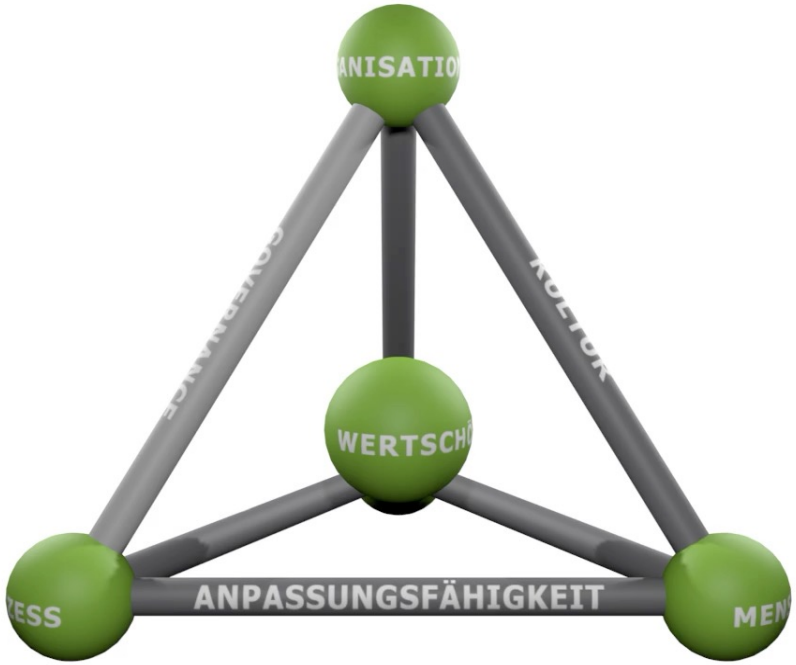
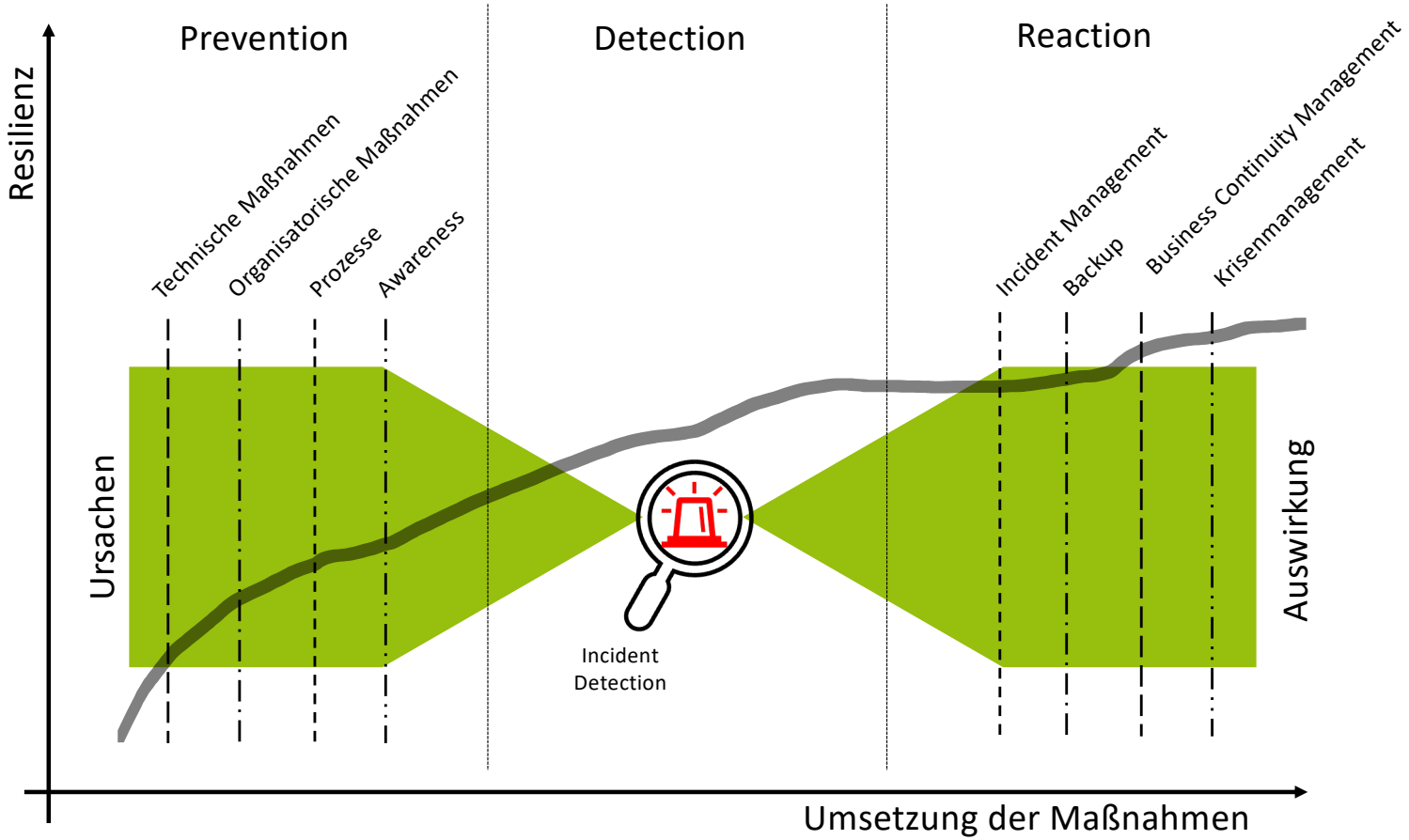
Workshop Organisation & Prozesse M2
Cybersecurity in der Produktion
08.11.2023

Mittelstand-Digital
Zentrum
Saarbrücken

Ganzheitliche Betrachtung über die gesamte Wertschöpfungskette
Mensch – Organisation – Prozesse – Technologie



Cybersecurity - Resilienzmodell



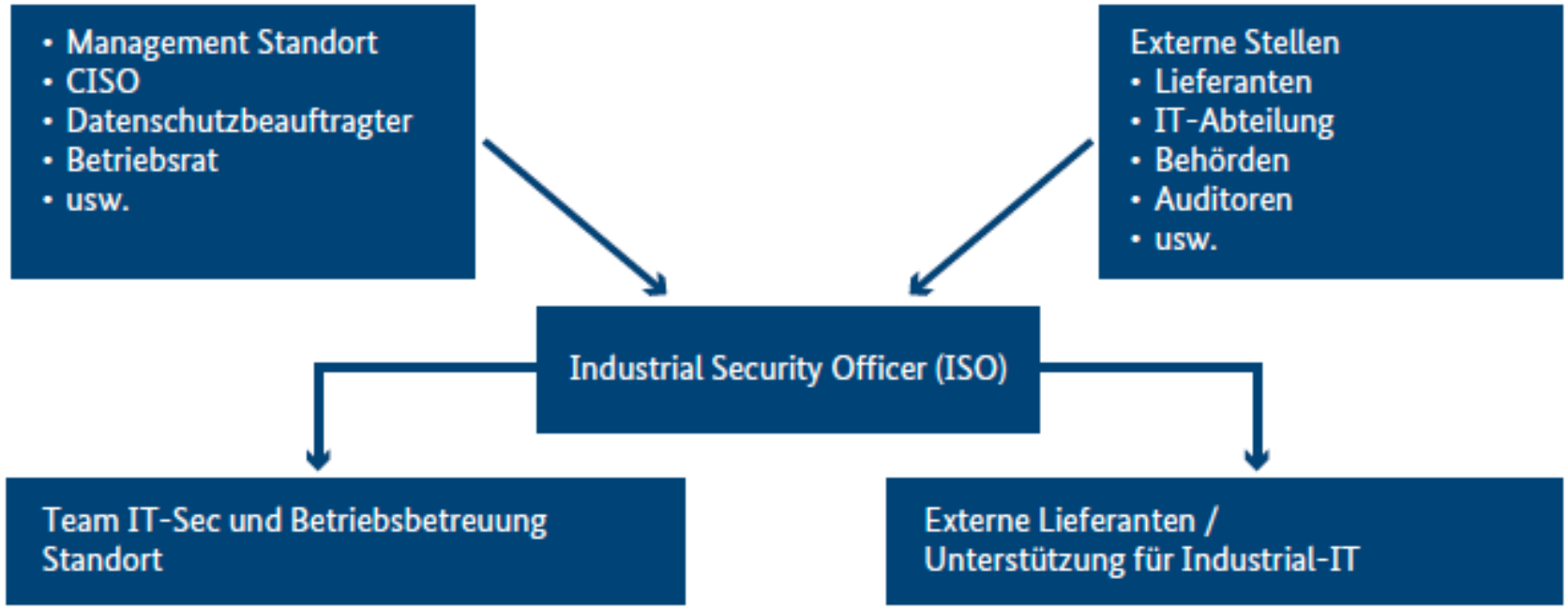
Wie sieht bei Ihnen die Security Organisation aus?

insbesondere im Kontext Industrial Security?

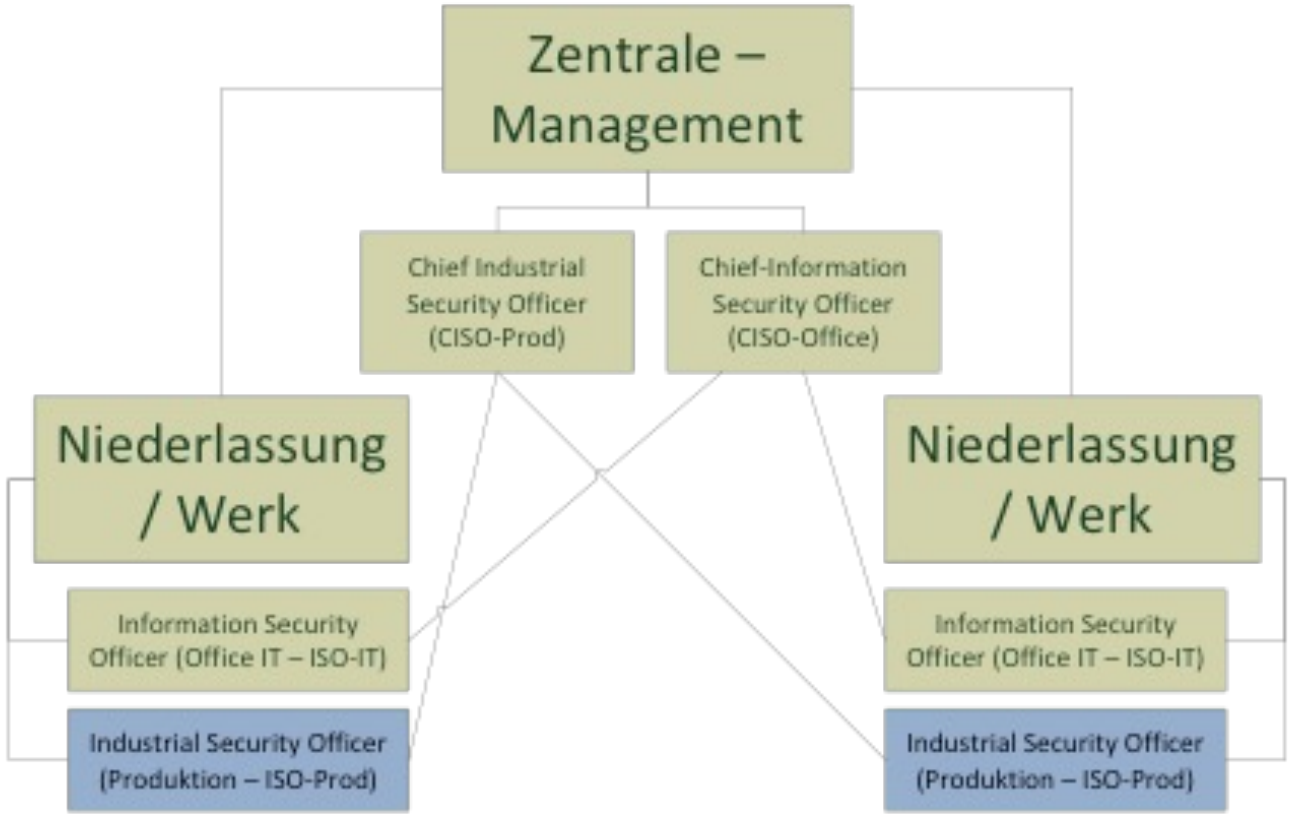
Was sehen Sie bei Ihren Kunden/Lieferanten?

Organisationsstruktur

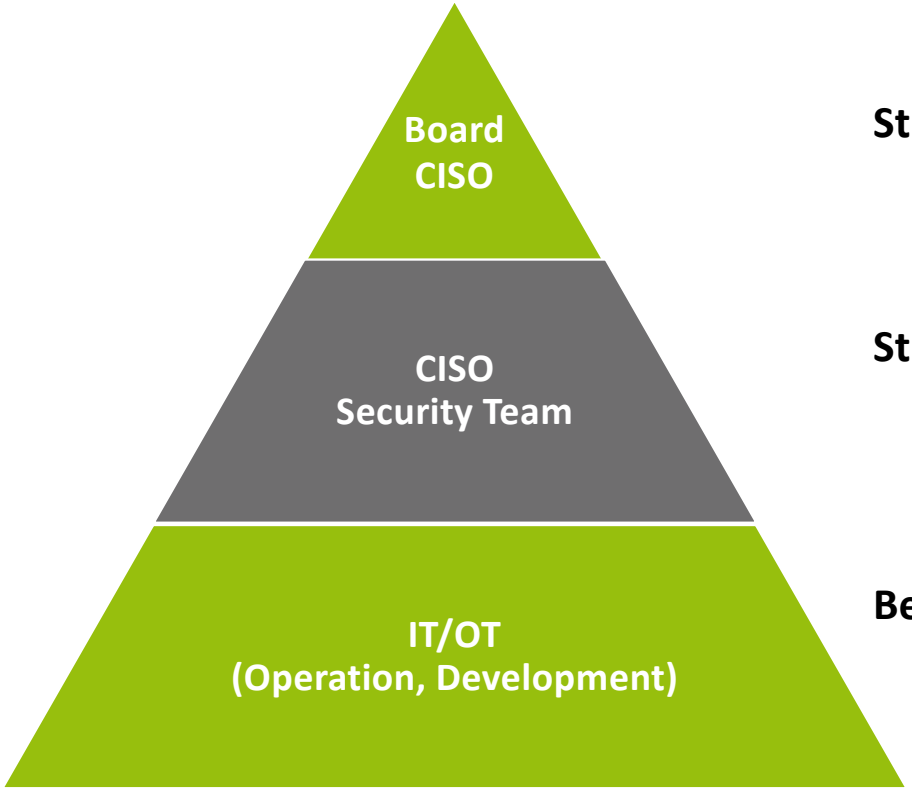
Abbildung 4: Organisatorische Einbindung eines Industrial Security Officer



