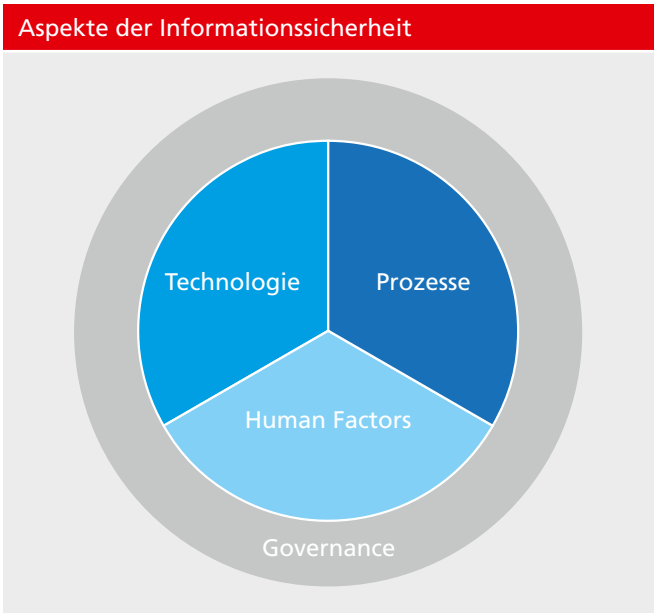

Abbildung 11: Aspekte der Informationssicherheit

Defense-in-Depth-Strategien sind individuell und müssen sich an den Bedürfnissen, Möglichkeiten und Risiken der Organisation orientieren. Die risikobasierte Vorgehensweise berücksichtigt dabei neben den eigenen auch die Abhängigkeiten von externen Prozessen oder Ressourcen.

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

WICHTIG: Informationssicherheit ist kein einmaliges Projekt, sondern ein fortlaufender Qualitäts-Sicherungs-Prozess, welcher dem Plan-Do-Check-Act-Zyklus (PDCA Zyklus) folgt!

6.3 Mögliche Massnahmen zur Stärkung des Informationsschutzes

Daten	Massnahme
E-Mail	Keine klassifizierten Informationen per Mail versenden; keine Passwörter via Mail versenden.
Klassifizierung von Daten	Korrekte Klassifizierung der Datenbestände.
Zugriffsrechte auf Daten	Berechtigungsmanagement richtig umsetzen.
Speicherort der Daten	Klassifizierte Daten nur auf gesicherten Datenträgern.
Datenaustausch mit Lieferanten	Sichere Datenaustauschplattform, nur relevante Daten austauschen.
Backup	Regelmässige Kontrolle der gesicherten Daten, Datenträger mit Daten ausser Haus oder Offline.
Daten in der Cloud	Wichtige Daten auch offline verfügbar machen, falls Verbindung zu Cloud nicht möglich ist.
Notfallpläne	Sollten ausgedruckt verfügbar sein.
Daten in sozialen Medien	Nur publizieren, was nötig ist, damit keine Rückschlüsse gezogen werden können.
Passwörter	Komplexität, in Passwort-Richtlinie zusammengefasst. Best Practice ist MFA. Referenz auf Nationales Zentrum für Cybersicherheit (NCSC): Schützen Sie Ihre Konten/Passwörter (admin.ch).

Tabelle 7: Umsetzungsmassnahmen Informationssicherheit (nicht abschliessend)

6.4 Datenschutz

Datenschutz beschreibt den Schutz von Personendaten[2] und besonders schützenswerten Personendaten[3] sowie den Schutz des Rechts auf informationelle Selbstbestimmung. Er umfasst organisatorische sowie technischen Massnahmen gegen missbräuchliche Verarbeitung und Verwendung von personenbezogenen Daten.

Der Datenschutz in der Schweiz richtetet sich grundsätzlich nach dem Bundesgesetz über den Datenschutz (DSG) sowie der Verordnung zum Bundesgesetz über den Datenschutz (VDSG). Sobald jedoch ebenfalls Daten von Bürgern (Kunden, Mitarbeiter) aus dem europäischen Raum verarbeitet werden, kann es sein, dass die Vorgaben der Europäischen Union (EU)-Datenschutz-Grundverordnung (EU-DSGVO) auch in der Schweiz mitberücksichtigt werden müssen.

Die Bedeutung des Datenschutzes hat seit Beginn der Digitalisierung stetig zugenommen, da die Datenhaltung, Datenverarbeitung, Datenerfassung, Datenweitergabe und Datenanalyse immer umfangreicher und einfacher werden. Digitale Innovationen wie Internet, E-Mail, Mobiltelefonie, Videoüberwachung sowie elektronische Zahlungsmethoden schaffen immer mehr und neue Möglichkeiten zur Erfassung von Personendaten.

Beim Speichern und Verarbeiten von personenbezogenen Daten gelten unter anderem die folgenden Grundsätze:

- Personendaten dürfen nur rechtmässig bearbeitet werden.
- Ihre Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.

Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.

6.5 IT-Sicherheit

Die IT-Sicherheit als Teilbereich des Informationsschutzes dient dem Schutz elektronisch gespeicherter Informationen (Daten), deren Verarbeitung sowie den Schutzzielen Vertraulichkeit, Verfügbarkeit und Integrität. Ebenfalls eingeschlossen ist das fehler- und unterbruchsfreie Funktionieren und die Zuverlässigkeit der IKT-Systeme.

Hierbei müssen auch Systeme einbezogen werden, die häufig nicht unmittelbar als IKT-Systeme identifiziert werden, wie z. B. Telefonanlagen, Steuerungs- (ICS) oder IoT-Systeme.

Beim Einsatz von Cloud Systemen weitet sich das Handlungsfeld der klassischen IT-Sicherheit über den Unternehmensperimeter in den Cyberraum hinaus.

Die Begehrlichkeit, Betriebsdaten von Geräten und Systemen zu erheben und auszuwerten, hat bei den Systemlieferanten stark zugenommen. Einerseits, um ihre Produkte zu verbessern, anderseits, um deren Nutzung und Einsatz zu verfolgen. Die bewusste Herausgabe von solchen Daten sollten im Vorfeld kritisch hinterfragt, eindeutig geklärt und vertraglich geregelt werden. Es sollte ebenfalls festgelegt werden, über welche sicheren Verbindungen und in welchen Intervallen (realtime, täglich, wöchentlich etc.) die Daten an die Lieferanten übermittelt werden.

[2] Def. gem. DSG Art.3 Abs.a
[3] Def. gem. DSG Art.3 Abs.c

6.6 Mitarbeiter Awareness

Erkenntnisse der letzten Jahre haben gezeigt, dass Sicherheits-Technologie allein nicht mehr ausreicht, um die immer raffinierteren Angriffe und steigenden Bedrohungen aus dem Cyberraum abzuwehren.

Aus diesem Grund sollten alle Mitarbeiter regelmässig hinsichtlich Informationssicherheit geschult, und dadurch Ihr Sicherheitsbewusstsein gestärkt werden.

Durch die stufengerechte Ausbildung der Mitarbeiter, wird das Risiko von unbewusstem Fehlverhalten deutlich vermindert.

Ziele der Schulung sind:

- Mitarbeitende zu sicherheitsbewusstem Verhalten motivieren.
- Vermitteln des richtigen Umgangs mit Risiken und Vorfällen.
- Fördern und stärken der Akzeptanz zum Thema Informationssicherheit.
- Mitarbeiter befähigen, Sicherheitsmassnahmen aktiv zu unterstützen und zu verstehen.

Ein Sensibilisierungsprogramm hat zum Ziel, dem Mitarbeiter eine unbewusste Kompetenz betreffend Informationssicherheit zu vermitteln. Das bedeutet, die Mitarbeiter verhalten sich in heiklen und schwierigen Situationen richtig, ohne überlegen zu müssen, was richtig ist. Um dieses Ziel zu erreichen, ist ein fortwährendes Awareness Programm unerlässlich.

6.7 Governance

Die Governance bezeichnet sämtliche Grundsätze und Regeln, mit deren Hilfe die Strukturen und das Verhalten durch die obersten Führungskräfte gesteuert und überwacht werden können.

Die Governance legt die Grundsteine für eine erfolgreiche und nachhaltige Umsetzung der Informationssicherheits-Strategie. In diesem Bereich werden die Voraussetzungen geschaffen, dass Bedrohungen gegen die Informationssicherheit im Unternehmen erkannt, bewertet und behandelt werden. Die Governance liefert dabei eine übergeordnete Struktur, um die Geschäftsziele bezüglich Informationssicherheit auf strategischer, funktionaler und operativer Ebene zu unterstützen. Bevor die Informationssicherheit operativ umgesetzt werden kann, muss ein Unternehmen seine IKT-Grundsätze festlegen. Dazu gehört insbesondere die Beantwortung der folgenden Fragen:

- Was wird getan?
- Wie wird es getan?
- Wer ist dafür verantwortlich?
- Wie wird es gemessen?

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

7 Fokusthemen

7.1 Netzwerkzonierung

7.1.1 Physische Trennung

Die physische Trennung von Netzwerksegmenten ist die zuverlässigste Variante, um Netzwerkverkehr zwischen verschiedenen Netzen zu kontrollieren und abzugrenzen. Die physische Trennung erfordert hohen Bedarf an Geräten wie Switches, Router und Security Gateways und ist daher mit hohen Kosten verbunden. Es wird deshalb empfohlen, eine physische Trennung von Netzwerksegmenten vor allem an besonders sensiblen Punkten des Netzwerks umzusetzen. Kritischen Punkte im Netzwerk können sein:

- Verbindungen zwischen Standorten
- Verbindungen zwischen sensitiven Netzzonen wie z. B. dem Leitsystem und der IT-Büroinformatik innerhalb eines Standortes
- Die Perimeter – Übergänge zwischen dem Unternehmensnetzwerk und externen Netzen (z. B. Internet)

7.1.2 Virtual Local Area Network (VLAN)

Für Anwendungsfälle, bei denen die physische Trennung von Netzwerksegmenten nach einer Risikobeurteilung als nicht zwingend notwendig erachtet wird, kann die Segmentierung durch VLANs auch logisch erfolgen. Hierbei ist das höhere Restrisiko gegenüber der physischen Trennung durch mögliche Fehlkonfigurationen oder Angriffsszenarien wie VLAN-Hopping zu beachten.

7.2 Netzwerksegmentierung nach dem «Purdue» Modell[4]

Das Purdue Reference Model wurde in den frühen 1990er Jahren von Theodore J. Williams an der US-amerikanischen Purdue Universität in Indiana, USA entwickelt. Es wurde ursprünglich für nichtindustrielle Unternehmensnetze entworfen, danach aber auch auf die Anwendung für Automationsnetze angepasst.

Das Purdue Reference Model gliedert ein Industrienetzwerk abstrakt in verschiedene Ebenen. So kann es auch als Ausgangslage für Massnahmen dienen, die nach dem «Defense-in-Depth»-Prinzip aufgebaut werden.

Auch das Prinzip, ein solches Netz in Zonen und Zonenübergänge zu unterteilen, findet sich im Purdue Reference Model wieder, wobei hier zwischen «Zone» und «Ebene» unterschieden werden muss. Eine Ebene stellt die hierarchische Einordnung in das gesamte Unternehmensnetz dar, wohingegen sich eine Zone um die spezifische Segmentierung nach den Sicherheitsanforderungen kümmert. Eine Zone kann sich unter Umständen auch über mehrere Level erstrecken.

7.2.1 Horizontale Netzwerksegmentierung

Dieses Modell schützt kritische und sensible Automatisierungsprozesse vor unberechtigten Zugriffen aus nicht vertrauenswürdigen Netzwerksegmenten. Das Zonenmodell fusst auf sieben Zonen, welche bestimmte Funktionen übernehmen und die nach Schutzbedarf eingeteilten Systeme aufnehmen. So werden kritische Endgeräte ausschliesslich in den Zonen 1 und 2 angeordnet und über geeignete Security Gateways von anderen Zonen separiert.

7.2.2 Vertikale Netzwerksegmentierung

Eine vertikale Zonierung segmentiert das Netzwerk z. B. nach Standorten oder Systemen. So können unterschiedliche Standorte mit differenziertem Schutzbedarf in derselben horizontalen Netzwerkebene betrieben werden. Hierfür notwendige Kommunikationswege und Schnittstellen werden über bereitgestellte Security Gateways realisiert. Die zonenübergreifende Kommunikation erfolgt über sichere, und klar definierte und dokumentierte Kommunikationswege.

Bei einem Sicherheitsvorfall kann der Schaden auf die jeweilige Zone und die darin befindlichen Systeme eingeschränkt werden. Die Systeme werden nach vordefinierten Kriterien klassifiziert, den horizontalen Zonen zugeordnet und innerhalb dieser gruppiert.

Kriterien für eine Gruppierung können sein: Kritikalität, Risiken, Technologien, organisatorische Verantwortungsbereiche und physikalische Gegebenheiten.

[4] *Quelle Beschreibung der Zonen und Modellbeschreibung: www.sichere-industrie.de*