Organisationsstruktur Security



Security Organisation

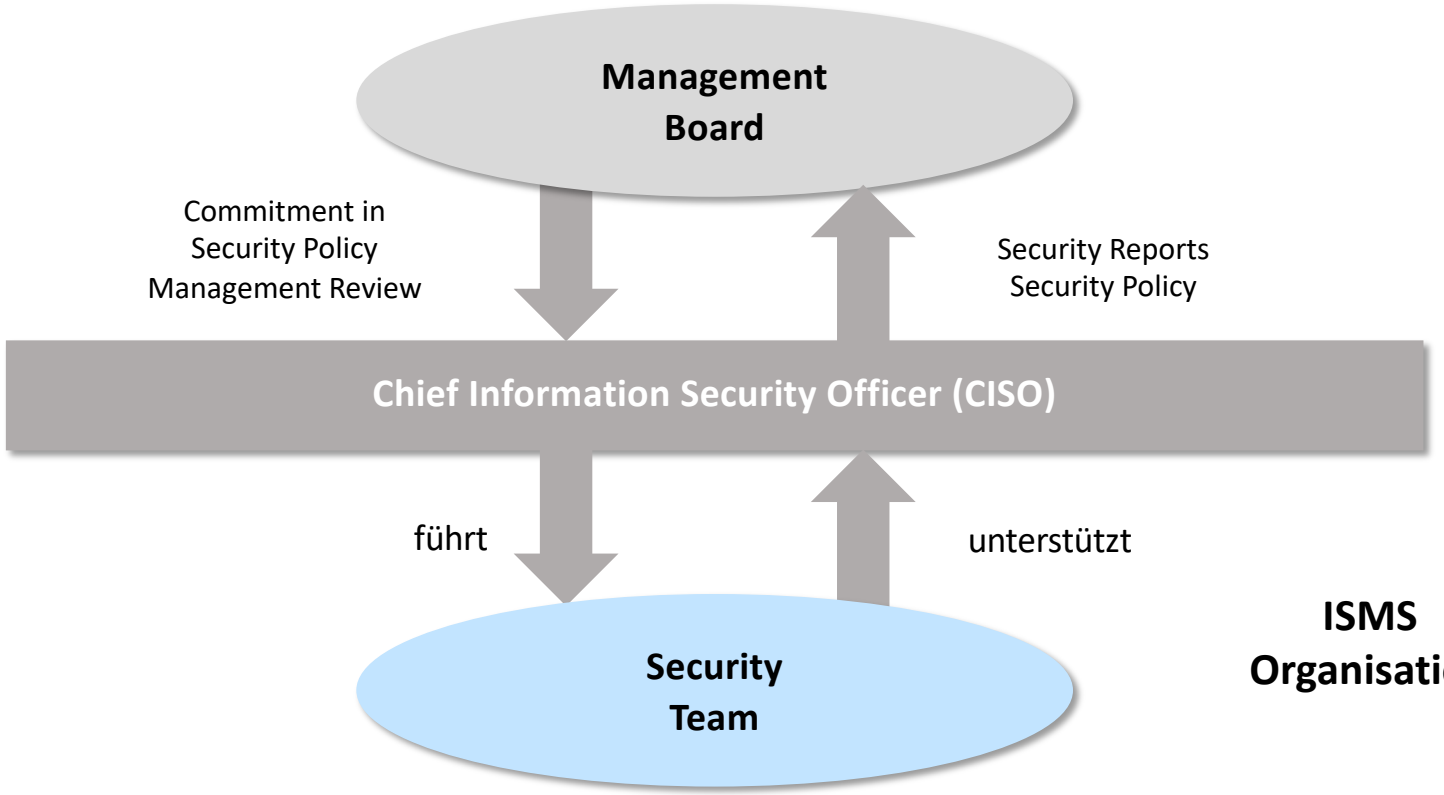


Strategische Entscheidungen

Strategische & taktische Aufgaben

Betrieb & Wartung

Security Organisation



ISMS Organisation

Organisation

Rollen:

- Management (Betreiber)
- IT-Sicherheitsbeauftragter
- IT-Betrieb
- ISMS-Team
- BCM Verantwortliche
- Qualitätsmanagement

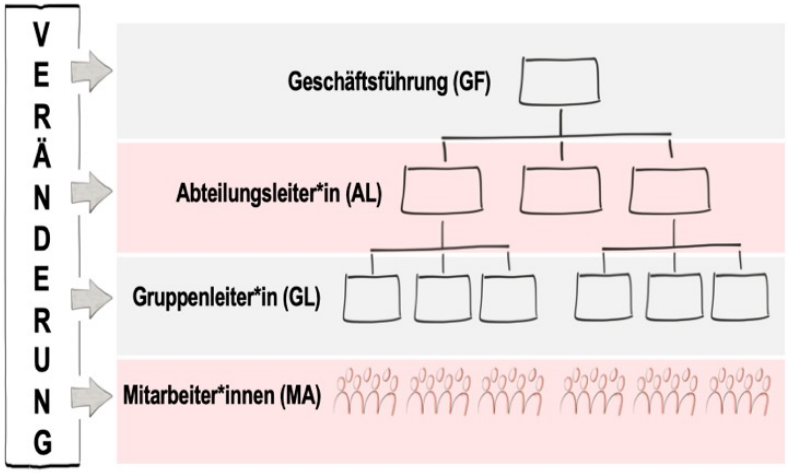
Inhalte:

- Wer meldet IT-Sicherheitsvorfälle - Wem?
- Wer ist verantwortlich für welche Teilbereiche?
- Welche Rolle hat welche Rechte & Aufgaben?

…Anpassungen Organisationsstruktur & Führung

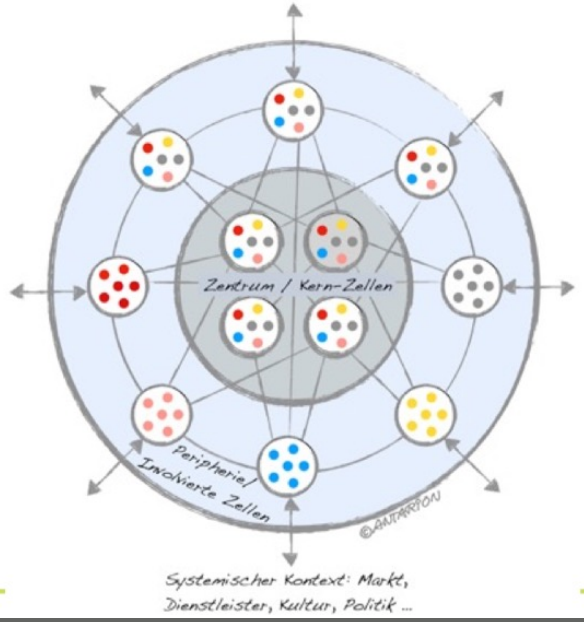
Kraft der 2 Systeme (Kotter)

In Organisationen gibt es neben dem klassischen Systemaufbau der Linien- oder Matrixorganisation zunehmend eine „Parallelwelt", die agile Zellenstruktur einer Netzwerkorganisation mit verflüssigenden Hierarchien. Das ist bedingt durch zunehmende Projekte, (agile) Transformationen – bis hin zum radikalen Umbau hin zu einem Teams-of-Teams-Ansatz. Kotter spricht von der „Kraft der 2 Systeme", die (bedingt) parallel laufen können.



Zellen-Architektur

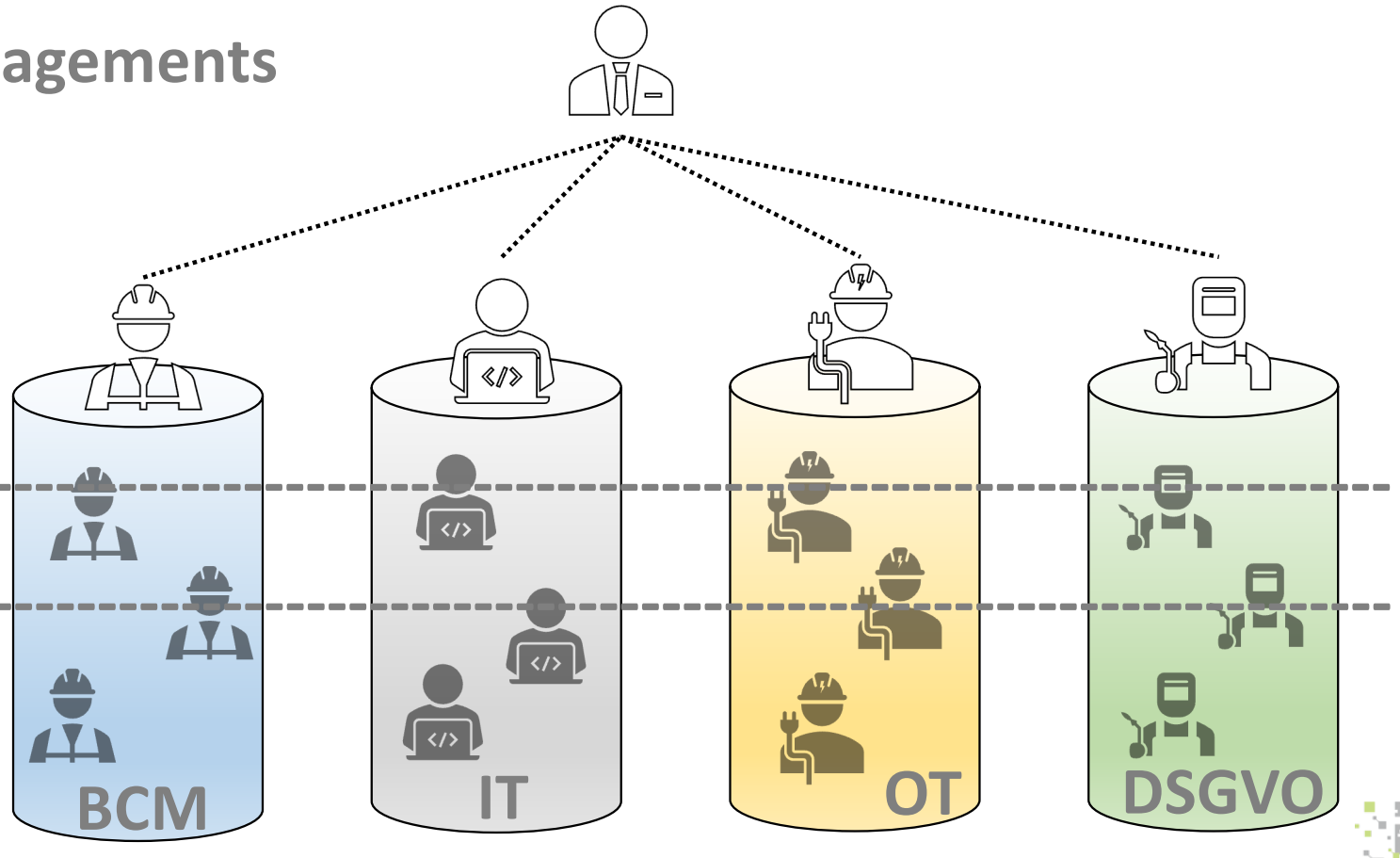
Systemische, vernetzte Zellen und Kreise ermöglichen agile und nachhaltige Architektur für kokreative Transformation, Organisation, (Inneres) Team …



Systemischer Kontext: Markt, Dienstleister, Kultur, Politik …

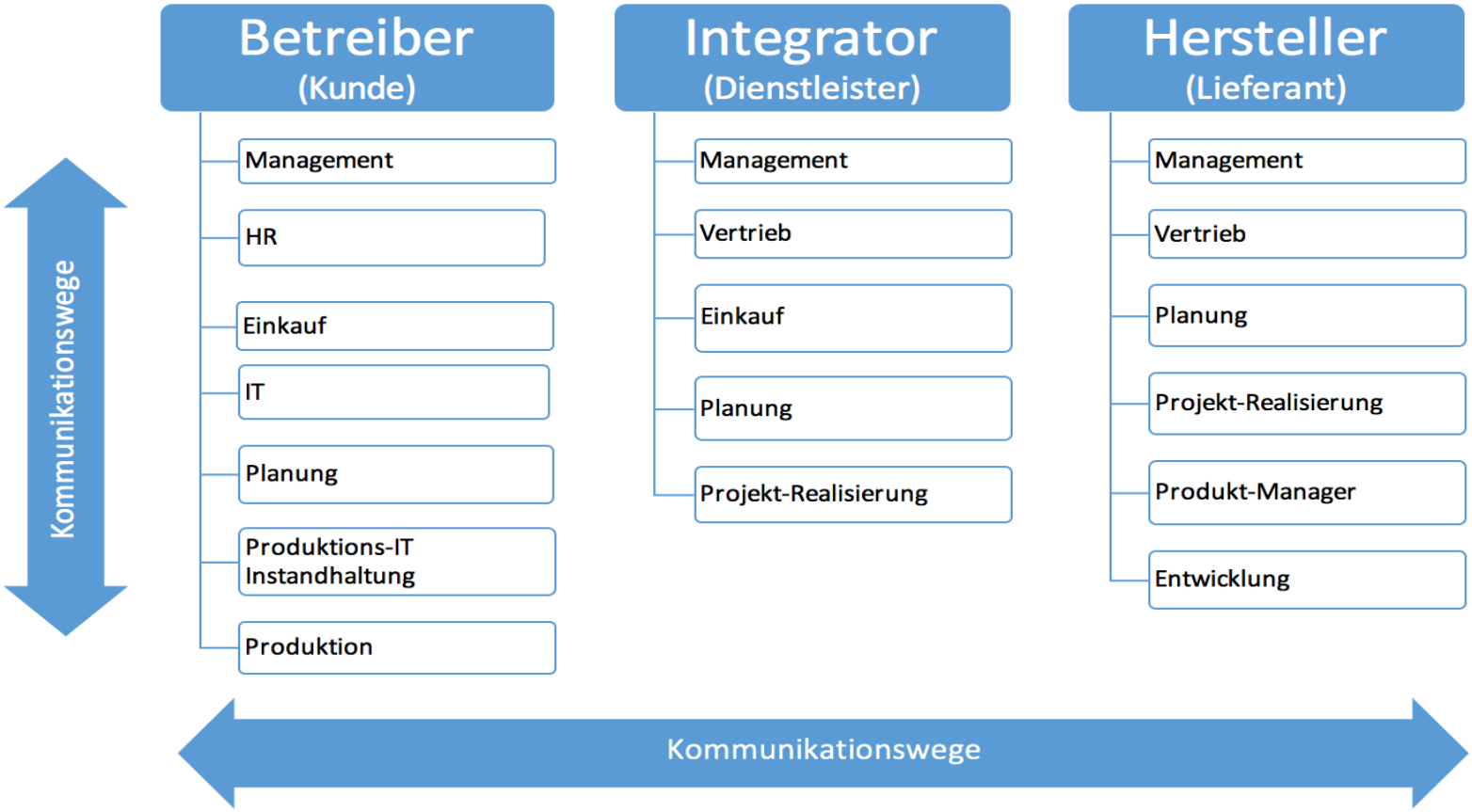
raus aus den Silos!