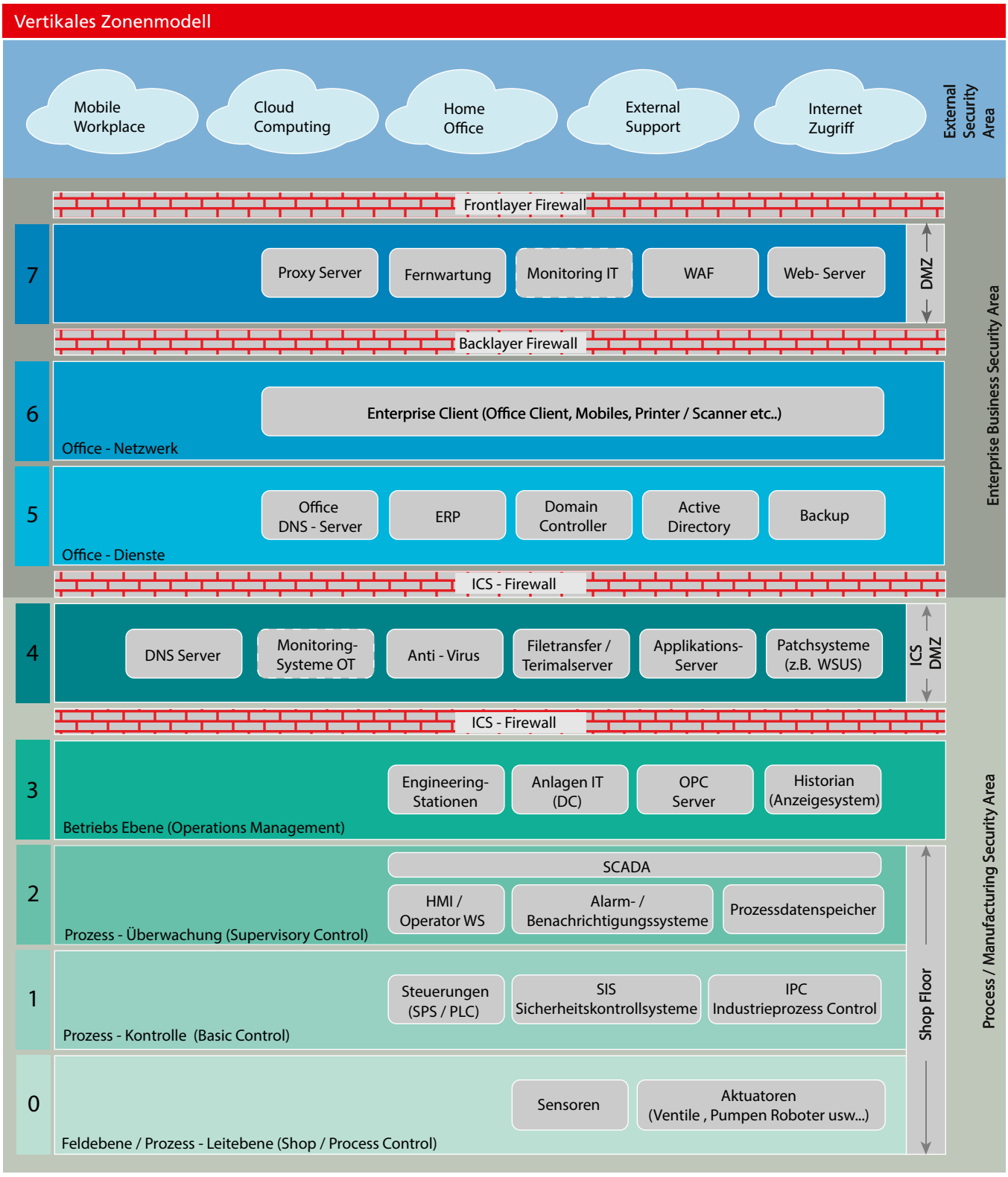

Abbildung 12: Vertikales Zonenmodell

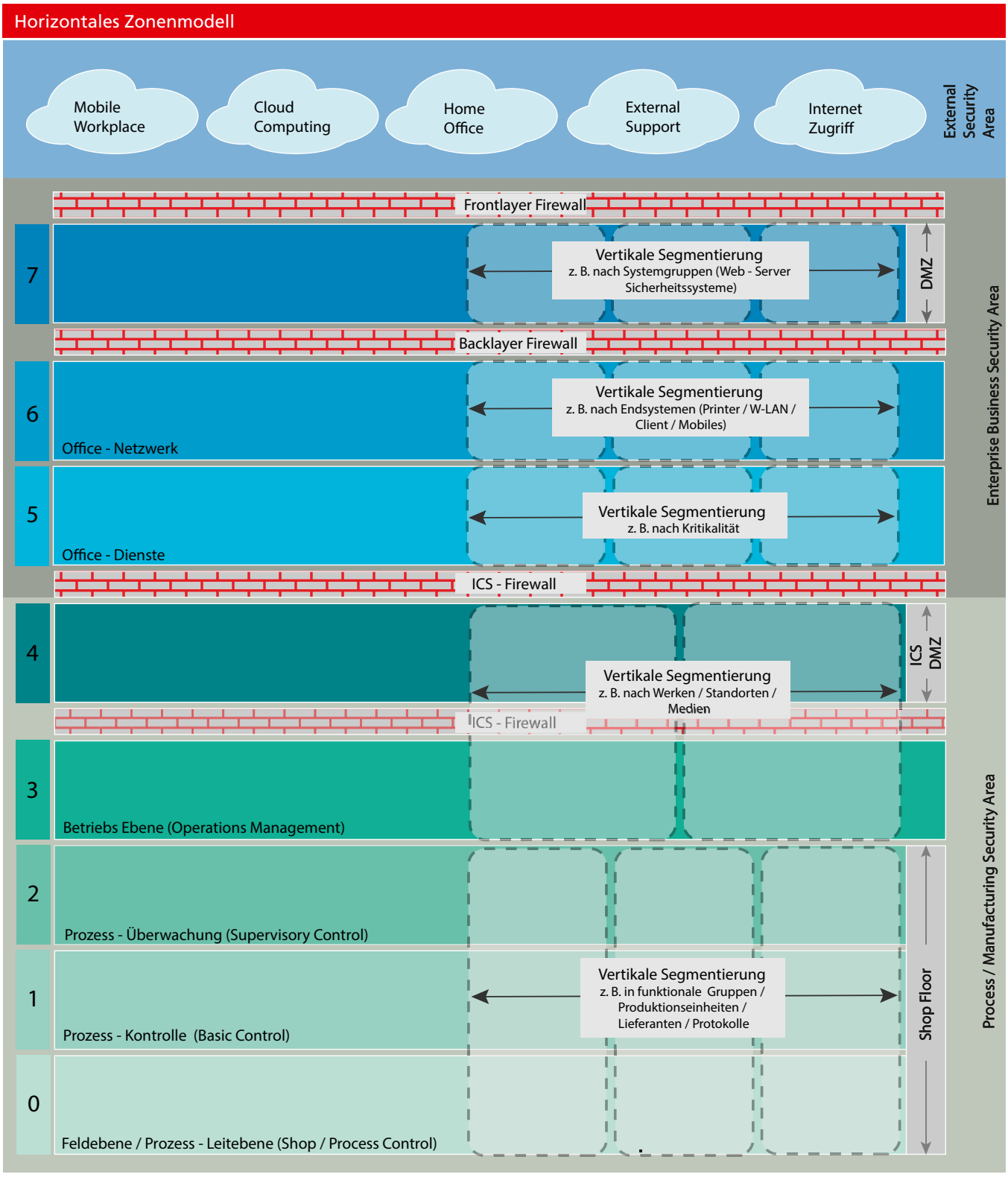

Abbildung 13: Horizontales Zonenmodell

Feldebene/Prozessleitebene (Ebene 0)

Im untersten Level läuft der eigentliche physikalische Geschäftsprozess ab. Die Befehle der auf Level 1 befindlichen Systeme werden hier in Echtzeit umgesetzt. Dieses Level wird auch als «Device»- oder Feldebene bezeichnet.
Typische Systeme sind: Motoren, Ventile, Pumpen, Remote I/O

Prozesskontrolle (Ebene 1)

In dieser Ebene befinden sich die Systeme, die unmittelbaren Einfluss auf die Ausführung und Steuerung des physischen Prozesses haben. Zu ihren Aufgaben gehört die Überwachung von Sensoren und die Aufrechterhaltung einer ordnungsgemäßen Funktion der Anlage. Sie arbeiten in Echtzeit, eine Störung auf diesem Level führt zu einer direkten Beeinträchtigung des automatisierten Prozesses.
Typische Systeme sind: SPS / PLC, SCADA, DCS, RTUs

Prozess Überwachung (Ebene 2)

Innerhalb von Ebene 2 befinden sich Systeme, die für die Überwachung und Steuerung der spezifischen Prozessführung verantwortlich sind. Die Datenverarbeitung erfolgt hier noch nicht in Echtzeit, eine Störung der ansässigen Systeme hat keinen unmittelbaren Einfluss auf die Verfügbarkeit der Automationslösung.
Typische Systeme sind: HMI, Alarm-/Benachrichtigungssysteme, Prozessdatenspeicher

Betriebsebene (Ebene 3)

Auf Ebene 3 sind Systeme angesiedelt, die in erster Linie die Funktion der Betriebsführung innehaben. Hierzu gehört zum einen das Bereitstellen jeglicher Systeme, Dienste und Anwendungen, die für das Industrienetz notwendig sind, zum anderen werden hier die einzelnen Automationsschritte geplant
Typische Systeme sind: Anlagen-IT (DNS, DHCP, Active Directory…), Engineering-Stationen, Manufacturing Execution System

ICS DMZ (Ebene 4)

Die DMZ ist ein «Zwischennetz», in das Verbindungen idealerweise aus Segmenten mit höherem Schutzbedarf eingebaut werden. Eine DMZ wird klassischerweise zwischen Office-Netz und Internet platziert, in die Systeme wie zum Beispiel Webserver, die aus dem Internet erreichbar sein müssen, gestellt werden. In unserem Kontext wird die demilitarisierte Zone zwischen Office- und Anlagenbereich betrieben, um darin beispielsweise geteilte Ressourcen zu platzieren.
Typische Systeme sind: Antivirus-Systeme, Fernwartungssysteme, Dateiaustausch-Server, Patchsysteme

Office Dienste/Office Netzwerk (Ebene 5 & 6)

Hier läuft der unterstützende (Geschäfts-)Betrieb eines Unternehmens ab. Dazu gehören beispielsweise Systeme, die in der Buchhaltung, im Vertrieb oder in der Personalabteilung genutzt werden. Zwischen Level 4 und Level 3 befindet sich die Schnittstelle zum Anlagennetz. Aus Sicht des Anlagennetzes gilt das Enterprise-Netz als hochgradig unsicher.
Typische Systeme sind: ERP-Systeme, Internetzugang, Fernwartungszugänge, Büroarbeitsplätze

DMZ (Ebene 7)

Diese Netzwerkebene stellt eine Art «Pufferzone» zur Integration zwischen Unternehmens-IT-Netzwerk und dem Internet oder anderen externen Netzwerken dar.

Datenverkehr zwischen den Zonen

Grundsätzlich sind alle Zonen untereinander isoliert und keine zonenübergreifende Kommunikation möglich. Wo dennoch Kommunikation stattfinden muss, ist Quelle, Ziel und der IP-Port zu definieren, zu dokumentieren und über einen Security Gateway zu öffnen. Diese Ausnahmen müssen periodisch überprüft werden.

Drahtlosnetzwerke

Drahtlosnetzwerke ermöglichen einen einfachen kabellosen Zugang zum Firmennetzwerk. Aus diesem Grund muss auf den Schutz der Drahtlosnetzwerke eine besondere Aufmerksamkeit gelegt werden.

Darüber hinaus bieten viele Systeme den Aufbau von Verbindungen mithilfe von Bluetooth, Infrarot oder Near Field Connection (NFC) an. Diese Verbindungen sind in der Regel schlecht geschützt und können als Angriffsvektoren genutzt werden.

Es wird daher empfohlen, gänzlich auf diese Verbindungsoptionen zu verzichten. Bei Systemen auf welchen Bluetooth, Infrarot und NFC nicht deaktiviert werden kann, müssen spezielle Schutzmassnahmen umgesetzt werden.

Massnahmenbeispiel:
Bluetooth kann, je nach Standort des Senders, über die Gebäudehülle hinaus strahlen und somit bis zu 100 m im öffentlichen Raum empfangbar sein. Mit geeigneten baulichen Massnahmen kann dies verhindert werden. Bluetooth sendet im 2,4 GHz-Band, somit beträgt die Wellenlänge ca. 12 cm. Ein geerdetes Metallgitter mit einer Maschenweite kleiner als 12 cm zwischen Sender und Gebäudehülle verhindert die Abstrahlung nach aussen effektiv.

7.2.3 Mobile Phones/Tablets[5]

Smartphones und Tablet-Computer werden heute zunehmend im Arbeitsumfeld eingesetzt und sind bereits vielfach zum wichtigsten Arbeitsgerät für Mitarbeiter geworden. Mittlerweile gibt es eine nicht mehr zu überschauende Anzahl an Geräten mit unterschiedlichen Betriebssystemen. Smartphones und Tablet-Computer mit iOS oder Android sind mit modernen, einfachen Bedienkonzepten eher auf den Consumer-Markt ausgerichtet und weniger für den geschäftlichen Einsatz mit hohem Schutzbedarf.

Damit unterscheiden sie sich grundlegend von anderen Konzepten mobiler Endgeräte, die speziell für den Unternehmenseinsatz konzipiert wurden. Trotzdem finden Geräte mit iOS und Android zunehmend in der Geschäftswelt Verwendung und verdrängen etablierte Lösungen wie Laptops.

Je nach Schutzbedarf ist abzuwägen, wie die mobilen Endgeräte eingesetzt und verwaltet werden. Für einen niedrigen bis normalen Schutzbedarf reicht der Einsatz der nativen Programme. Für einen erhöhten bis hohen Schutzbedarf sollte eine MDM-Lösung (Mobile Device Management), eventuell in Verbindung mit einem Device Enrollment Program (DEP) eingesetzt werden. Bei hohem Schutzbedarf wird der Einsatz eines Secure Containers empfohlen, weil nur damit eine Wechselwirkung zwischen privater und beruflicher Verwendung des mobilen Endgerätes weitestgehend vermieden werden kann und Unternehmensdaten sicher gespeichert werden können.

Bevor mobile Endgeräte in eine Unternehmensstruktur eingebunden werden können, ist es empfehlenswert klare Regeln für die Integration festzulegen. Mit diesen Sicherheitsrichtlinien werden u. a. die Rahmenbedingungen bezüglich Auswahl der Geräte, Auswahl der Daten, die auf den Geräten verarbeitet werden dürfen, Einschränkungen der Benutzer und Limitierung der Möglichkeiten der Geräte (Hardware wie Software) festgelegt.

Selbst bei der Verwendung von sicheren Einstellungen auf dem mobilen Endgerät, die sowohl den Benutzer als auch die Apps weitgehend in ihren Freiheiten einschränken, bleibt ein Restrisiko. Dieses Restrisiko beruht in erster Linie darauf, dass die Geräte ausserhalb einer gesicherten Umgebung eingesetzt werden, oft auch in Umgebungen, in denen man einen Laptop nicht einsetzen würde. Es besteht immer die Gefahr, dass die Geräte (und damit die darauf befindlichen Daten) abhandenkommen. In einem solchen Fall kann man nur darauf vertrauen, dass die eingesetzten Mechanismen zum Schutz der Daten noch wirksam greifen und nachträglich initiierte Aktionen (beispielsweise Remote Wipe) funktionieren.

Sogar beim Einsatz eines Secure Containers verbleiben Restrisiken, denen nicht ohne weiteres begegnet werden kann. Als Beispiel sei die unerlaubte Verwendung des Gerätemikrofons zum Abhören genannt.

Weiterführende Informationen zu Schutzmassnahmen von Mobilen Geräten finden sich im Dokument «Konfigurationsempfehlung auf Basis betriebssystemeigener Mittel für eine Nutzung mit erhöhter Sicherheit» des Bundesamt für Sicherheit in der Informationstechnik (BSI).

7.3 Cloud-Dienste

Der Begriff Cloud steht als Kurzform für Cloud Computing. Eine Cloud besteht aus räumlich entfernt stationierten Servern, auf die über eine gesicherte und geschützte Internetverbindung von jedem beliebigen Ort aus jederzeit zugegriffen werden kann.

Private Cloud

Wenn Unternehmen eigene Server für Cloud Computing benutzen, spricht man von einer Private Cloud. Der Nutzer greift also praktisch auf den Firmen-Server zu. Die dort gespeicherten Daten und Dienste stehen nicht der Öffentlichkeit zur Verfügung. Damit bleiben sicherheitskritische Daten also im Unternehmen. Eine Private Cloud stellt allerdings sehr hohe Ansprüche an die System-Administration und gilt als zeitaufwändig sowie kostenintensiv.

Public Cloud

Eine Public Cloud stellt ihre Dienste mehreren Benutzern gleichzeitig über das Internet zur Verfügung (Shared Infrastruktur). Das System wird vom Anbieter überwacht, gewartet und immer an den Bedarf der Nutzer angepasst. Damit entfallen im Unternehmen die Kosten für die Errichtung, Unterhaltung und laufende Anpassung einer firmeninternen Serverarchitektur.

[5] Quellennachweis: BSI-Veröffentlichungen zur Cyber-Sicherheit | iOS (https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_074.pdf?_blob=publicationFile&v=1)

Hybrid Cloud

Die Kombination aus den beiden Lösungen Private und Public Cloud ist die Hybrid Cloud, bei der sensible Daten im Unternehmen gespeichert werden und andere Arbeitsdateien gesichert auf einer geteilten Infrastruktur zugänglich sind.

Anwendungsfälle für Cloud-Dienste sind beispielsweise:

- Betriebsdaten-Auswertungen (OT-Prozesse)
- Kommunikations- und Workflow-Anwendungen
- Endpoint-Protection
- Mail-Gateway, Mail-Service
- Telefonsysteme
- Büro-Informatik
- Alarmierungs-Systeme (SMS, Mail, Workflow)

Cloud Service Modelle

Die verfügbaren Servicemodelle auf einer Cloud sind
- IaaS (Infrastructure as a Service)
- PaaS (Platform as a Service)
- SaaS (Software as a Service)
- DaaS (Desktop as a Service).

Sicherheitsarchitektur der Cloud

Jedes Cloud-Servicemodell hat eine eigene Sicherheitsarchitektur, die vom Cloud Provider und vom Kunden verwaltet wird. Cloud-Sicherheitsarchitekturen unterscheiden sich insbesondere darin, ob die betreffende Cloud als Public Cloud, Private Cloud oder Hybrid Cloud bereitgestellt wird.

Je nach Kritikalität der verarbeiteten Informationen ist auch eine Cloud Anwendung (Private Cloud) in die entsprechende Schutzstufe einzuordnen und mittels angemessener Massnahmen zu schützen.

Sicherheitsverantwortlichkeiten in der Cloud

Diese hängen vom Service- und Bereitstellungsmodell ab, grundsätzlich aber wird die Verantwortlichkeit für die Cloud-Sicherheit bis zu einem gewissen Grad immer geteilt.

Bei der IaaS-Lösung eines Public Cloud Services Anbieters, verwaltet der Anbieter beispielsweise die physischen Netzwerkschnittstellen, die Hypervisoren und den Datenspeicher, während der Kunde für die zugehörigen Betriebssysteme, Anwendungen und Daten zuständig ist.

Der Cloud Provider überwacht bei dieser Architektur die «externe» Sicherheit der Cloud, also die wesentliche Hardware und Software, z. B. Datenbanken und Rechenkapazität in einem Rechenzentrum. Der Kunde konzentriert sich auf die «innere» Sicherheit – wie Zugriffsanfragen gewährt oder verweigert werden, wie die Firewalls des Unternehmens konfiguriert und andere Aktivitäten bei der Nutzung eines Cloud-Service gehandhabt werden.

Bei PaaS, SaaS und DaaS in der Public Cloud übernimmt der Cloud Service Anbieter im Vergleich zu IaaS einen grösseren Anteil der Sicherheitsverantwortung. Bei SaaS muss der Kunde sich beispielsweise nicht um die Verwaltung der zugrunde liegenden Server, Datenbanken und der damit verbundenen Sicherheitsmechanismen (z. B. das Verschlüsseln mit einer Ende-zu-Ende-Verschlüsselung) kümmern. Dieses Arrangement bedeutet aber nicht, dass SaaS risikofrei sind, da der Kunde den Cloud Provider gründlich prüfen und sicherstellen muss, dass der Anwendungszugriff ausreichend gesichert ist.