Aufgabe des Managements



Was sehen Sie für Rollen, welche im Kontext Industrial Security zu involvieren sind bzw. welche benötigt werden?

beispielhaft betroffene Rollen über die gesamte Wertschöpfungskette



IEC 62443

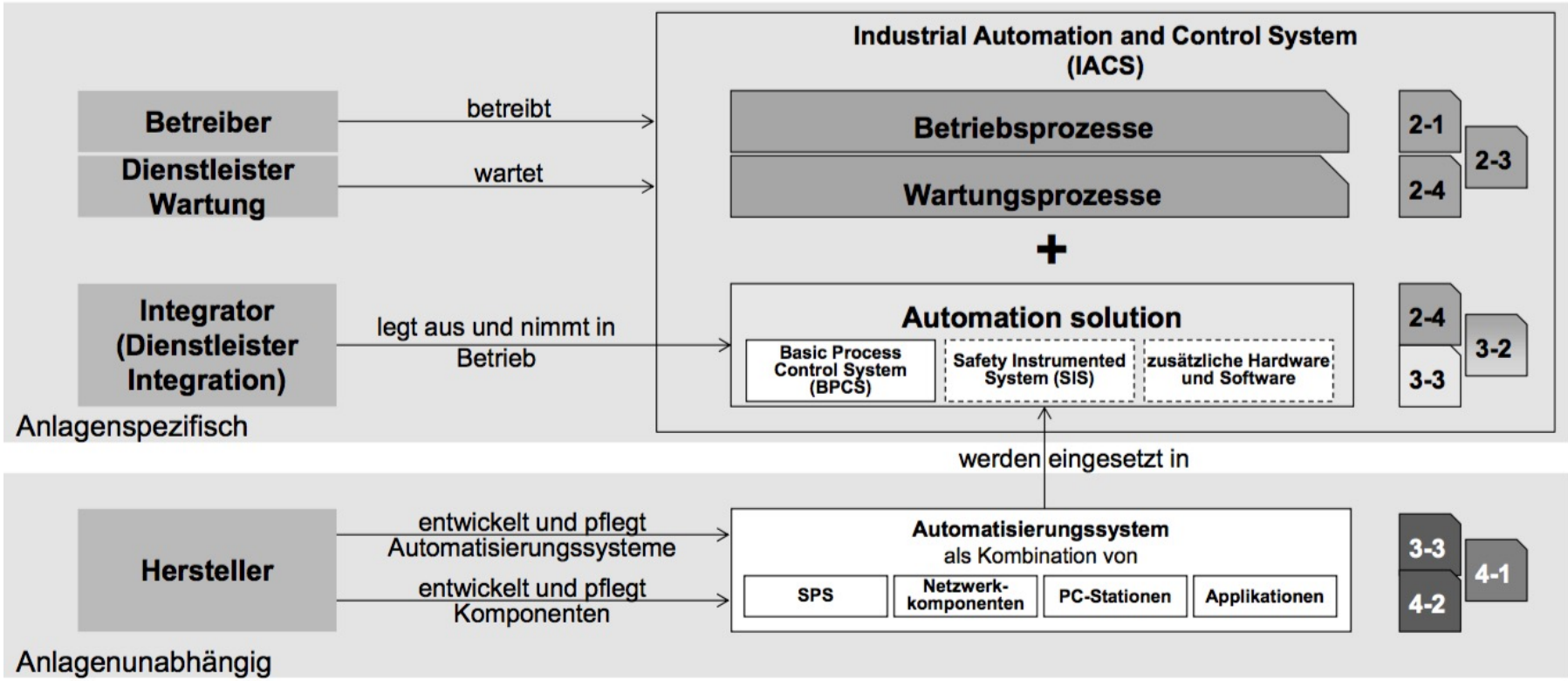
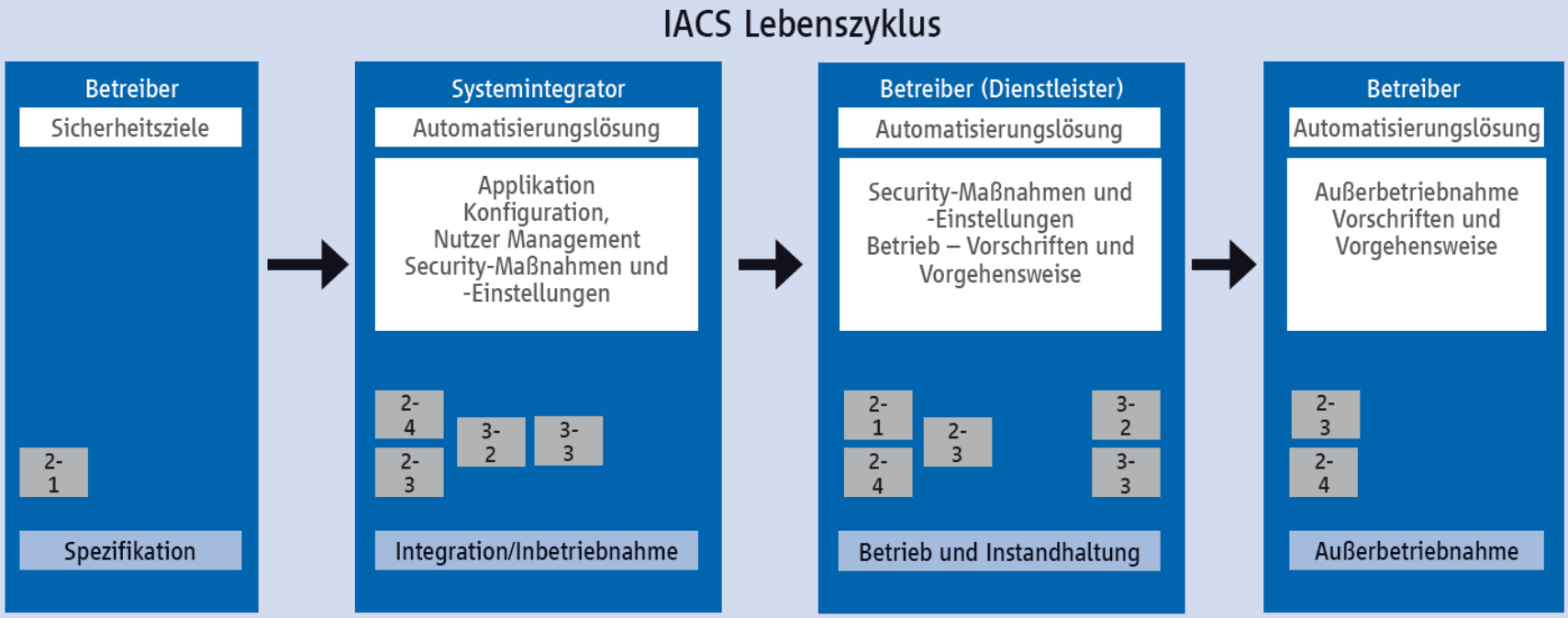


Bild 1 Basisrollen in der IEC 62443

IEC 62443

Abbildung 4: Lebenszyklus und seine Zusammenhänge gemäß IEC 62443



Quelle: ZVEI

Was sind wesentliche Aspekte für eine Verantwortungsrolle Industrial Security?

Industrial Security Verantwortlicher - Rollenbeschreibung

Organisation

- Der IT Sicherheitsverantwortliche besitzt eine unabhängige und organisatorisch herausgehobene Stellung.
- Der IT Sicherheitsverantwortliche ist weisungsbefugt bezüglich Maßnahmen und Handlungen, welche die Sicherheitspolitik seines Aufgabenfeldes betreffen.
- Je nach Organisationsstruktur berichtet der IT Sicherheitsverantwortliche direkt an die Geschäftsleitung, oder indirekt über eine weitere Organisationsstelle wie z.B. einem zentralen IT-Sicherheitsbeauftragten oder CIO (Chief Information Officer)
- Die Geschäftsführung unterstützt den IT-Sicherheits-verantwortlichen bei der Wahrnehmung seiner sich aus dem Verantwortlichkeitsbereich ergebenden Aufgaben.
- Der IT Sicherheitsverantwortliche arbeitet mit anderen Verantwortlichen aus dem Gebiet der Informationssicherheit zusammen.(z.B. Datenschutz, Werkschutz, Produktionsschutz, IT)
- Je nach Organisationsstruktur des Unternehmens müssen z.B. Aufgabenfelder der operativen Umsetzung, Einhaltung und des Betriebes von Maßnahmen zum Erhalt der Sicherheitspolitik personell unterstützt werden. Dazu können unterstützende Teams bzw. lokale Plant Security Koordinatoren eingesetzt werden.

Industrial Security Verantwortlicher

Verantwortungsbereich/Aufgaben

- Aufbau und Betrieb einer lokalen Organisation zur Umsetzung der IT Sicherheitsziele im industriellen Security Umfeld
- Durchführen der Entwicklung und Einführung einer unternehmensweiten Sicherheitspolitik, Handlungsleitlinien und Regelungen zur Absicherung des Erhalts der industriellen Sicherheit
- Identifizieren von Risiken und Bedrohungen
- Aufrechterhalten der Beziehungen mit lokalen und überregionalen Vertretern und Organisationen des Gesetzes, sowie mit anderen Behörden.
- Überwachen der aus Sicherheitsverstößen resultierenden Maßnahmen & Kontrolle der Effektivität von Maßnahmen
- Koordinieren von unabhängigen Sicherheitsaudits
- Unterstützen und Promoten der Bewusstseinsbildung und Ausbildung für IT-Sicherheit.
- Vorabprüfung und Einbeziehen in geplante Migrations-, Veränderungs- oder Umbaumaßnahmen in System oder Infrastrukturmaßnahmen
- Koordinieren und Steuern von externen Beratern und Partnerfirmen, welche im Aufgabengebiet der Industrial Security tätig sind.
- Unterstützung des Management bei IT Sicherheitsfragen

Industrial Security Verantwortlicher

Befugnisse und Kompetenzen

- Ist in allen für die Informationssicherheit relevanten Themen rechtzeitig zu informieren (sowohl auf Nachfrage, als auch unaufgefordert, soweit eine Relevanz für sein Aufgabengebiet besteht)
- Vorhaben und Änderungen, welche die Informationssicherheit berühren können (z.B. Migrations- oder Neuprojekte, Änderungen der IT-Infrastruktur, Änderungen von Rahmenbedingungen mit Auswirkung auf die Informationssicherheit) müssen frühzeitig in der Planungsphase mit dem IT Sicherheitsverantwortlichen abgestimmt werden.
- Hat ein Mitsprache- und Vetorecht bei allen Entscheidungen, die seinen/ihren Verantwortungsbereich betreffen. (z.B. Initiierung von Projekten, Beschaffung von informationsverarbeitenden Systemen, Änderung von Geschäftsprozessen, Ausbildung von Mitarbeitern)
- Hat direktes Vortragsrecht zur Geschäftsführung.
- Hat Zutrittsrecht zu allen Bereichen, in denen Informationstechnik seines Verantwortungsbereiches eingesetzt wird und damit zusammenhängende Daten verarbeitet werden, und zu allen Bereichen, in denen relevante Geschäftsprozesse und Informationen bearbeitet werden. Je nach Art der Daten muss er sich hierzu vorab mit dem Verantwortlichen des Daten- oder Produktschutzes abstimmen.
- Führt Prüfungen im Themenbereich der Informationssicherheit Verantwortungsbereich bezogen durch bzw. veranlasst Prüfungen durch unabhängige Dritte und überprüft so das aktuelle Informationssicherheitsniveau in seinem Aufgabenbereich.
- Ist Mitglied in Unternehmens-Ausschüssen zur Informationssicherheit

Industrial Security Verantwortlicher

Skill Profil – Industrie spezifische Aspekte

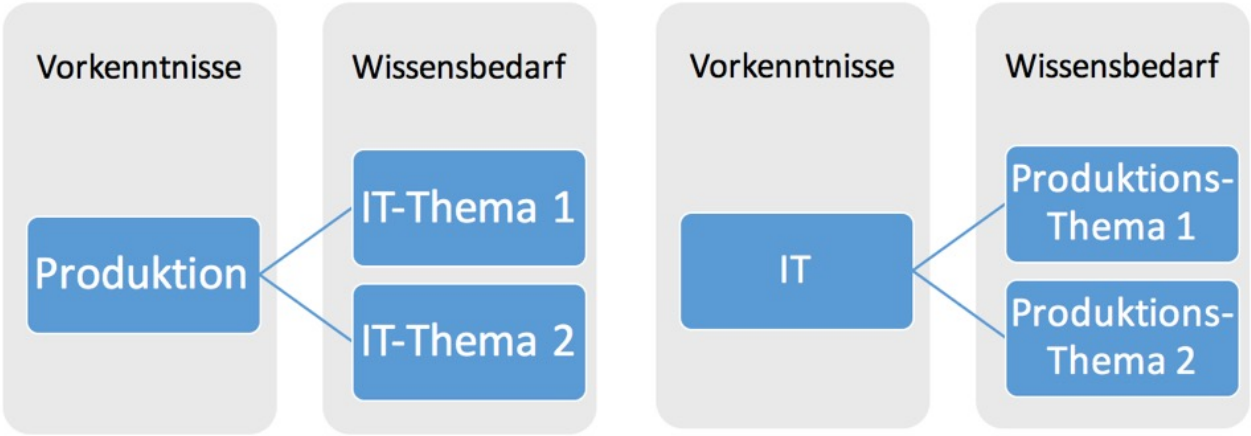
- Kenntnisse über Prozesse und Verfahrensabläufe der industriellen Umgebung
- Kenntnisse über die leittechnisch spezifischen IT und Infrastrukturen (z.B. Kenntnisse über Funktionsweise, Besonderheiten und Vielfalt der eingesetzten ICS Komponenten, sowie der proprietären, als auch standardisierten Industrieprotokolle und spezifischen Kommunikationsstrukturen, sowie Schnittstellen.
- Kenntnisse über Konfigurations- und Changemanagement der leittechnischen Prozesse und System-Umgebungen.
- Kenntnisse bezüglich Instandhaltung- und Service/Support relevanter Prozesse und Aspekte.
- Sprach- und Verständnisfähigkeit im verwendeten industriellen & leittechnisch spezifischen Glossar
- Softskills bezüglich Verantwortungskompetenz, sowie Teamfähigkeit und Konfliktmanagement
- Wissen über relevante Richtlinien im Industrieumfeld, sowie Kompetenz zur Anwendung
- Wissen über Sicherheitsmaßnahmen und Lösungsansätze (auch als Best Practice-Ansatz) im Industrieumfeld.
- Kenntnisse bezüglich Audits & Zertifizierungen im Industrieumfeld

Industrial Security Verantwortlicher

Skill Profil – IT spezifische Aspekte

- Kenntnisse bezüglich Netzwerke (Ethernet)
- Kenntnisse bezügliche eingesetzter Betriebssysteme
- Kenntnisse bezüglich Software-Lifecycle
- Kenntnisse bezüglich organisatorischer Security Maßnahmen
- Kenntnisse bezüglich Risikomanagement
- Kenntnisse bezüglich User / Rechte-Management
- Kenntnisse bezüglich technologischer Security Maßnahmen
- Kenntnisse bezüglich Reporting, KPI-Entwicklung, Überwachung und Monitoring
- Kenntnisse bezüglich Angriffs-Muster & Bedrohungen
- Kenntnisse bezüglich Forensik Maßnahmen

Rollenbesetzung aus der Produktion oder IT?



Erfahrungswerte aus dem Markt
Aufgrund des notwendigen sehr spezialisierten Wissens aus dem Industrie/Produktionsumfeld ist für Personen, welche dieses aus dieser Umgebung besitzen, und eine IT Affinität bereits mitbringen der notwendige fehlende Wissenstransfer für diese Rolle in der Regel leichter zu übermitteln.