Private- und Hybride-Clouds, in denen eine Organisation Ressourcen ausschliesslich für den eigenen Gebrauch verwaltet, erfordern in der Regel mehr Verantwortung von Seiten des Kunden in Bezug auf eine sichere Datenspeicherung. Für Private- und Hybrid-Cloud-Daten bestehen einige Vorteile, da diese nicht so stark von gemeinsam genutzter Infrastruktur abhängig sind wie Public-Cloud-Daten. Der direkte Sicherheitsaufwand für den Kunden kann jedoch grösser sein.

Service Level Agreement

Ein Cloud SLA (Cloud Service Level Agreement) ist eine Vereinbarung zwischen einem Cloud-Service-Anbieter und einem Kunden, die sicherstellt, dass ein Mindestmass an Service aufrechterhalten wird. Sie garantiert ein gewisses Niveau an Zuverlässigkeit, Verfügbarkeit und Reaktionsfähigkeit von Systemen und Anwendungen, legt fest, wer im Falle einer Serviceunterbrechung zuständig ist, und beschreibt Sanktionen für den Fall, dass das Serviceniveau nicht erreicht wird.

Die Rolle der SLA ist im Grunde dieselbe wie die eines jeden Vertrags – es handelt sich um ein Dokument, welches die Beziehung zwischen Kunde und Anbieter regelt. Diese vereinbarten Regeln bilden die Grundlage der Zusammenarbeit.

Das in der SLA definierte Serviceniveau sollte spezifisch und messbar sein, damit ein Benchmarking möglich ist und, falls in der Vereinbarung vorgesehen, entsprechende Belohnungen oder Strafen ausgelöst werden können.

8 Schlussfolgerung

Informationssicherheit ist kein Selbstzweck. Alle Massnahmen zur Abwehr von Cyber-Angriffen stehen im Dienst der Betriebssicherheit und Zuverlässigkeit der gesamten Anlage. KVA sind systemrelevant zur Erfüllung des primären Auftrages der Abfallentsorgung wie auch des sekundären der Energieversorgung von Industrie und Haushalten. So sind Cybersecurity und Cyber-Resilience Teil des umfassenden Risikomanagements und damit ein Top-Management-Thema.

Informationssicherheit bleibt jedoch nicht auf die Führungsebene beschränkt, die Sensibilisierung aller Mitarbeiter auf immer wieder neue und sich ändernde Angriffsszenarien spielt eine zentrale Rolle.

Die vorliegenden IKT-Standards sollen helfen, den Stand der eigenen Informatikumgebung beurteilen zu können, wie hoch die Maturität der Informationssicherheit ist:

- Sind Richtlinien ausgearbeitet und Prozesse definiert?
- Werden Massnahmen partiell oder vollständig umgesetzt?
- Werden sie regelmässigen Beurteilungen unterzogen?
- Ist ein kontinuierlicher Verbesserungsprozess implementiert (KVP)?

Erfolgreiche Cyber-Angriffe können massive Betriebseinschränkungen oder gar zu einem Stillstand der Anlage führen, was betriebswirtschaftliche Konsequenzen und auch Reputationsschaden zur Folge hat. Bei kleinen und mittleren Unternehmen (KMU) in der Privatwirtschaft sind Cyber-Angriffe nicht selten sogar existenzgefährdend. Die in diesem IKT-Minimalstandards als «Best Practices» formulierten Richtlinien und ein kontinuierlicher Verbesserungsprozess zielen darauf ab, die Betriebszuverlässigkeit zu erhöhen.

Neben dem hier vorliegenden Handbuch Cybersecurity stellt die wirtschaftliche Landesversorgung den Betrieben der Abfallentsorgung einen IKT-Minimalstandard als Excel-basiertes Assessment Tool[6] zur Verfügung. Zur Einschätzung des Maturitätsniveaus des Unternehmens oder der Organisation ist insbesondere das Assessment Tool hilfreich. Zu diesem Tool besteht der IKT-Minimalstandard, in dem die Vorgehensweise beschrieben ist und welches an das Thema heranführt, damit die Fragen beantwortet werden können.

Dieses Handbuch ist keine bindende Vorgabe, sondern soll die Akteure/innen der Abfallentsorgung zur eigenen Reflektion hinsichtlich Cybersecurity anregen. Informationssicherheit ist kein Zustand, sondern ein Prozess. Das Handbuch Cybersecurity soll diesen Prozess anstossen und bei der Umsetzung helfen.

[6] *Link zu Excel Tool: IKT-Minimalstandard (admin.ch)*

9 Grundlagen, Dokumente und Standards

Das vorliegende Handbuch IKT-Minimalstandard berücksichtigt Konzepte, Empfehlungen und Massnahmen von verschiedenen Standards und anderen normativen Dokumenten (nachfolgende Tabelle).

Titel	Jahr	Herausgeber & Beschreibung
Massnahmen zum Schutz von industriellen Kontrollsystemen (ICS)	2018	Hrsg.: **Nationales Zentrum für Cybersicherheit NCSC** 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	2015/ 2017	Hrsg.: **Bundesamt für wirtschaftliche Landesversorgung (BWL)** Die Risiko- und Verwundbarkeitsanalyse ist basierend auf der Nationalen Cyber Strategie (NCS) und der Strategie zum Schutz kritischer Infrastrukturen (SKI) entwickelt worden. Ziel ist die Analyse der Verwundbarkeit gegenüber Ausfällen oder Störungen der IKT.
Leitfaden Schutz kritischer Infrastrukturen (Leitfaden SKI)	2018	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)	2018	Hrsg.: **Bundesamt für Bevölkerungsschutz (BABS)** Die Strategie umschreibt den Geltungsbereich, bezeichnet die kritischen Infrastrukturen und hält die übergeordneten Grundsätze beim Schutz kritischer Infrastrukturen fest. Die nationale SKI-Strategie richtet sich an alle Stellen, die im Umfeld des Schutzes kritischer Infrastrukturen Verantwortlichkeiten aufweisen, insbesondere an die jeweils zuständigen Behörden, die politischen Entscheidungsträger und die Betreiber von kritischen Infrastrukturen.
Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)	2018	Hrsg.: **Informatiksteuerungsorgan des Bundes (ISB)** Da der Schutz der Informations- und Kommunikationsinfrastrukturen vor Cyber-Risiken im nationalen Interesse der Schweiz liegt, hat der Bundesrat die nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken in Auftrag gegeben. Diese Strategie soll aufzeigen, wie diese Risiken heute aussehen, wie die Schweiz dagegen gerüstet ist, wo die Mängel liegen und wie diese am wirksamsten und effizientesten zu beheben sind. Die Strategie identifiziert vorhandene Strukturen, definiert Zielsetzungen mit entsprechenden Massnahmen (z. B. Risiko- und Verwundbarkeitsanalysen eines Teilsektors).

Tabelle 8: Grundlagen Dokumente

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 Landesversor-gung fördern, sofern die Massnahmen im Rahmen der Vorbereitung auf eine schwere Mangellage zu einer wesentlichen Stärkung lebenswichtiger Versorgungssysteme und Infrastrukturen beitragen. Eine dieser Massnahmen bildet das vorliegende Handbuch Cybersecurity.

Tabelle 8: Grundlagen Dokumente

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

Titel	Herausgeber & Beschreibung
ISO 27001 **Information technology – Security techniques – Information security management systems – Requirements**	Hrsg: **International Standard Organization (ISO)** Detailliert die Anforderungen an ein Information Security Management System (ISMS). Die ISO 27k Serie umfasst eine Reihe von *Information Security Standards,* wovon folgende hier von Interesse sind: • 27000 Übersicht und Vokabular • 27001 Anforderungen: Grundlagen mit Kontrollen und Kontrollzielen im Anhang • 27002 Leitfaden für Informationssicherheitsmassnahmen • 27003 Informationssicherheitsmanagementsysteme – Anleitung zur Umsetzung • 27005 Risikomanagement • 27019 Informationssicherheitsmassnahmen für die Energieversorgung Die ISO 27000 Security Normenreihe ist mittlerweile weit verbreitetet und dürfte sich in den kommenden Jahren als die massgebende erweisen. Schon heute liegt durchaus richtig, wer ISO Security Standards befolgt. Im Gegensatz zu anderen Standards oder Frameworks sind sie nicht so sehr detailliert, dementsprechend flexibel anwendbar und können über eine längere Zeitspanne kontinuierlich verbessert und erweitert werden. Das ISMS, der Inhalt der Massnahmen, muss fachspezifisch adaptiert und umgesetzt werden.
ISO 27002 **Information technology – Security techniques – Code of practice for information security controls**	
ISO 22301 **Security and resilience – Business continuity management systems – Requirements**	Hrsg: **International Standard Organization (ISO)** Detailliert die Anforderungen an ein Business Continuity Management System.
ISO 31000 **Risk management**	Hrsg: **International Standard Organization (ISO)** Diese Norm legt Leitlinien fest, die den Umgang mit Risiken in einer Organisation beschreiben. Die spezielle Anwendung dieser Leitlinien kann an jedes Unternehmen in seiner spezifischen Umgebung angepasst werden. Der Standard liefert einen sehr allgemeinen Ansatz, der nicht industrie- oder sektorspezifisch ist und gleichzeitig für jegliche Art von Risiken anwendbar ist. Darüber hinaus kann die Norm während der gesamten Lebensdauer eines Unternehmens verwendet werden und ist auf allen Unternehmensebenen sowie im Prozess der Entscheidungsfindung implementierbar.
ISO27005 **Information security risk management**	Hrsg: **International Standard Organization (ISO)/ International Electrotechnical Commission (IEC)** Der Standard enthält Leitlinien für ein systematisches und prozessorientiertes Risikomanagement, das gegebenenfalls auch die Einhaltung der Anforderungen an das Risikomanagements nach ISO/IEC 27001 unterstützt.

Tabelle 9: Nationale und internationale Standards zu IKT-Sicherheit

Titel	Herausgeber & Beschreibung
ISO 27019 Information security controls for the energy utility industry	Hrsg: **International Standard Organization (ISO)** Im Fokus des Standards stehen Systeme und Netzwerke zur Steuerung, Regelung und Überwachung von Gewinnung oder Erzeugung, Übertragung, Speicherung und Verteilung von elektrischer Energie, Gas, Öl und Wärme. Dazu gehören Steuerungs- und Automatisierungssysteme, Schutz- und Sicherheits- sowie Messsysteme inklusive der Kommunikationstechnik. Der Standard fasst diese als Prozessleittechnik zusammen. Im Unterschied zu ISO/IEC 27002 stehen hier kritische Infrastrukturen im Vordergrund, die für einen sicheren und zuverlässigen Betrieb notwendig sind und damit auch in den Managementprozessen entsprechend berücksichtigt werden müssen (Verfügbarkeit und Integrität der Daten).
IEC 62264 ff Enterprise Control System Integration	Hrsg: **Internationale Elektrotechnische Kommission** Eine Normenreihe von insgesamt 4 Standards zur Integration von Unternehmens-IT und Kontroll- und Leitsystemen.
IEC 62443 ff Industrial communication networks – Network and system security	Hrsg: **Internationale Elektrotechnische Kommission** Serie von insgesamt 13 Industrial Automation and Control System (IACS) Security Normen und technischen Spezifikationen. Die IEC 61508 ff (Sicherheitsgrundnorm für programmierbare Steuerungssysteme) wird um das Thema Informationssicherheit erweitert und deckt das Thema für Automatisierung- und Steuerungssysteme für Industrieanlagen komplett und eigenständig ab. Es werden vier verschiedene Aspekte bzw. Ebenen der Informationssicherheit abgedeckt: • Allgemeine Aspekte wie Konzepte, Terminologie oder Metriken: IEC 62443-1-x • IT-Sicherheits-Management: IEC 62443-2-x • System-Ebene: IEC 62443-3-x • Komponenten-Ebene: IEC 62443-4-x Speziell zu erwähnen ist die Behandlung von Netzwerk- und Zonenarchitektur, die sich in anderen Standards kaum oder nicht so detailliert findet. Aktuell entwickelt sich diese Norm zur grundlegenden normativen Vorgabe im Kontext mit den RAMS-Normen der CENELEC (EN 50126 und weitere).
BDEW Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme	Hrsg: **BDEW Bundesverband der Energie- und Wasserwirtschaft e.V., Österreichs E-Wirtschaft** Das «BDEW-White» wurde für die grundsätzlichen Sicherheitsmassnahmen der Steuerungs- und Telekommunikationssysteme der Energiewirtschaft mit entwickelt. Das strategische Ziel des Whitepapers ist die positive Beeinflussung der Produktentwicklung für die oben genannten Systeme im Sinne der IT-Sicherheit und die Vermittlung eines gemeinsamen Verständnisses in der Branche für den Schutz dieser Systeme. Das BDEW-Whitepaper hat sich in der DACH-Region im Bahnstrombereich zu einer massgebenden Grundlage für die Beschaffung entwickelt. Das Whitepaper wird durch Ausführungshinweise ergänzt.

Tabelle 9: Nationale und internationale Standards zu IKT-Sicherheit

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

Tabelle 9: Nationale und internationale Standards zu IKT-Sicherheit

Titel	Herausgeber & Beschreibung
Zuordnungstabelle ISO zum modernisierten IT-Grundschutz	Der IT-Grundschutz interpretiert im BSI-Standard 200-2 die Anforderungen bzw. Massnahmen der ISO-Normen 27001 sowie 27002. Die IT-Grundschutz-Anwender werden mit einer Zuordnungstabelle bei der Abbildung der Inhalte von der ISO 27001/2 auf den IT-Grundschutz unterstützt.
Industrielle Steuerungs- und Automatisierungssysteme (ICS) – Allgemeine Empfehlungen	Hrsg: **Bundesamt für Sicherheit in der Informationstechnik (BSI)** Das Kompendium stellt ein Grundlagenwerk dar und soll einen einfachen Zugang zur SCADA IT Security ermöglichen. Es werden einige allgemeinen Grundlagen der Automation erläutert, sowie auf Besonderheiten und Standards in diesem Bereich aufmerksam gemacht. Abgerundet wird das Thema durch eine Sammlung von Massnahmen und einer Vorgehensweise um die Umsetzung zu prüfen. Auf dieser Seiter erhält der Anwender zusätzliche fachspezifische Hilfestellungen.
Zuordnungstabelle – Mapping of Dependencies to International Standards	Hrsg: **European Union Agency for Network and Information Security ENISA** In diesem Bericht wurden die Abhängigkeiten und Zusammenhänge zwischen Betreibern von essentiellen Diensten (OES) und Anbietern digitaler Dienste (DSP) analysiert und eine Reihe von Indikatoren für ihre Bewertung ermittelt. Diese Indikatoren sind internationalen Standards und Rahmenbedingungen zugeordnet, nämlich ISO IEC 27002, COBIT5, Sicherheitsmassnahmen der NIS-Kooperationsgruppe und NIST Cybersecurity Framework.
Communication network dependencies for ICS/SCADA Systems	Hrsg: **European Union Agency for Network and Information Security ENISA** Dieser Bericht konzentriert sich auf die Aspekte der Kommunikationsnetze und der Interkommunikation zwischen ICS/SCADA und der Erkennung von Schwachstellen, Risiken, Bedrohungen und Sicherheitsauswirkungen, die durch 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.
ENISA Threat Landscape/Taxonomy	Hrsg: **European Union Agency for Network and Information Security ENISA** Die ENISA Threat Landscape bietet einen Überblick über Bedrohungen sowie aktuelle und sich abzeichnende Trends. Sie basiert auf öffentlich zugänglichen Daten und bietet eine unabhängige Ansicht zu beobachteten Bedrohungen, Bedrohungsakteuren und Bedrohungstrends. In der Taxonomy werden die Bedrohungen systematisch zusammengestellt.