Wissensmanagement Industrial Security

Training & Ausbildung diverse Formate bis zu Coaching

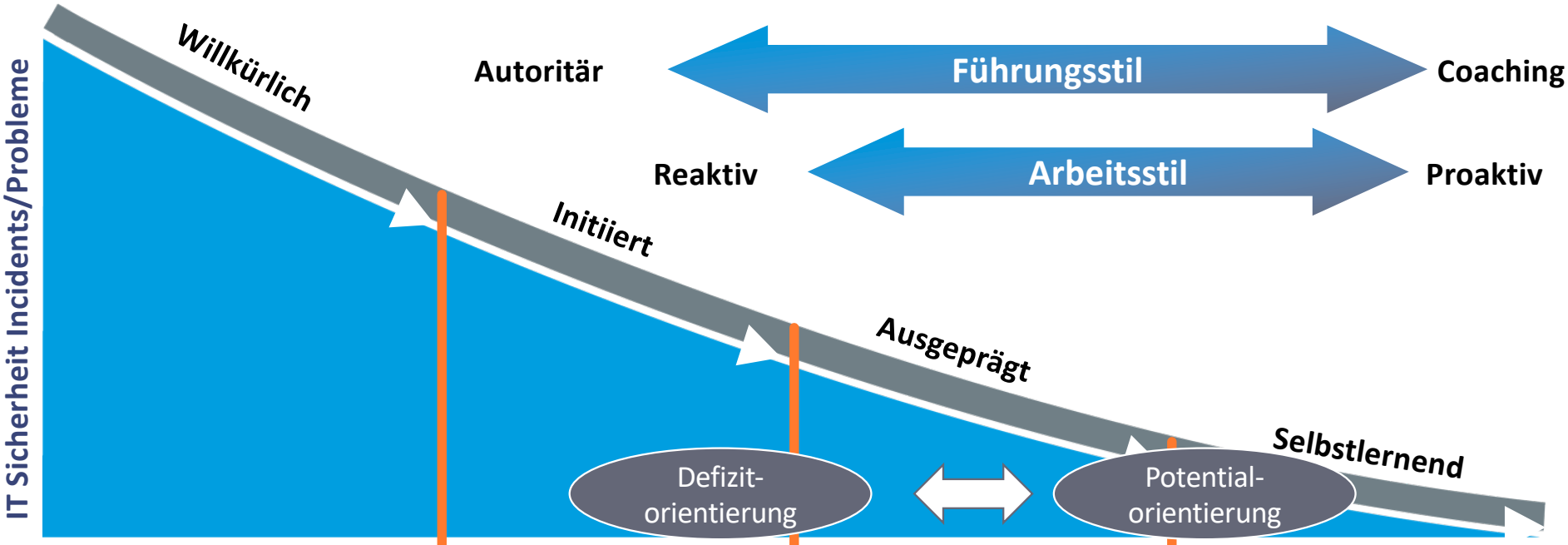
Vernetzen

Community

Verbände oder Arbeitskreise


PLATTFORM
INDUSTRIE 4.0
ERGEBNISPAPIER
Industrie 4.0-Security in der
Aus- und Weiterbildung
Neue Aspekte für Unternehmensorganisation und Kompetenzen

Schlüsselfaktor Unternehmenskultur



- Fehlendes Bewusstsein für ITS in der Organisation.
- ITS ist nicht definiert.
- Willkürliche Behandlung von IS-Vorfällen.
- Verantwortungen sind verwaist und Prozesse willkürlich gestaltet.
- ITS-Bewusstsein individuell.

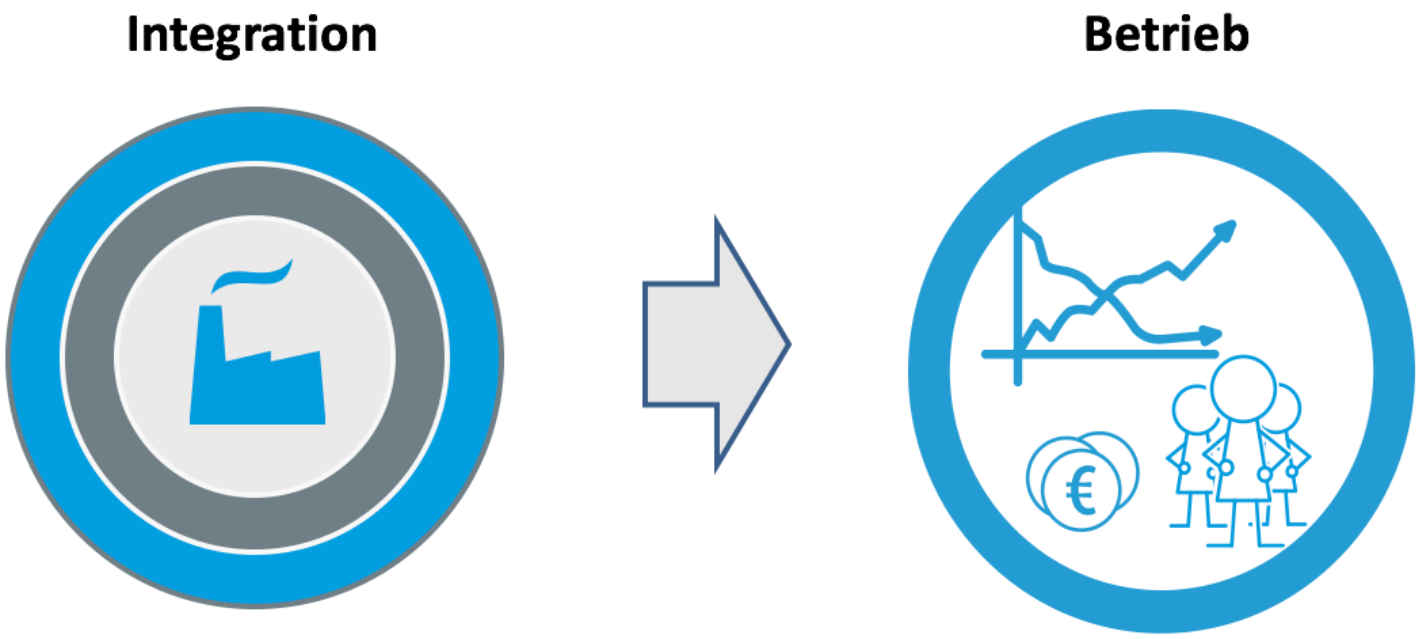
- Management zeigt Engagement.
- Schutzziele der ITS sind festgelegt (Leitlinie).
- Gelenkte Behandlung von ITS-Vorfällen.
- ITS ist in Teilen organisiert.
- IS-Bewusstsein wächst.
- Anlassbezogene Überprüfungen.

- Management gestaltet ITS
- IT Sicherheitsverantwortlicher wirkt als interner Berater.
- Ein ISMS wird erfolgreich betrieben.
- Proaktive Bewusstseinsbildung.
- Wirksamkeitsmessung

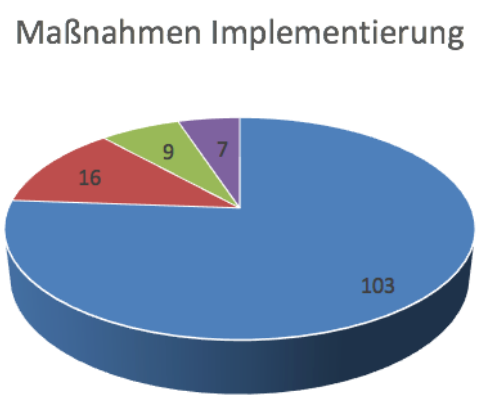
- Die Organisation lebt ITS.
- Externe sind nahtlos ins ISMS integriert.
- Resilienz stark ausgeprägt.
- Autonomes Anpassen an neue Gegebenheiten.
- Zukunftsorientierte Gestaltung.

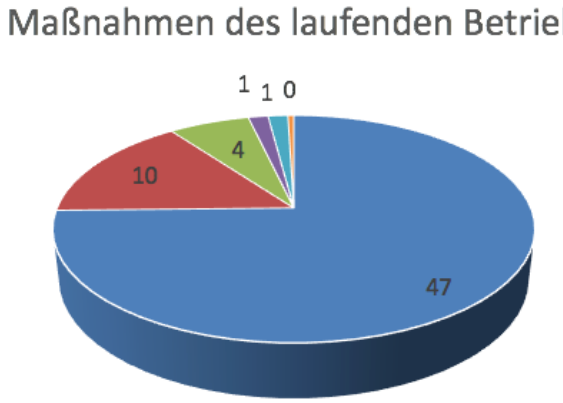
Ressourcen & Aufwendungen Industrial Security?

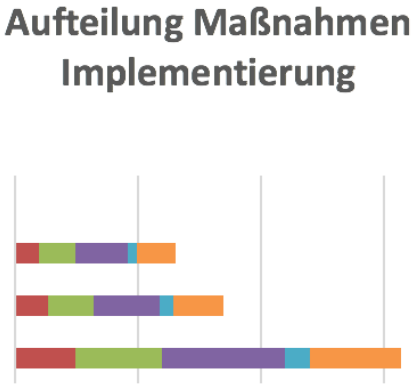
Kappa & Ressourcen-Bedarf Industrial Security ermitteln



notwendige Kappa & Ressourcen-Bedarfsanalyse für die Aufstellung der Organisation...







leider nicht mehr weiter verfolgt interessante Aspekte

notwendige Kappa & Ressourcen-Bedarfsanalyse für die Aufstellung der Organisation...

Produktionsbereich	Personalbedarf im 1. Jahr in Personentage (PT)	Anteil einer Vollzeitkraft im 1. Jahr (PT /205 Arbeitstage pro Jahr)	Personalbedarf im Folgejahr in Personentage (PT)	Anteil einer Vollzeitkraft in den Folgejahren (PT /205 Arbeitstage pro Jahr)	Aufwände von Dritten (PT)	Personalaufwand für Schulung pro Jahr
Schokolinsen – grün	11	0,05	84	0,41		
Schokolinsen – rot	22	0,05	118	0,41		
Schokolinsen – gelb	33	0,16	152	0,74		
Schokolinsen – gelb	43	0,21	182	0,89		
Schokolinsen – gelb	53	0,26	212	1,03		
0	0	0,00	0	0,00		
0	0	0,00	0	0,00		
0	0	0,00	0	0,00

Was sind wesentliche Prozesse im Kontext Security & wie werden diese organisiert?

Big Picture ganzheitlicher Ansatz

Analyse Geschäftsprozesse

Geschäfts-prozess 1 | Geschäfts-prozess 2 | Geschäfts-prozess 3 | Geschäfts-prozess 4 | Geschäfts-prozess 5 | Geschäfts-prozess 6

Verfahrensprozess Produktionsprozess

Ermitteln Maximum tolerable period of disruption (MTPD)

Ermitteln Recovery Time Objective (RTO)

Identifikation notwendiger Services

Produktions-services | Produktions-logistik | Produktions-steuerung | Energie-management

Service- und Funktionsebene

Zuordnung IT- und OT Systeme

Systemebene

Sicherheitsmanagement Systeme

Informationssicherheit – Datenschutz – Kontinuität der Geschäftsprozesse

Einleitung

Sicherheits-Management-Systeme sichern den Fortbestand des Unternehmens und schützen Unternehmenswerte in den Bereichen:

- der Informationssicherheit
- des Datenschutzes
- der Kontinuität der Geschäftsprozesse.

Die Sicherheits-Management-Systeme der Unternehmen sind sehr unterschiedlich ausgestaltet und müssen sich an die unterschiedlichsten Anforderungen aus der jeweiligen Branche, dem Geschäftsmodell, der Organisationsstruktur, der Kunden und Lieferanten angepasst werden müssen. Darüber hinaus hat die Unternehmenskultur-/ und Strategie einen hohen Einfluss auf die Gestaltung eines Sicherheits-Management-Systems.

Für jedes Sicherheits-Management-Systems sind Normen entwickelt worden, die für die Planung, Umsetzung, Betrieb und Weiterentwicklung einen Mindeststandard sicherstellen und trotzdem den Unternehmen die Möglichkeit geben, sie an ihre unternehmensspezifischen Anforderungen anzupassen:

- ISO 27001 Information Security Management System (ISMS)
- ISO 27701 Datenschutz Management System (DMS)
- ISO 22301 Business Continuity Management System (BCMS).

Gesetzliche Verantwortlichkeit

1

Sicherheits-Management-Systeme unterstützen die Geschäftsführung dabei, ihre gesetzlich vorgeschriebenen Verantwortlichkeiten umzusetzen und Haftungsrisiken zu reduzieren.

ISO 27001
-> Kapitel: 4.2 -> Verstehen der Erfordernisse und Erwartungen interessierter Parteien
-> Kapitel: 4.3 -> Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems
-> A.18.1 -> Einhaltung gesetzlicher und vertraglicher Anforderungen

- Gesetz zur Kontrolle und Transparenz im Unternehmensbereich" (KonTraG)
  Risikomanagement für das gesamte Unternehmen

- GmbH-Gesetz und HGB
  Sorgfaltspflicht: Die Geschäftsführer haben die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden.
  Internes Kontrollsystem (IKS): Sicherung und Schutz des Unternehmens

- HGB

  Grundsätze ordnungsmäßiger Buchführung: Namentlich sind alle vorhersehbaren Risiken und Verluste zu berücksichtigen.

Schutz der Unternehmenswerte

2

Sicherheits-Management-Systeme schützen Unternehmenswerte wie IT-Systeme, personenbezogene Daten, Geschäftsprozesse.

ISO 27001
-> Kapitel: 4.2 -> Verstehen der Erfordernisse und Erwartungen interessierter Parteien
-> Kapitel: 4.3 -> Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems

Information Security Management System (ISMS)

IT-Systeme:
- Hardware
- Rechnerräume
- Zutritt zu Gebäuden
- …

Datenschutz Management System (DMS)

Personenbezogener Daten:
- Kundendaten
- Abrechnungsdaten
- Zugriff auf Daten
- …

Business Continuity Management System (BCMS)

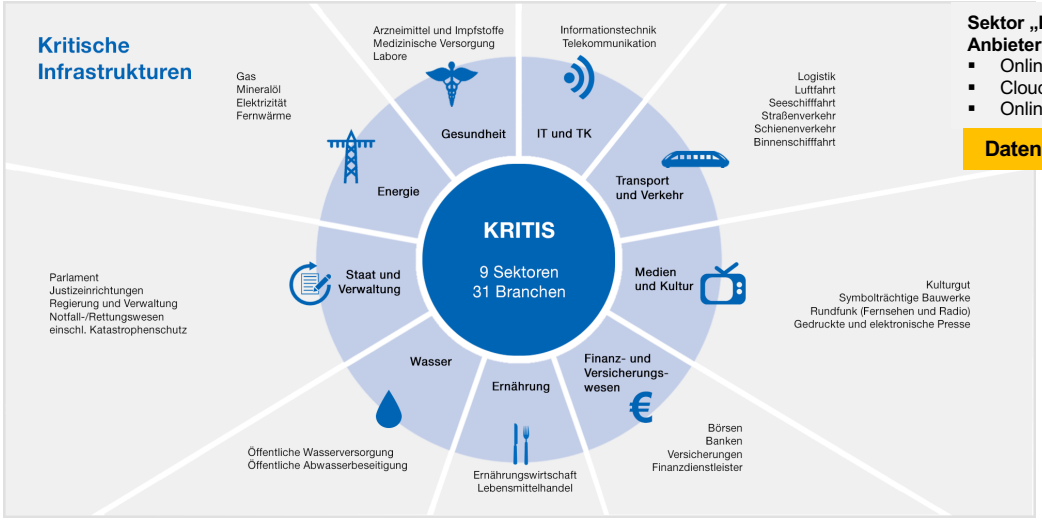
Geschäftsprozesse:
- Auftragsannahme
- Versand
- Rechnungserstellung
- …

Kritische Infrastruktur

3

Sicherheits-Management-Systeme sind für Unternehmen die Teil der Kritischen Infrastruktur inkl. der gesamten Lieferkette gesetzlich vorgeschrieben (IT-Sicherheitsgesetz und der KRITIS-Verordnung).

ISO 27001
-> Kapitel: 4.2 -> Verstehen der Erfordernisse und Erwartungen interessierter Parteien
-> Kapitel: 4.3 -> Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems
-> A.18.1 -> Einhaltung gesetzlicher und vertraglicher Anforderungen

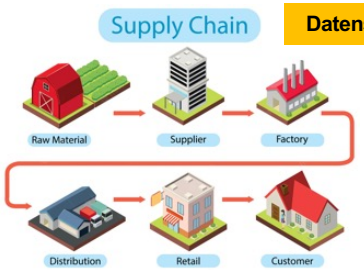


Sektor „IT und TK“:
Anbieter digitaler Dienste
- Online-Suchmaschinen
- Cloud-Computing-Dienste
- Online-Marktplätze

Datenschutz

Datenschutz

Datenschutz



EU-Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie) national IT-Sicherheitsgesetz

Internes Kontrollsystem

4 Sicherheits-Management-Systeme sind Teil des Internen Kontrollsystem (IKS) mit dem Ziel, Unternehmensrisiken zu reduzieren.