Tabelle 9: Nationale und internationale Standards zu IKT-Sicherheit

10 Regulatorische Anforderungen für die Abfallentsorgung

Folgende nationale und internationale Regelwerke sowie Standards kommen in der Abfallentsorgung zur Anwendung:

Nationale Rechtsgrundlagen

Organhaftung gemäss Obligationenrecht, Art. 754
SR 220 – Bundesgesetz vom 30. März 1911 betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) (admin.ch)

Bundesgesetz über den Umweltschutz (Umweltschutzgesetz, USG) vom 7. Oktober 1983 (SR 814.01)
SR 814.01 – Bundesgesetz vom 7. Oktober 1983 über den Umweltschutz (Umweltschutzgesetz, USG) (admin.ch)

Verordnung über die Vermeidung und die Entsorgung von Abfällen (VVEA) vom 4. Dezember 2015 (SR 814.600)
SR 814.600 – Verordnung vom 4. Dezember 2015 über die Vermeidung und die Entsorgung von Abfällen (Abfallverordnung, VVEA) (admin.ch)

Verordnung über den Verkehr mit Abfällen (VeVA) vom 22. Juni 2005 (SR 814.610)
SR 814.610 – Verordnung vom 22. Juni 2005 über den Verkehr mit Abfällen (VeVA) (admin.ch)

Verordnung des UVEK über Listen zum Verkehr mit Abfällen vom 18. Oktober 2005 (SR 814.610.1)
SR 814.610.1 – Verordnung des UVEK vom 18. Oktober 2005 über Listen zum Verkehr mit Abfällen (admin.ch)

Verordnung über die Rückgabe, die Rücknahme und die Entsorgung elektrischer und elektronischer Geräte (VREG) vom 20. Oktober 2021 (SR 814.620)
SR 814.620 – Verordnung vom 20. Oktober 2021 über die Rückgabe, die Rücknahme und die Entsorgung elektrischer und elektronischer Geräte (VREG) (admin.ch)

Verordnung über Getränkeverpackungen (VGV) vom 5. Juli 2000 (SR 814.621)
SR 814.621 – Verordnung vom 5. Juli 2000 über Getränkeverpackungen (VGV) (admin.ch)

Verordnung über die Höhe der vorgezogenen Entsorgungsgebühr für Getränkeverpackungen aus Glas vom 7. September 2001 (SR 814.621.4)
SR 814.621.4 – Verordnung vom 7. September 2001 über die Höhe der vorgezogenen Entsorgungsgebühr für Getränkeverpackungen aus Glas (admin.ch)

Verordnung des UVEK über die Höhe der vorgezogenen Entsorgungsgebühr für Batterien vom 28. November 2011 (SR 814.670.1)
SR 814.670.1 – Verordnung des UVEK vom 28. November 2011 über die Höhe der vorgezogenen Entsorgungsgebühr für Batterien (admin.ch)

Verordnung über die Sanierung von belasteten Standorten (Altlasten-Verordnung, AltlV) vom 26. August 1998 (SR 814.680)
SR 814.680 – Verordnung vom 26. August 1998 über die Sanierung von belasteten Standorten (Altlasten-Verordnung, AltlV) (admin.ch)

Verordnung über die Abgabe zur Sanierung von Altlasten (VASA) vom 26. September 2008 (SR 814.681)
SR 814.681 – Verordnung vom 26. September 2008 über die Abgabe zur Sanierung von Altlasten (VASA) (admin.ch)

Kernenergiegesetz (KEG) vom 21. März 2003 (SR 732.1)
SR 732.1 – Kernenergiegesetz vom 21. März 2003 (KEG) (admin.ch)

Kernenergieverordnung (KEV) vom 10. Dezember 2004 (SR 732.11)
SR 732.11 – Kernenergieverordnung vom 10. Dezember 2004 (KEV) (admin.ch)

Verordnung über tierische Nebenprodukte (VTNP) vom 25. Mai 2011 (SR 916.441.22)
SR 916.441.22 – Verordnung vom 25. Mai 2011 über tierische Nebenprodukte (VTNP) (admin.ch)

Luftreinhalteverordnung (LRV)
https://www.fedlex.admin.ch/eli/cc/1986/208_208_208/de#app7ahref0

Gewässerschutzverordnung (GSchV)
https://www.fedlex.admin.ch/eli/cc/1998/2863_2863_2863/de

Bundesgesetz über den Datenschutz (DSG)
https://fedlex.data.admin.ch/eli/cc/1993/1945_1945_1945

Strahlenschutzverordnung (StSV)
https://www.fedlex.admin.ch/eli/cc/1994/1947_1947_1947/de

Strahlenschutzverordnung neue Version nur in PDF
https://fedlex.data.admin.ch/filestore/fedlex.data.admin.ch/eli/cc/2017/502/20210101/de/pdf-a/fedlex-data-admin-ch-eli-cc-2017-502-20210101-de-pdf-a.pdf

Nationale Standards und Empfehlungen

Bundesamt für Gesundheit (BAG), Entsorgung radioaktiver Abfälle, Übersichtsseite
https://www.bag.admin.ch/bag/de/home/gesund-leben/umwelt-und-gesundheit/strahlung-radioaktivitaet-schall/radioaktive-materialien-abfaelle/entsorgung-von-radioaktiven-abfaellen.html#193585208

Entsorgung radioaktiver Abfälle, Wegleitung BAG, PDF
https://www.bag.admin.ch/dam/bag/de/dokumente/str/str-wegleitungen/abfaelle/artikel-114.pdf.download.pdf/201021_V1_Strahlenschutz_Wegleitung_Art-114_DE.pdf

IEEE802.11i Network Standards
https://standards.ieee.org/products-services/index.html

Sicheres Verhalten im digitalen Raum
https://www.s-u-p-e-r.ch/de/

IKT Minimalstandard – Hauptteil
https://www.bwl.admin.ch/dam/bwl/de/dokumente/themen/ikt/broschuere_minimalstandard.pdf.download.pdf/IKT_DE_2018_Web.pdf

IKT Minimalstandard – Excel-Tool
IKT-Minimalstandard (admin.ch)

IKT-Minimalstandard Strom
https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard/ikt_branchenstandards/minimalstandard_strom.html

IKT-Minimalstandard Abwasser
https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard/ikt_branchenstandards/abwasser.html

Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie (IKT) für Fernwärme- und Fernkälteversorgung
https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard/ikt_branchenstandards/fernwaerme-und-fernkaelteversorgung.html

Sichere Passwörter
https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-private/aktuelle-themen/schuetzen-sie-ihre-konten.html

Internationale Regelwerke

Halbzeitbilanz auf hoher Ebene des Europäischen Prozesses Umwelt und Gesundheit
https://www.euro.who.int/_data/assets/pdf_file/0007/290185/EHTF-MTR-Haifa_Report_de.pdf

WHO World Health Assembly 2015 resolution
https://www.euro.who.int/en/health-topics/environment-and-health/air-quality/news/news/2015/05/air-quality-and-health-resolution-adopted-at-the-sixty-eighth-world-health-assembly

ISA-62443-1-1, Security for industrial automation and control systems
https://www.isa.org/intech-home/2018/september-october/departments/new-standard-specifies-security-capabilities-for-c

NIST, Cybersecurity Framework
https://www.nist.gov/cyberframework

Glossar

Begriff	Beschreibung
Awareness	Bewusstsein, Wahrnehmung
Resilienz	Psychische Widerstandskraft; Fähigkeit, schwierige Lebenssituationen ohne anhaltende Beeinträchtigung zu überstehen
POLYCOM	Polycom ist ein Schweizer Funknetzwerk auf Basis von Tetrapol.
SIP-Telefonie	Unter SIP-Telefonie wird die gängige Sprachkommunikation über das Internet Protocol verstanden.
ESXi	VMware ESXi (vormals ESX) ist ein Bare-Metal-Hypervisor, der auf Ihrem Server installiert wird und diesen in mehrere virtuelle Maschinen unterteilt.
Unbewusste Kompetenz	Das Individuum hat so viel praktische Erfahrung mit seinen Fähigkeiten, dass sie ihm in Fleisch und Blut übergehen und jederzeit abgerufen werden können, oftmals ohne höhere Konzentration in Anspruch nehmen zu müssen. Diese Person kann ihre Fähigkeiten, da sie sich ihrer nicht bewusst ist, nicht mehr problemlos weitervermitteln. Mit unbewusster Kompetenz handeln die Menschen zwar intuitiv richtig, können ihr Handeln aber nicht mehr analysieren.
Shop Floor	Werkstadt und Produktion

Weitere Begriffe können aus dem Glossar des NCSC entnommen werden (Referenz): https://www.ncsc.admin.ch/ncsc/de/home/glossar.html

Abkürzungsverzeichnis

Abkürzung	Beschreibung
BABS	Bundesamt für Bevölkerungsschutz
BAG	Bundesamt für Gesundheit
BCM	Business Continuity Management
BIA	Business Impact Analysis
BWL	Bundesamt für wirtschaftliche Landesversorgung
BSI	Bundesamt für Sicherheit in der Informationstechnik, D
CNA	Corporate Network Access
DaaS	Desktop as a Service
DCS/PLS	Distributed Control System, Prozessleitsystem
DCS oder ICS	Industrial Control Systems, Industrielle Steuerungsanlagen wie z. B. SPS
DECT	Digital Enhanced Cordless Telecommunications
DEP	Device Enrollment Program
DMZ	Demilitarized Zone, Demilitarisierte Zone (Netzwerk)
DNS	Domain Name System
DSG	Datenschutzgesetz
EMS	Energiemanagementsystem
ERP	Enterprise-Resource-Planning
EU	Europäische Union
FLR	Feuer-Leistungsregelung
GSchV	Gewässerschutzverordnung
GSM	Global System for Mobile Communications
HMI	Human Machine Interface
IaaS	Infrastructure as a Service
ICS	Informations Controll System
IEC	International Electrotechnical Commission (Normen und Standards)
IKT	Informations- und Kommunikations Technologie (umfasst alles)
ISB	Instandhaltung Betrieb
ISMS	Information Security Management System (ISMS, engl. für «Managementsystem für Informationssicherheit»)
ISO	Internationale Organisation für Normung
IT	Information Technology, klassische Büro Netzwerk Infrastruktur
KMU	Kleine und mittlere Unternehmen
KPE	Kernprozess «Abfall Entsorgen»

Abkürzung	Beschreibung
KPI	Key Performance Indicator
KVA	Kehrichtverbrennungsanlage
KVP	Kontinuierlicher Verbesserungsprozess
LRV	Luftreinhalteverordnung
MFA	Multifaktor Authentifizierung
NCSC	Nationales Zentrum für Cybersicherheit
NFC	Near Field Connection
NIST	National Institute of Standards and Technology
OS	Operating System, Betriebssystem
OT	Operation Technology, Netzwerk Infrastruktur Bediensystem
PaaS	Platform as a Service
PDCA	Plan-Do-Check-Act-Zyklus, Deming-Zyklus
PLC, SPS	Programmable Logic Controller oder Speicherprogrammierbare Steuerung
PRJV	Parlament, Regierung, Justiz, Verwaltung
SaaS	Software as a Service
SCADA	Supervisory Control and Data Acquisition, Prozessleitsystem
SIP	Session Initiation Protocol
SKI	Schutz kritischer Infrastrukturen
SLA	Service Level Agreement
SMS	Short Message Service
SPS	Speicherprogrammierbare Steuerung
StSV	Strahlenschutzverordnung
UTD	Untertages-Deponie
VBSA	Verband der Betreiber schweizerischer Abfallverwertungsanlagen
VLAN	Virtual Local Area Network
VVEA	Verordnung über die Vermeidung und die Entsorgung von Abfällen (Abfallverordnung)
WAF	Web Application Firewall
WLAN	Wireless Local Area Network
WSUS	Windows Server Update Services

Abbildungsverzeichnis

Tabellenverzeichnis

11 Anhang

11.1 Business-Impact-Analyse (BIA)

Die auf das Thema Abfallentsorgung angepasste BIA, schlüsselt die kritischen Prozesse, welche in «Tabelle 3 Kritische Prozesse in den Kehrichtverbrennungsanlagen» im Minimalstandard als Angriffsvektoren identifiziert wurden, auf. Damit können die oben gewonnenen Erkenntnisse recht einfach in die BIA überführt werden. Diese liegt als Beispiel im Anhang bei. Da die finanziellen Bewertungskriterien anlagenabhängig sind, verstehen sich die Ereignissummen der Risikomatrizen als Beispiel.

Das Ergebnis der BIA ist dann das Produkt der Rest-Risikobereitschaft, welche man dann trotz umgesetzter Massnahmen bereit ist zu gehen.

Risiko Matrizen (Beispielgrössen)

	Prozess Entsorgung (Abfall) bezogen auf Gesamtlage						
E	Umstände, die zu längeren (>1 Tag) Leistungsunterbrechung führen	E1	E2	E3	E4	E5	E6
D	Umstände, die zu längeren (<1 Tag) Leistungsunterbrechung führen	D1	D2	D3	D4	D5	D6
C	Umstände, die zu kurzen (<12h) Leistungsunterbrechung führen	C1	C2	C3	C4	C5	C6
B	Umstände, die zu einer geringfügigen Einschränkung des Betriebs führen	B1	B2	B3	B4	B5	B6
A	Umstände, die zu unbedeutenden Auswirkungen führen	A1	A2	A3	A4	A5	A6

	Prozess Infrastruktur (ISB)						
E	>60 Mio CHF	E1	E2	E3	E4	E5	E6
D	30-60 Mio CHF	D1	D2	D3	D4	D5	D6
C	10-30 Mio CHF	C1	C2	C3	C4	C5	C6
B	1-10 Mio CHF	B1	B2	B3	B4	B5	B6
A	<1 Mio CHF	A1	A2	A3	A4	A5	A6

	Prozess Unternehmensführung						
E	>60 Mio CHF	E1	E2	E3	E4	E5	E6
D	30-60 Mio CHF	D1	D2	D3	D4	D5	D6
C	10-30 Mio CHF	C1	C2	C3	C4	C5	C6
B	1-10 Mio CHF	B1	B2	B3	B4	B5	B6
A	<1 Mio CHF	A1	A2	A3	A4	A5	A6

	Sehr gering	gering	begrenzt	erhöht	hoch	sehr hoch
in 10 Jahren	< 5%	5-25%	15-30%	50-75%	>75-90%	>95-100%
	1	2	3	4	5	6
	Eintrittswahrscheinlichkeit					

Abbildung 14: Risiko-Matrizen mit Beispielgrössen

Analysedetails

	Risiken						Mitigation				Korrekturmassnahmen
Nr.	Risiko Kategorie	Risiko Kategorie Detail	Detaillierte Beschreibung	Prozess Entsorgung	Prozess Infrastruktur (ISB)	Unternehmensführung (Business)	Risiko Mitigation	Prozess Entsorgung	Prozess Infrastruktur (ISB)	Unternehmens-Führung (Business)	Massnahme
1a	Global	Nachrichtenkommunikation	Ausfall Kommunikation, Daten, keine Prozessdaten für Verrechnung und Instandhaltung, PLS nicht betroffen								
1b	Global	Nachrichtenkommunikation	Ausfall Kommunikation, Voice, Internet, Telefon, Funkt und Internet gestört								
2a	Global	Faktor Mensch	Fehlbedienung, Überforderung, Unachtsamkeit, Unterforderung								
2b	Global	Faktor Mensch	Unzufriedenheit, Sabotage								
2c	Global	Faktor Mensch	Ungewolltes Opfer (Pishing, Social Engineering)								
3a	Fernwartung IT/OT	Fernwartung externe Dienstleister	Unkontrollierte Veränderung von Programm und Ablaufsteuerungen								
3b	Fernwartung IT/OT	Fernwartung externe Dienstleister	Fernwartungszugänge unterbrochen								
4a	Fernwartung IT/OT	Betriebsdaten	Unkontrolliertes Abfliessen, Verändern, Löschen								
4b	Fernwartung IT/OT	Betriebsdaten	Betriebsdaten nicht mehr zugänglich								
5	Fernwartung IT/OT	Automatische Updates	Fehlerhafte Updates, nicht verifizierbare Updatequelle								
6	Fernwartung IT/OT	Entwicklung	Durch fehlendes Maintenance System, Entwicklung und Anpassung am Produktivsystem (am offenen Herzen)								
7a	Fernwartung IT/OT	Backup Sicherung OT	Keine, falsche oder nicht plausible Backups								

Abbildung 15: Analysedetails gemäss Tabelle 3 Kritische Prozesse in den Kehrichtverbrennungsanlagen

Das Dokument BIA kann über diesen Link heruntergeladen werden:

https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard/ikt_branchenstandards/abfallentsorgung.html

Autoren/innen und Fachexperten der Erstausgabe

Vorname, Name	Firma	Funktion
Hans-Peter Käser	BWL	Projektleiter
Sven Peter	BWL	Fachexperte/Quality Assurance
Sandra Rüfenacht	BABS	Fachexpertin/Quality Assurance
Ariane Stäubli	VBSA	PL VBSA/Fachexpertin/Quality Assurance
Patric Imhof	Eniwa	Fachexperte/Quality Assurance
Thomas Bücherer	EWB	Fachexperte/Quality Assurance
Andreas Tschanz	EWB	Fachexperte/Quality Assurance
Christoph Beleda	IWB	Fachexperte/Quality Assurance
Bruno Hottinger	KVATG	Fachexperte/Quality Assurance
Marco Weber	KVATG	Fachexperte/Quality Assurance
Martin Muheim	Renergia	Fachexperte/Quality Assurance
Jonas Tschudi	SAIDEF	Fachexperte/Quality Assurance

Impressum und Kontakt

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

Konsultierter Verband
Verband VBSA