ISO 27001
-> Kapitel: 4.2 -> Verstehen der Erfordernisse und Erwartungen interessierter Parteien
-> Kapitel: 4.3 -> Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems
-> Kapitel: 4.4 -> Informationssicherheitsmanagementsystem
-> A.18.1 -> Einhaltung gesetzlicher und vertraglicher Anforderungen

Geschäftsführer und Vorstände sind gemäß GmbH-Gesetz bzw. AktG verpflichtet dafür zu sorgen, dass „ein den Anforderungen des Unternehmens entsprechendes“ ***Internes Kontrollsystem (IKS)*** geführt wird.

Ein IKS beinhaltet ein internes Überwachungssystem zur Sicherstellung der Einhaltung aller Regelungen (Kontrollen) wie z.B. durch Sicherheitsrichtlinien, Sicherheitsbeauftragten, Sicherheitsaudits, interne Revision, ...

Die Ziele sind unter anderem:
- die Einhaltung der für das Unternehmen maßgeblichen rechtlichen Vorschriften und Regelwerke
- die Umsetzung und Einhaltung der unternehmensinternen Grundsätze, Verfahren und Regelungen
- Schutz des Vermögens des Unternehmens, Verhinderung und Aufdeckung von Vermögensschädigungen
- Sicherung der Wirksamkeit und Wirtschaftlichkeit der betrieblichen Prozesse
- Sicherung der im Unternehmen vorhandenen Informationen und Kenntnisse.

zum Beispiel:
- Informationssicherheit
- Datenschutz
- Kontinuität der Geschäftsprozesse
- Handbücher, Leitfäden
- Nachweise, Dokumentationen
- …

Gesetzte im Bereich IT-Sicherheit und Datenschutz

- EU Datenschutz-Grundverordnung (EU-DSGVO)
- EU Network and Information Security Directive (EU-NIS Richtlinie)
- IT-Sicherheitsgesetz (IT SIG), entspricht der EU-NIS Richtlinie, der Geltungsbereich ist national
- Verweis auf den Schutz der Kontinuität der Geschäftsprozesse (BCM)

ISO 27001 Information Security Management System (ISMS)

ISO 27701 Datenschutz Management System (DMS)

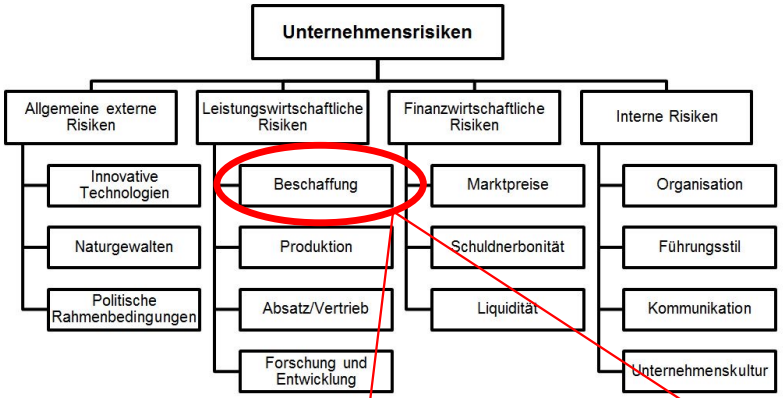
ISO 22301 Business Continuity Management System (BCMS)

Unternehmensrisiken

5

Sicherheits-Management-System müssen sich an den Unternehmensrisiken orientieren. Besonders wichtig ist die Berücksichtigung der Lieferanten außerhalb des europäischen Rechtsraums (Schrems II, Auftragsdatenverarbeitung).

ISO 27001
-> Kapitel: 4.2 -> Verstehen der Erfordernisse und Erwartungen interessierter Parteien
-> Kapitel: 6.1 -> Maßnahmen zum Umgang mit Risiken und Chancen
-> A.18.1 -> Einhaltung gesetzlicher und vertraglicher Anforderungen



- EU Datenschutz-Grundverordnung (EU-DSGVO)
- EU Network and Information Security Directive (EU-NIS Richtlinie)
- IT-Sicherheitsgesetz (IT SIG), entspricht der EU-NIS Richtlinie, der Geltungsbereich ist national
- Verweis auf den Schutz der Kontinuität der Geschäftsprozesse (BCM)

Schrems II / Auftragsdatenverarbeitung:

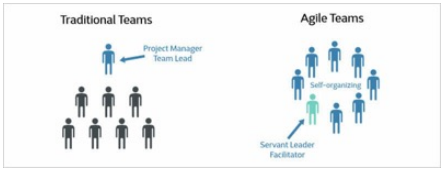
- Transfer personenbezogener Daten aus der EU
- Vereinbarung von Standardvertragsklauseln zur Einhaltung des europäische Datenschutzstandards zwischen Datenexporteuren im Europäischen Wirtschaftsraum und Datenimporteuren in Drittstaaten
- Jedes in der EU ansässige Unternehmen muss diese Risikobewertung beim Übermitteln von Daten in Drittländer durchführen.

Unternehmensstrategie

6

Jedes Unternehmen hat eine andere Unternehmensstrategie. Sicherheits-Management-System müssen in die Unternehmensstrategie durchgängig integriert sein. Dies ist besonders in komplexen / globalen Organisationsstrukturen und internationalen Lieferketten von Bedeutung.

ISO 27001
-> Kapitel: 5.1 -> Führung und Verpflichtung
-> Kapitel: 5.2 -> Politik
-> Kapitel: 5.3 -> Rollen, Verantwortlichkeiten und Befugnisse in der Organisation



Information Security Management System (ISMS)

Datenschutz Management System (DMS)

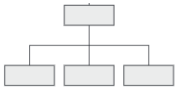
Business Continuity Management System (BCMS)

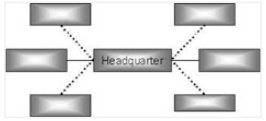
Sicherheitskultur

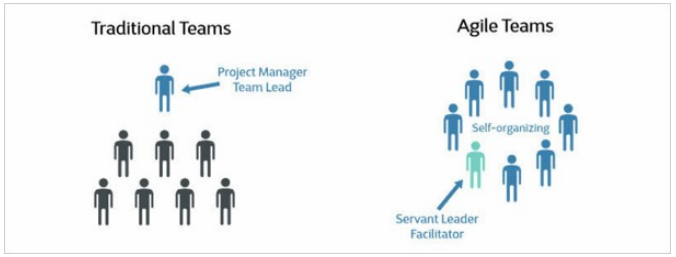
7

Jedes Unternehmen hat eine eigene Sicherheitskultur. Organisationsstruktur und Führungsstruktur des Unternehmens haben maßgeblichen Einfluss auf die Festlegung von Sicherheitsanforderungen und deren Umsetzung und Überwachung durch ein Sicherheits-Management-System.

ISO 27001
-> Kapitel: 5.1 -> Führung und Verpflichtung
-> Kapitel: 5.2 -> Politik
-> Kapitel: 5.3 -> Rollen, Verantwortlichkeiten und Befugnisse in der Organisation







Information Security Management System (ISMS)

Datenschutz Management System (DMS)

Business Continuity Management System (BCMS)

Stakeholder

8

Die Anforderungen der Sicherheits-Management-Systeme müssen die Interessen und Erwartungen der unterschiedlichen Interessen-/ Zielgruppen (Stakeholder) beachten.

ISO 27001
-> Kapitel: 4.2 -> Verstehen der Erfordernisse und Erwartungen interessierter Parteien

- Behörden
- Banken
- Versicherung

- Geschäftsführung
- Anteilseigner

- Kunden
- Lieferanten
- Partner

- unternehmensweite Sicherheitsgrundsätze
- themenspezifische Sicherheitsanforderungen
- Handbücher für ISMS, DMS, BCMS
- Anweisungen, Guidelines, Formulare
- Zertifikate, interne Audits, Nachweise
- Nachweis der Compliance

- IT-Abteilung
- IT-Betrieb
- IT-Entwicklung

- Personalabteilung
- Finanzabteilung
- Einkaufsabteilung
- Vertrieb

- Sicherheitsbeauftragter
- Datenschutzbeauftragter
- Brandschutzbeauftragter

- Gebäudemanager
- Haustechnik
- Gärtner
- Betriebsrestaurant

Regelwerke und rechtliche Vorgaben

9

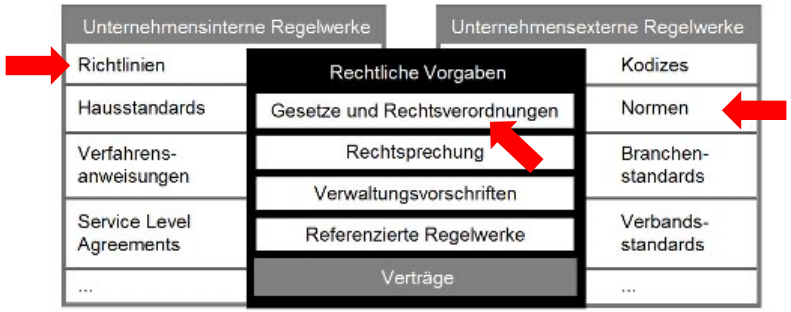
Sicherheits-Management-System müssen interne & externe Regelwerke und rechtliche Vorgaben an IT-Sicherheit, Datenschutz, BCM nachweisbar umsetzten. Dabei müssen alle Lieferanten auch außerhalb des europäischen Rechtsraums berücksichtigt werden (Schrems II, Auftragsdaten-verarbeitung).

ISO 27001
-> Kapitel: 4.2 -> Verstehen der Erfordernisse und Erwartungen interessierter Parteien
-> Kapitel: 4.4 -> Informationssicherheitsmanagementsystem
-> A.18.1 -> Einhaltung gesetzlicher und vertraglicher Anforderungen

ISO 27001
Information Security
Management System (ISMS)

ISO 27701
Datenschutz Management
System (DMS)

ISO 22301
Business Continuity
Management System (BCMS)



Gesetzte im Bereich IT-Sicherheit und Datenschutz

- EU Datenschutz-Grundverordnung (EU-DSGVO)
- EU Network and Information Security Directive (EU-NIS Richtlinie)
- IT-Sicherheitsgesetz (IT SIG), entspricht der EU-NIS Richtlinie - national
- Verweis auf den Schutz der Kontinuität der Geschäftsprozesse (BCM)

Schrems II / Auftragsdatenverarbeitung:

- Transfer personenbezogener Daten aus der EU
- Vereinbarung von Standardvertragsklauseln zur Einhaltung des europäische Datenschutzstandards zwischen Datenexporteuren im Europäischen Wirtschaftsraum und Datenimporteuren in Drittstaaten
- Jedes in der EU ansässige Unternehmen muss diese Risikobewertung beim Übermitteln von Daten in Drittländer durchführen.

Zertifizierung

10 Eine erfolgreiche Umsetzung eines Sicherheits-Management-Systems kann mittels einer Zertifizierung allgemeingültig nachgewiesen werden.

ISO 27001
-> Kapitel: 4.2 -> Verstehen der Erfordernisse und Erwartungen interessierter Parteien
-> A.18.1 -> Einhaltung gesetzlicher und vertraglicher Anforderungen

- Die Anforderungen an ein Sicherheits-Management-System sind in internationalen Normen beschrieben.
- Sie bilden einen Rahmen für die Planung, Umsetzung, Überwachung und Verbesserung eines Sicherheits-Management-Systems. Die Normen lassen ganz bewusst Freiräume zur operativen Ausgestaltung und Umsetzung zu.
- Die konkrete operative Umsetzung richtet sich nach der Zielsetzung des jeweiligen Unternehmens, welches mit der Umsetzung des Sicherheits-Management-Systems verfolgt wird.
- Auch Non-Profitorganisationen oder öffentlichen Institutionen können sich zertifizieren lassen.
- Zertifizierungen dürfen nur von akkreditierten Dienstleistern wie z.B. TÜV oder DEKRA ausgeführt werden.
- Die Vorbereitung, Planung, Durchführung und Nachbereitung ist mit organisatorischen, personellen und monetären Aufwänden verbunden.
- Zertifizierungen müssen in regelmäßigen Abständen erneuert werden.

Vorteile einer Zertifizierung

- Nachweis der Compliance
- Minimierung von Haftungsrisiken
- Minimierung von Geschäftsrisiken
- Senkung von Versicherungsprämien
- Optimierung von Prozess- und IT-Kosten (angemessene Sicherheit)
- Steigerung der Wettbewerbsfähigkeit
- Schaffung von Vertrauen bei Kunden, Geschäftspartnern und in der Öffentlichkeit
- Bedrohungen im Unternehmen zuverlässig erkennen und reduzieren
- Schnellere Wiederherstellung von Prozessen und Systemen bei eingetretenen Unterbrechungen
- Schutz von vertraulichen Daten vor Missbrauch, Verlust und Offenlegung

Information Security Management System (ISMS)	ISO 27001
Datenschutz Management System (DMS)	ISO 27701
Business Continuity Management System (BCMS)	ISO 22301

ISO International Organization for Standardization

K4

Integriertes Security Management System

Sicherheits-Management-Systeme können einzeln aufgebaut und betrieben werden, oder - je nach Erfordernisse - im Verbund als „integriertes Security Management System" (iSMS) nach einem übergeordneten zentralen Regelwerk.

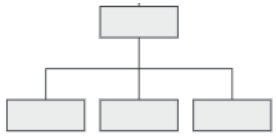
ISO 27001
-> Kapitel: 4.4 -> Informationssicherheitsmanagementsystem
-> Kapitel: 5.1 -> Führung und Verpflichtung
-> Kapitel: 5.2 -> Politik
-> Kapitel: 5.3 -> Rollen, Verantwortlichkeiten und Befugnisse in der Organisation

Information Security Management System (ISMS)

Datenschutz Management System (DMS)

Business Continuity Management System (BCMS)

je nach Erfordernisse



integriertes Security Management System (iSMS)

Zentrales Regelwerk

Information Security Management System (ISMS)

Datenschutz Management System (DMS)

Business Continuity Management System (BCMS)

Anforderungen an SMS

12 Die Anforderungen an Sicherheits-Management-Systeme können sich ändern und müssen regelmäßig überprüft und ggf. angepasst werden. Beispiele für Änderungen: Geschäftsmodell, Unternehmensstrategie, Kunden, Auftraggeber, Märkte.

ISO 27001
-> Kapitel: 4.2 -> Verstehen der Erfordernisse und Erwartungen interessierter Parteien
-> A.18.1 -> Einhaltung gesetzlicher und vertraglicher Anforderungen

wenn Teil der Kritischen Infrastruktur

- interner Vorgaben
- interne Prüfungen

- normative Vorgaben
- interne Audits

- interner Vorgaben
- interne Prüfungen

- normative Vorgaben
- externe Zertifizierungen

- normative Vorgaben
- interne Audits

- interner Vorgaben
- interne Prüfungen

IST → Soll

IST → Soll

Aufwand

Dokumentenmanagementsystem

13

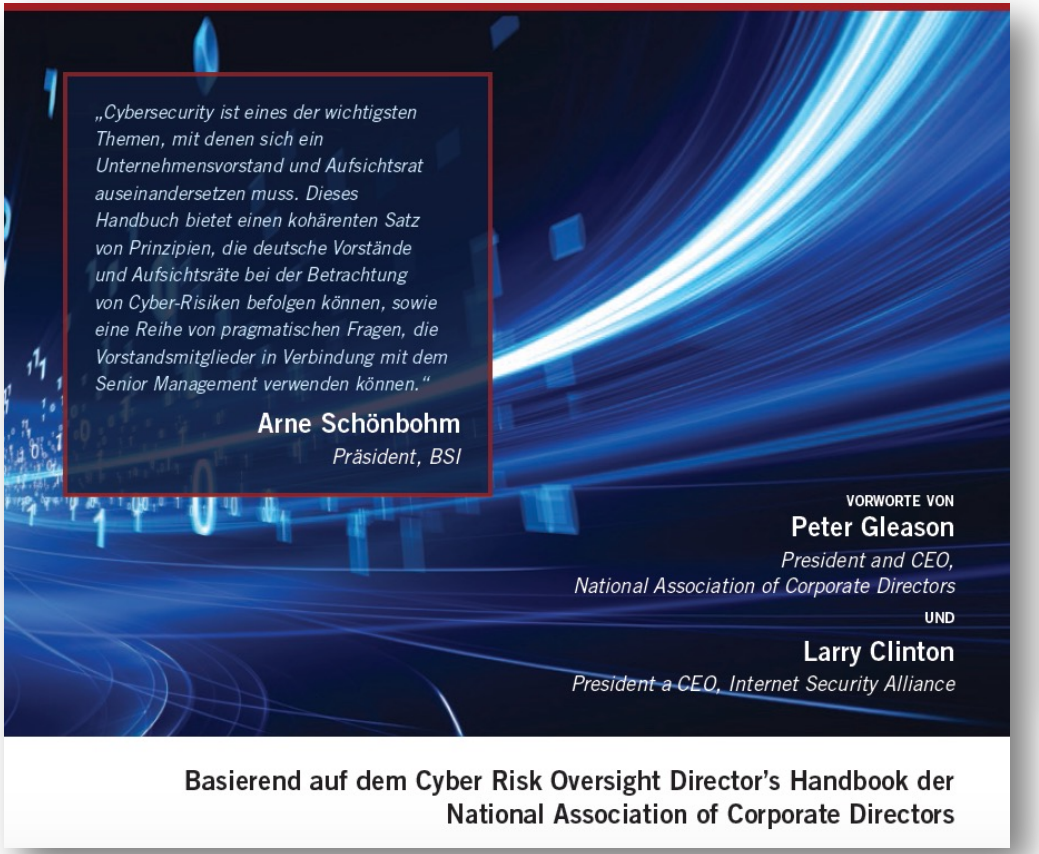
Die Umsetzung der Sicherheits-Management-Systeme muss in einem Dokumenten-managementsystem für die Interessen-/ Zielgruppen (Stakeholder) stets aktuell nachweisbar sein.

ISO 27001
-> Kapitel: 4.3 -> Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems
-> Kapitel: 4.4 -> Informationssicherheitsmanagementsystem

- unternehmensweite Sicherheitsgrundsätze
- themenspezifische Sicherheitsanforderungen
- Handbücher für ISMS, DMS, BCMS
- Anweisungen, Guidelines, Formulare
- Zertifikate, interne Audits, Nachweise
- Nachweis der Compliance

- Geschäftsführung
- Anteilseigner
- Behörden
- Banken
- Versicherung
- Kunden
- Lieferanten
- Partner
- Mitarbeiter
- …

Unternehmens-Risikomanagement



Mit Unterstützung von:

AIG

Allianz für Cyber-Sicherheit

INTERNET SECURITY ALLIANCE

Management von Cyber-Risiken:

Handbuch für Unternehmensvorstände und Aufsichtsräte

Best Practice - Notfallmanagement

VERHALTEN BEI IT-NOTFÄLLEN

Ruhe bewahren & IT-Notfall melden
Lieber einmal mehr als einmal zu wenig anrufen!

IT-Notfallrufnummer:

Wer meldet?

Welches IT-System ist betroffen?

Wie haben Sie mit dem IT-System gearbeitet?
Was haben Sie beobachtet?

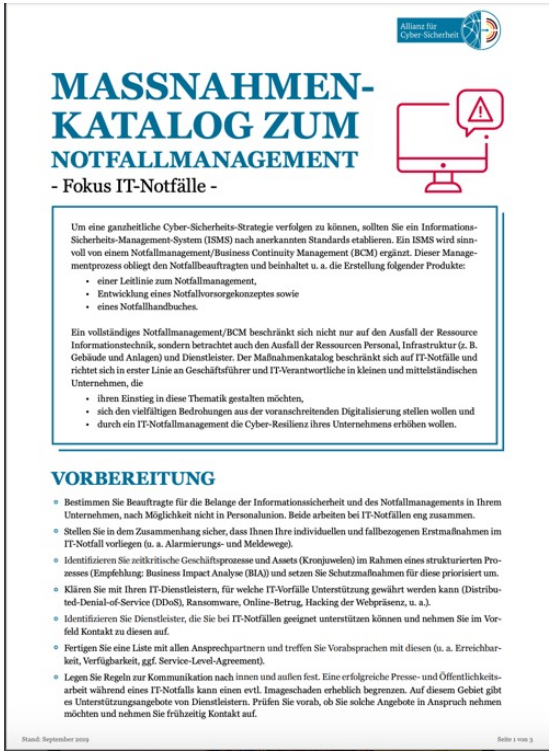
Wann ist das Ereignis eingetreten?

Wo befindet sich das betroffene IT-System?
(Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

Weitere Arbeit am IT-System einstellen | Beobachtungen dokumentieren | Maßnahmen nur nach Anweisung einleiten

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik



Allianz für Cyber-Sicherheit

MASSNAHMEN-KATALOG ZUM NOTFALLMANAGEMENT

- Fokus IT-Notfälle -

Um eine ganzheitliche Cyber-Sicherheits-Strategie verfolgen zu können, sollten Sie ein Informations-Sicherheits-Management-System (ISMS) nach anerkannten Standards etablieren. Ein ISMS wird sinnvoll von einem Notfallmanagement/Business Continuity Management (BCM) ergänzt. Dieser Managementprozess obliegt den Notfallbeauftragten und beinhaltet u. a. die Erstellung folgender Produkte:

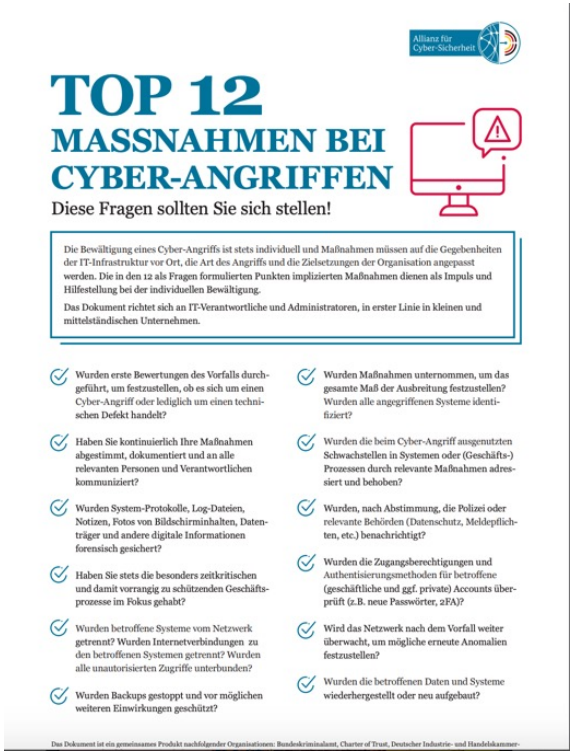
- einer Leitlinie zum Notfallmanagement,
- Entwicklung eines Notfallvorsorgekonzeptes sowie
- eines Notfallhandbuches.

Ein vollständiges Notfallmanagement/BCM beschränkt sich nicht nur auf den Ausfall der Ressource Informationstechnik, sondern betrachtet auch den Ausfall der Ressourcen Personal, Infrastruktur (z. B. Gebäude und Anlagen) und Dienstleister. Der Maßnahmenkatalog beschränkt sich auf IT-Notfälle und richtet sich in erster Linie an Geschäftsführer und IT-Verantwortliche in kleinen und mittelständischen Unternehmen, die

- ihren Einstieg in diese Thematik gestalten möchten,
- sich den vielfältigen Bedrohungen aus der voranschreitenden Digitalisierung stellen wollen und
- durch ein IT-Notfallmanagement die Cyber-Resilienz ihres Unternehmens erhöhen wollen.

VORBEREITUNG

- Bestimmen Sie Beauftragte für die Belange der Informationssicherheit und des Notfallmanagements in Ihrem Unternehmen, nach Möglichkeit nicht in Personalunion. Beide arbeiten bei IT-Notfällen eng zusammen.
- Stellen Sie in dem Zusammenhang sicher, dass Ihnen Ihre individuellen und fallbezogenen Erstmaßnahmen im IT-Notfall vorliegen (u. a. Alarmierungs- und Meldewege).
- Identifizieren Sie zeitkritische Geschäftsprozesse und Assets (Kronjuwelen) im Rahmen eines strukturierten Prozesses (Empfehlung: Business Impact Analyse (BIA)) und setzen Sie Schutzmaßnahmen für diese priorisiert um.
- Klären Sie mit Ihren IT-Dienstleistern, für welche IT-Vorfälle Unterstützung gewährt werden kann (Distributed-Denial-of-Service (DDoS), Ransomware, Online-Betrug, Hacking der Webpräsenz, u. a.).
- Identifizieren Sie Dienstleister, die Sie bei IT-Notfällen geeignet unterstützen können und nehmen Sie im Vorfeld Kontakt zu diesen auf.
- Fertigen Sie eine Liste mit allen Ansprechpartnern und treffen Sie Vorabsprachen mit diesen (u. a. Erreichbarkeit, Verfügbarkeit, ggf. Service-Level-Agreement).
- Legen Sie Regeln zur Kommunikation nach innen und außen fest. Eine erfolgreiche Presse- und Öffentlichkeitsarbeit während eines IT-Notfalls kann einen evtl. Imageschaden erheblich begrenzen. Auf diesem Gebiet gibt es Unterstützungsangebote von Dienstleistern. Prüfen Sie vorab, ob Sie solche Angebote in Anspruch nehmen möchten und nehmen Sie frühzeitig Kontakt auf.



Allianz für Cyber-Sicherheit

TOP 12 MASSNAHMEN BEI CYBER-ANGRIFFEN

Diese Fragen sollten Sie sich stellen!

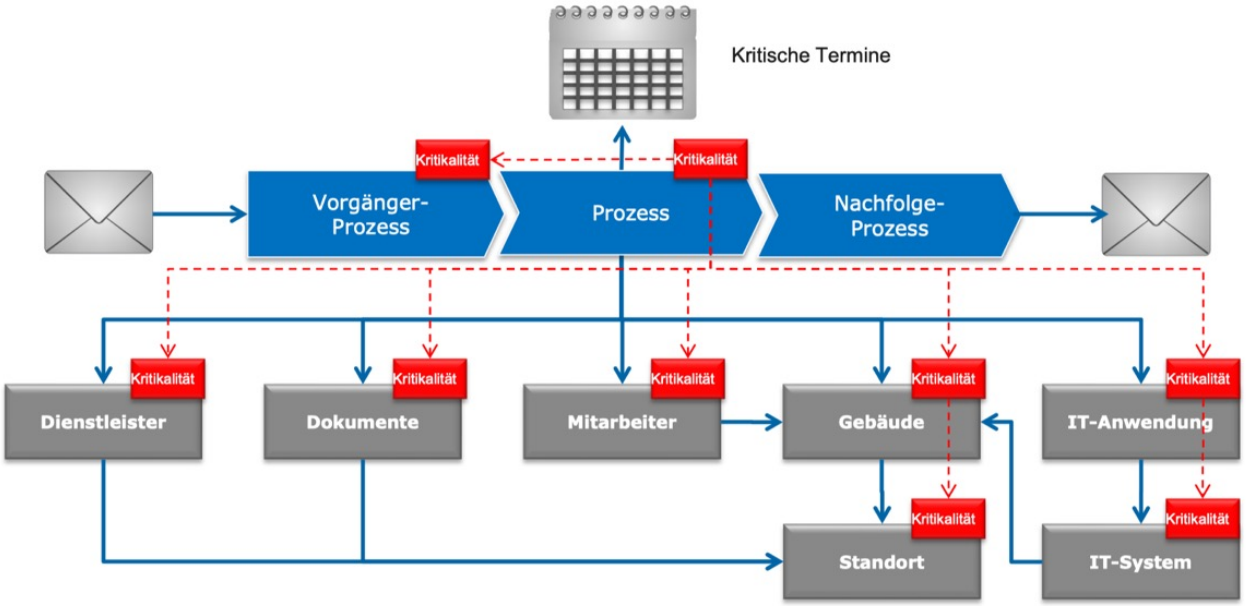
Die Bewältigung eines Cyber-Angriffs ist stets individuell und Maßnahmen müssen auf die Gegebenheiten der IT-Infrastruktur vor Ort, die Art des Angriffs und die Zielsetzungen der Organisation angepasst werden. Die in den 12 als Fragen formulierten Punkten implizierten Maßnahmen dienen als Impuls und Hilfestellung bei der individuellen Bewältigung.

Das Dokument richtet sich an IT-Verantwortliche und Administratoren, in erster Linie in kleinen und mittelständischen Unternehmen.

- Wurden erste Bewertungen des Vorfalls durchgeführt, um festzustellen, ob es sich um einen Cyber-Angriff oder lediglich um einen technischen Defekt handelt?
- Haben Sie kontinuierlich Ihre Maßnahmen abgestimmt, dokumentiert und an alle relevanten Personen und Verantwortlichen kommuniziert?
- Wurden System-Protokolle, Log-Dateien, Notizen, Fotos von Bildschirminhalten, Datenträger und andere digitale Informationen forensisch gesichert?
- Haben Sie stets die besonders zeitkritischen und damit vorrangig zu schützenden Geschäftsprozesse im Fokus gehabt?
- Wurden betroffene Systeme vom Netzwerk getrennt? Wurden Internetverbindungen zu den betroffenen Systemen getrennt? Wurden alle unautorisierten Zugriffe unterbunden?
- Wurden Backups gestoppt und vor möglichen weiteren Einwirkungen geschützt?
- Wurden Maßnahmen unternommen, um das gesamte Maß der Ausbreitung festzustellen? Wurden alle angegriffenen Systeme identifiziert?
- Wurden die beim Cyber-Angriff ausgenutzten Schwachstellen in Systemen oder (Geschäfts-) Prozessen durch relevante Maßnahmen adressiert und behoben?
- Wurden, nach Abstimmung, die Polizei oder relevante Behörden (Datenschutz, Meldepflichten, etc.) benachrichtigt?
- Wurden die Zugangsberechtigungen und Authentisierungsmethoden für betroffene (geschäftliche und ggf. private) Accounts überprüft (z.B. neue Passwörter, 2FA)?
- Wird das Netzwerk nach dem Vorfall weiter überwacht, um mögliche erneute Anomalien festzustellen?
- Wurden die betroffenen Daten und Systeme wiederhergestellt oder neu aufgebaut?

Business Continuity Management

Welche Ressourcen benötigt der Geschäftsprozess für dessen Durchführung?



Die BIA identifiziert die kritischen Prozess-Ressourcen. Dieser erben die Kritikalität aus den Prozessen

Vorgehensmodell ISMS Einführung

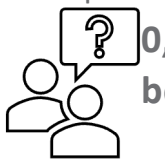
Grundlagen → Analyse → Risiken & Maßnahmen → Überprüfen

Ziele
- Leadership & Commitment
- Stakeholder identifizieren
- Sicherheitsziele definieren
- Sicherheitsleitlinie erstellen
- Geltungsbereich bestimmen und dokumentieren
- Verantwortlichkeiten definieren
- Formaler Rahmen bestimmen

Ziele
- Prozesse identifizieren und dokumentieren
- Schadensanalyse
- Werte strukturieren

Ziele
- Gefahren und Bedrohungen bestimmen
- Risiken identifizieren
- Maßnahmen ableiten und priorisieren

Ziele
- KPI definieren
- Maßnahmen überprüfen
- Wirksamkeit feststellen
- Management einbinden

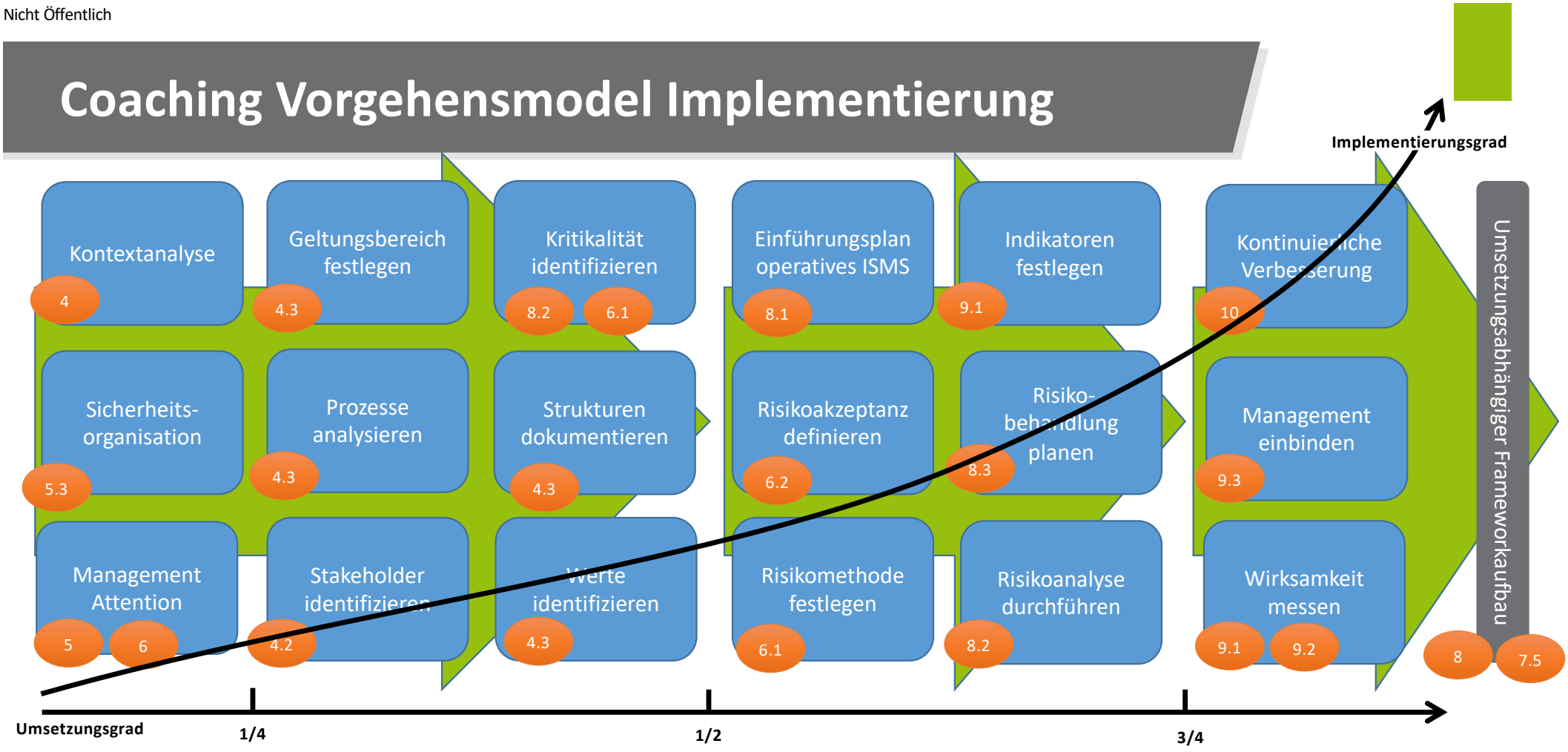


0,5 – 1 FTE-Aufbau 1,5-2 Jahre / je nach Geltungs-bereich Zertifizierungsoption ca. 12-15 Monate

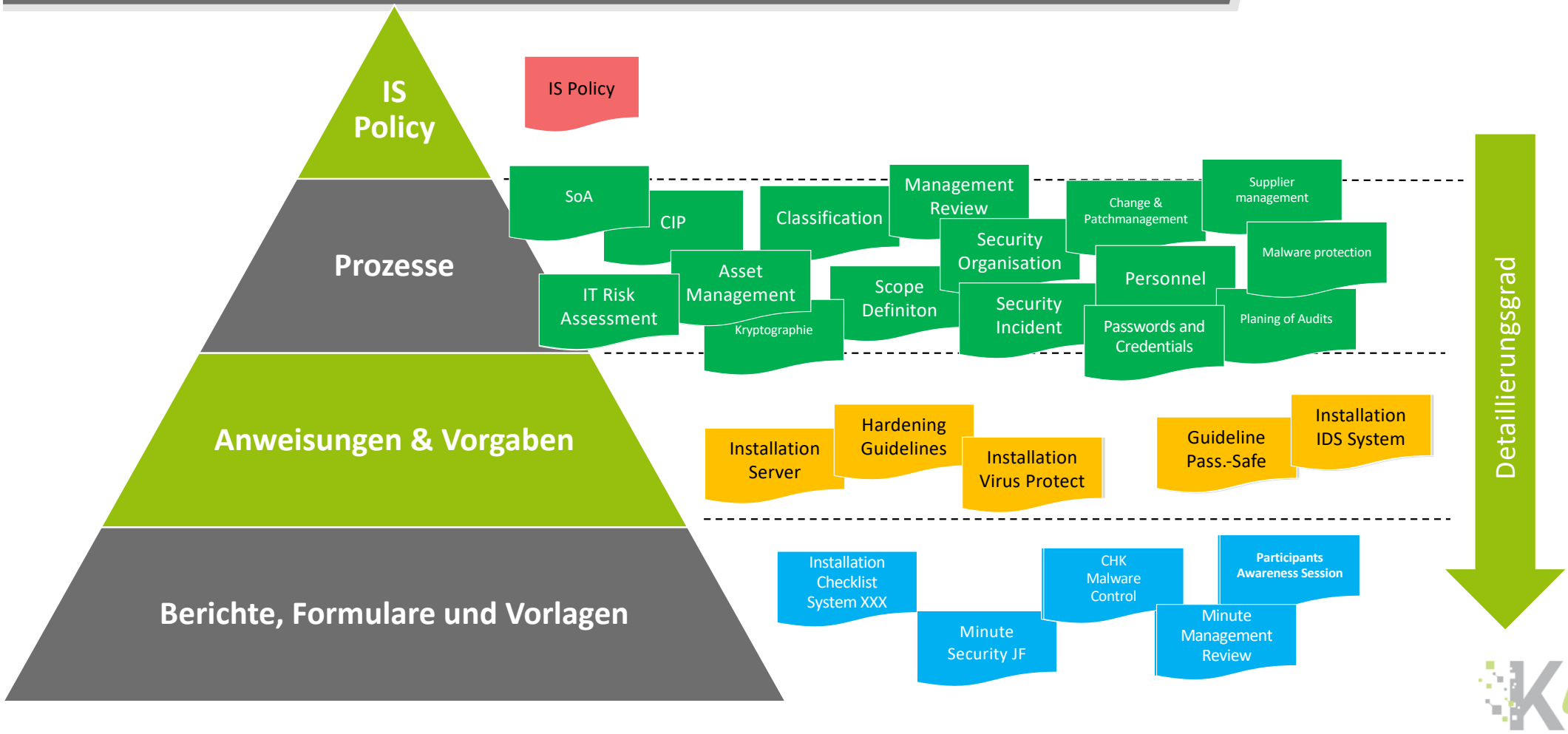
Informationssicherheit Überwachen und Steuern

M0 M1 M2 M3 M4 M5

Coaching Vorgehensmodel Implementierung



Dokumente & Prozesse ISMS



Erstellung von Dokumenten & Prozessbeschreibungen im Kontext ISMS

Mindestens folgende Dokumente zu folgenden Themen:

Leitlinie für Informationssicherheit

Definition und Beschreibung des Geltungsbereichs des ISMS (Information Security Management System)

Security Organisation mit Einbeziehung von Datenschutz und QM

Security Monitoring

Schutz vor Malware

Kryptographie

Methode der Risikoanalyse

Sicherheitsarchitektur (Netzwerk- Plattform und Applikationssicherheit

Folgende Prozesse

Asset Management

Risikomanagement

Informationsklassifizierung

Planung und Durchführung von Audits

Security Incident Handling

Notfallmanagement

Change und Patch Management

Projektdurchführung mit Beschaffung und Entwicklung

Verwaltung von Passwörtern und Credentials

Prozesse der Public Key Infrastructure (PKI)

Lizenzmanagement

Benutzer- und Rechteverwaltung

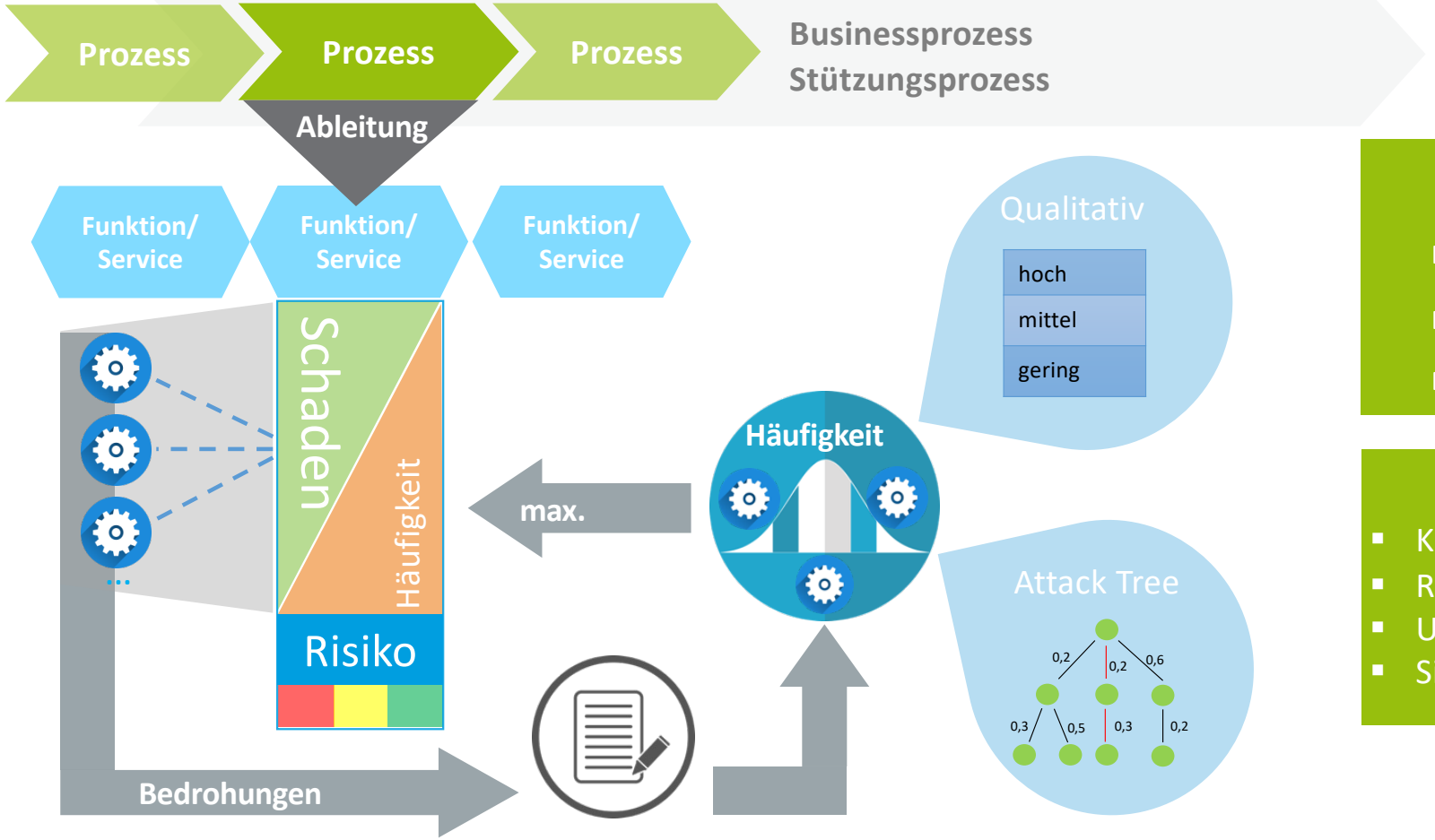
Sicherheit beim Personal

Schulung/Awareness

Lieferantenmanagement

müssen erstellt und über eine Dokumentenlenkung gesteuert werden.

Vorgehen Risikoanalyse



INPUT

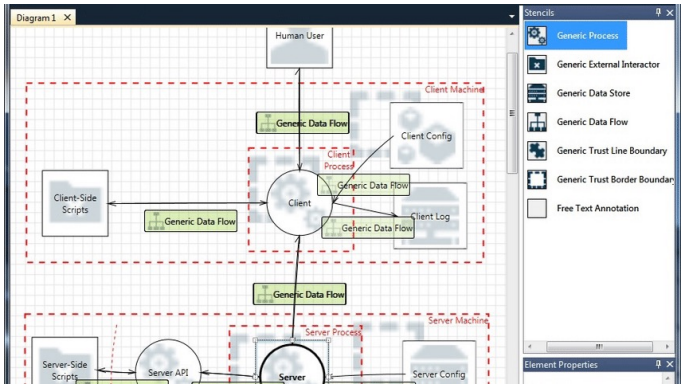
- Business Impact Analyse
- Bedrohungskatalog
- Eintrittswahrscheinlichkeit

OUTPUT

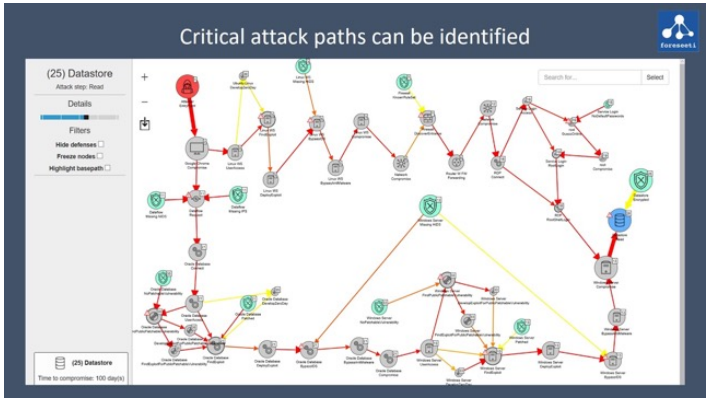
- Kritische Komponenten
- Risiken
- Umzusetzende Maßnahmen
- Sicherheitskonzept

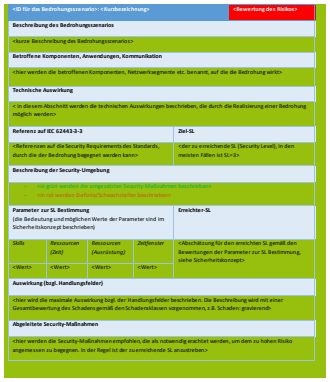
Risiko & Bedrohungsanalyse Methodik?

Microsoft Thread Modeling Tool



SecuriCAD Attack-Trees





IEC 62443 klassisch

Parameter	Wertebereich	Definition	SL
keine	keine	Beiläufige oder zufällige Verletzung der Informationssicherheit.	1
Wissen	generisch	Detailliertes Wissen über die Sicherheit, der Domäne oder dem spezifischen System ist nicht notwendig	2
	spezifisch	Spezifisches Wissen über die Sicherheit (z.B. Brechen von kryptographischen Verfahren, Reverse Engineering), der Domäne oder dem spezifischen System ist erforderlich	3,4
Ressource (Zeit)	Niedrig	Minuten bis Stunden	2
	Mittel	Tage	3
	Hoch	Monate	4
Ressource (Ausrüstung)	Niedrig	Keine besondere Ausrüstung notwendig.	2
	Mittel	Der Angreifer greift auf Exploits im Betriebssystem zurück, welche nicht weitreichend bekannt sind. Er nutz Cracking-Tools für Passwörter und Schlüssel und kann auf Hash-Tables zurückgreifen.	3
	Hoch	Hochleistungsrechner, Botnetze und Supercomputer werden benutzt.	4
Zeitfenster (notwendige Zeit zur Erkennung eines Angriffs)	Niedrig	Stunden	4
	Mittel	Einige Tage	3
	Hoch	Tage - Wochen	2

Gesamtprozess

Strukturanalyse

- Abgrenzung des Geltungsbereichs
- Erfassung des gesamten OT-Systems im Geltungsbereich
  - Alle Assets erfassen / Zonen & Conduits
  - Alle Kommunikationsverbindungen erfassen
  - Organisationsstrukturen erfassen
    - Aufbauorganisation (Rollen, Verantwortlichkeiten, Hierarchien, etc.)
    - Ablauforganisation (Change-Management, Asset Management, Capacity Management, etc.)
  - Umgesetzte Sicherheitsmaßnahmen erfassen

Bedrohungsanalyse

- Identifizierung der Bedrohungen
  - Bedrohungskatalog
- Anwenden der Bedrohungen auf das System
  - Zonen & Conduits / Assets
  - Kommunikationsverbindungen
  - Organisationsstrukturen und Prozesse

ID	Bedrohungs-szenarien	Gründe und Beispiele	Auswirkungen auf Schutzziele			IEC 62443-3-3 References (STRIDE Category)	Threat categories according to IEC 62443-3
			Vertraulichkeit	Integrität	Verfügbarkeit		
T_IA_4	Ausnutzung von Schwachstellen in Software	▪ Injection-Attacken ▪ Session-Hijacking ▪ Cross-Site-Attacks ▪ Replay-Attacks ▪ Unautorisierte Rechte	X	X	X	SR 2.1, SR 3.8, SR 4.2 / (Tampering/Elevation of Privilege)	System Integrity (SI)
T_IA_5	Manipulation der Kommunikation	▪ Man-in-the-Middle-Angriffe ▪ ARP-Injection ▪ Ein Angreifer erhält Zugriff auf das Rechenzentrum und manipuliert die Hardware, um die Kommunikationsleitungen zu manipulieren	X	X	X	SR 3.1, SR 4.3 / (Repudiation)	System Integrity (SI)

Begrifflichkeiten

- **Conduit**
  Eine logische Gruppierung von Kommunikationskanälen, die gemeinsamen Security-Anforderungen unterliegen und zwei oder mehr Zonen miteinander verbinden.

- **Auswirkung**
  Maß des gesamten Verlusts oder Schadens in Verbindung mit einer Folge.

- **Betrachtetes System (SUC)**
  Eine festgelegte Sammlung von Betriebsmitteln des IACS-, die zur Bereitstellung einer vollständigen Automatisierungslösung benötigt werden, einschließlich der gesamten relevanten Netzinfrastruktur.

- **Zone**
  Eine Gruppierung logischer oder physischer Anlagen auf der Grundlage des Risikos oder anderer Kriterien wie etwa der Kritikalität der Anlagen der Betriebsfunktion, des physischen oder logischen Standorts, des erforderlichen Zugangs (zum Beispiel Prinzip der minimal erforderlichen Rechte) oder der verantwortlichen Organisation.

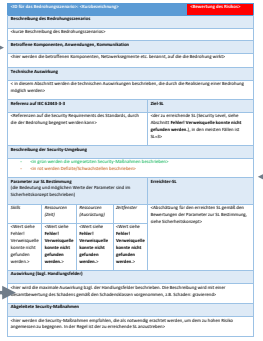
Risikomethode in Anlehnung der Security Level

Abschätzung Wirkungsgrad der umgesetzten Maßnahmen

(Wie stark muss ein Angreifer sein, um den Angriff erfolgreich umzusetzen, unter Berücksichtigung der umgesetzten Maßnahmen.)

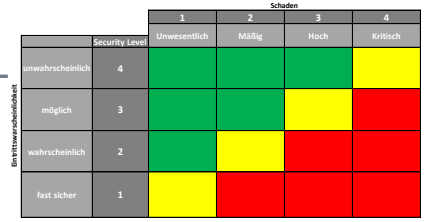
Erreichter SL

Weitere Maßnahmen



Lfd.Nr	Schadenskategorie	Definition Schadensklassen
1	Verstöße gegen Gesetze / Verträge / Vorschriften	**1: Unwesentlich** - keine oder geringe Konventionalstrafen **2: Mäßig** - Mäßige Verstöße oder mäßige Konventionalstrafen **3: Hoch** - Erhebliche Verstöße mit hohen Konventionalstrafen **4: Kritisch** - Fundamentale Verstöße mit existenzbedrohenden Strafen
2	- Beeinträchtigung der Aufgabenerfüllung - Auswirkung auf die Resilienz von Führungs-prozessen	**1: Unwesentlich** - Beeinträchtigung einzelner Mitarbeiter / Tätigkeiten können verschoben werden / keine oder geringe Nacharbeit / behindert die Aufgabenerfüllung nicht / andere Organisationseinheiten, Institutionen oder Externe werden in ihrer Arbeit nicht gestört. **2: Mäßig** - Beeinträchtigung mehrerer Mitarbeitern / andere Tätigkeiten können vorgezogen werden / Nacharbeit behindert die Aufgabenerfüllung nicht merklich / andere Organisationseinheiten, Institutionen oder Externe werden in ihrer Arbeit nicht wesentlich gestört. **3: Hoch** - Nicht tolerierbare Unterbrechungen bzw. Einschränkungen / Minderung der Arbeitsqualität / Fristversäumnisse nach außen wirksam / das Auffholen von Arbeitsrückständen ist nicht innerhalb der normalen Arbeitszeit möglich / andere Organisationseinheiten, Institutionen oder Externe werden in ihrer Arbeit erheblich gestört, auch dort müssen Rückstände aufgeholt werden. **4: Kritisch** - Gravierende Beeinträchtigung der Aufgabenerfüllung / Rückstände können nur mit externer Hilfe oder gar nicht aufgeholt werden / Verzögerte und fehlerhafte Ergebnisse werden extern deutlich bemerkt / schwerwiegende Minderung der Servicequalität.
3	Gefährdung für Leib und Leben / der persönlichen Unversehrtheit	**1: Unwesentlich** – Keine Beeinträchtigung **2: Mäßig** - Bestenfalls geringe Beeinträchtigungen **3: Hoch** - Beeinträchtigungen nicht auszuschließen/meldepflichtige Personenschäden **4: Kritisch** - Gefahr für Leib und Leben
4	Gefährdung für Datensicherheit und Datenschutz durch Offenlegung oder Manipulation	**1: Unwesentlich** - Verstöße ohne Auswirkungen / keine meldepflichtigen Vorfälle **2: Mäßig** - Verstöße mit geringfügigen Konsequenzen oder Konventionalstrafen (z.B. Buß- oder Zwangsgeldstrafungen >= 25000 €) - Verstöße werden außerhalb nicht bemerkt und müssen nicht nach außen gemeldet werden **3: Hoch** - Verstöße mit erheblichen Konsequenzen oder Konventionalstrafen sind abzusehen oder bereits fällig (z.B. Buß- 25.000 und 500.000 €) - Verstöße werden außerhalb bemerkt **4: Kritisch** - Verstöße mit gravierenden Konsequenzen oder Haftungsansprüchen (z.B. Buß- oder Zwangsgeldstrafungen >= 1.000.000 €) - Verstöße müssen außerhalb gemeldet werden
5	Finanzielle Auswirkungen	**1: Unwesentlich –** Geringer finanzieller Schaden < 5.000€ **2: Mäßig** - Finanzieller Schaden 5.000€ - 25.000€ **3: Hoch** - Finanzieller Schaden 25.000€ - 100.000€ **4: Kritisch** - Finanzieller Schaden > 100.000€
6	Negative Außenwirkung (Reputationsschaden)	**1: Unwesentlich** - Ausschließlich interne Auswirkungen **2: Mäßig** - Geringe mediale Außenwirkung **3: Hoch** - Externe, regional begrenzte mediale Außenwirkung (regionale Medien, Politik) **4: Kritisch** - Externe, weit reichende überregionale Außenwirkung (überregionale Medien, Politik)

Ziel SL



Risikoanalyse-Methodik

- Schutzziele:
  - Verfügbarkeit
  - Integrität
  - Vertraulichkeit
- Schadensklassen
  - Niedrig – Mittel
  - Hoch
  - Sehr hoch

Klasse	Erläuterung	
sehr hoch	Vertraulichkeit	Sehr geheime Daten. Diese sind nur einem sehr eingeschränkten Benutzerkreis zugänglich oder werden vom Kunden als besonders vertrauenswürdig eingestuft (z.B. personenbezogene Daten zum Beispiel bei Smartmeter, Rezepturen, Konstruktionspläne etc.).
	Integrität	Nur ein sehr eingeschränkter Personenkreis darf die Änderung dieser Daten veranlassen oder durchführen.
	Verfügbarkeit	Die maximale Wiederanlaufzeit darf **??? Stunden** nicht überschreiten. Die definierte max. kumulierte Ausfallzeit[1] innerhalb eines Quartals darf **??? Stunden / Quartal** nicht überschreiten
	mögliche Folgen eines Verstoßes / einer Verletzung: sehr hohe finanzielle Verluste bis hin zur existentiellen Bedrohung des Geschäftes des Unternehmens, Vertrauensverlust einer sehr breiten Öffentlichkeit Verstoß gegen folgende Gesetze, Verträge **????** (z.B. Datenschutz)	
hoch	Vertraulichkeit	Geheime Daten sind nur einem eingeschränkten Benutzerkreis zugänglich oder werden vom Kunden als vertrauenswürdig eingestuft (z.B. kumulierte Verbrauchsdaten, Konfigurationsdaten, Prozessdaten).
	Integrität	Nur ein eingeschränkter Personenkreis darf die Änderung der Daten veranlassen oder durchführen.
	Verfügbarkeit	Die maximale Wiederanlaufzeit darf **??? Stunden** nicht überschreiten. Die definierte max. kumulierte Ausfallzeit[2] innerhalb eines Quartals darf **??? Stunden / Quartal** nicht überschreiten
	mögliche Folgen eines Verstoßes: hohe finanzielle Verluste, die unter Kontrolle/Verantwortung es Top Management stehen, die in der Bilanz einen deutlichen Niederschlag haben. Eine existentielle Bedrohung des Unternehmens ist nicht absehbar. Vertrauensverlust in einer breiten Öffentlichkeit (z.B. regional, nur in einem Land) Verstoß gegen Gesetze, Verträge **????**	
Niedrig bis mittel	Vertraulichkeit	die Daten sind einem breiteren Personenkreis zugänglich
	Integrität	Ein breiterer Personenkreis darf die Änderung der Daten veranlassen oder durchführen.

[1] Die Ausfallzeit ist definiert als die Zeit in der ein Service während der Betriebszeiten nicht zur Verfügung steht. Wartungszeiten sind generell nicht den Betriebszeiten anzurechnen.
[2] Die Ausfallzeit ist definiert als die Zeit in der ein Service während der Betriebszeiten nicht zur Verfügung steht. Wartungszeiten sind generell nicht den Betriebszeiten anzurechnen.

Definition Angreifer

Security Level	Beschreibung
SL 1	Schutz gegen **ungewollten** oder **zufälligen** Missbrauch
SL 2	Schutz gegen gewollten Missbrauch unter Verwendung von **einfachen** Ressourcen, mit **niedrigem** Aufwand, **allgemeinen** Fähigkeiten und **niedriger** Motivation
SL 3	Schutz gegen gewollten Missbrauch unter Verwendung von **technisch ausgefeilten** Ressourcen, mit **moderatem** Aufwand, **spezifischen** Fähigkeiten und **moderater** Motivation
SL 4	Schutz gegen gewollten Missbrauch unter Verwendung von **technisch ausgefeilten** Ressourcen, mit **erheblichem** Aufwand, **spezifischen** Fähigkeiten und **hoher** Motivation

Security Level nach IEC 62443

Angreifer Typen

extern/ intern	Typ	Charakterisierung	Stärke des Angreifers
Intern	Werksinterner	Wissen: sehr gutes IT Know How auch im industriellen Umfeld, spezielles Know How über den Geltungsbereich vorhanden Ressource Zeit, die aufgewendet werden kann: Tage Ressource Equipment: Laptop, Wissens- und Tooldatenbank Internet, auch spezielle Software/Hardware aus dem Steuerungsumfeld Motivation: niedrig bis hoch	SL=3 bis 4

Angreifer Typen

extern/ intern	Typ	Charakterisierung	Stärke des Angreifers
Extern	Dienstleister	Wissen: sehr gutes IT und Security Know How auch im industriellen Umfeld, spezielles Know How über den Geltungsbereich vorhanden Ressource Zeit, die aufgewendet werden kann: Tage Ressource Equipment: Laptop, Wissens- und Tooldatenbank Internet, auch spezielle Software/Hardware aus dem Steuerungsumfeld Motivation: niedrig bis hoch	SL=3
	Allgemeiner Angreifer	Wissen: sehr gutes IT und Security Know How auch im industriellen Umfeld, kein spezielles Know How über den Geltungsbereich vorhanden Ressource Zeit, die aufgewendet werden kann: Monate Ressource Equipment: Laptop, Wissens- und Tooldatenbank Internet, auch spezielle Software/Hardware aus dem Steuerungsumfeld Motivation: hoch	SL=3

Attribute Angreifer

Parameter	Wertebereich	Definition	Security Level
Keine	Keiner	Beiläufige oder zufällige Verletzung der Informationssicherheit.	SL 1
Fähigkeiten	Allgemeinen	Detailliertes Wissen über die Sicherheit, der Domäne oder dem spezifischen System ist nicht notwendig.	SL 2
	Spezifisch	Spezifisches Wissen über die Sicherheit (z.B. Brechen von kryptographischen Verfahren, Reverse Engineering), der Domäne oder dem spezifischen System ist erforderlich.	SL 2/3
Aufwand (Zeit)	Niedrig	Minuten bis Stunden	SL 2
	Moderat	Tage	SL 3
	Erheblich	Monate	SL 4
Ressourcen (Ausrüstung)	Einfach	Keine besondere Ausrüstung notwendig.	SL 2
	Ausgefeilt	Der Angreifer greift auf Exploits im Betriebssystem zurück, welche nicht weitreichend bekannt sind. Er nutzt Cracking-Tools für Passwörter und Schlüssel und kann auf Hash-Tables zurückgreifen.	SL 3
	Ausgereift	Hochleistungsrechner, Botnetze und Supercomputer werden benutzt.	SL 4
Zeitfenster (Notwendige Zeit zur Erkennung eines Angriffs)	Niedrig	Stunden	SL 4
	Mittel	Einige Tage	SL 3
	Hoch	Tage / Wochen	SL 2

Security Level	Beschreibung
SL 1	Schutz gegen ungewollten oder zufälligen Missbrauch
SL 2	Schutz gegen gewollten Missbrauch unter Verwendung von einfachen Ressourcen, mit niedrigem Aufwand, allgemeinen Fähigkeiten und niedriger Motivation
SL 3	Schutz gegen gewollten Missbrauch unter Verwendung von technisch ausgefeilten Ressourcen, mit moderatem Aufwand, spezifischen Fähigkeiten und moderater Motivation
SL 4	Schutz gegen gewollten Missbrauch unter Verwendung von technisch ausgereiften Ressourcen, mit erheblichem Aufwand, spezifischen Fähigkeiten und hoher Motivation

Attribute Angreifer

<ID für das Bedrohungsszenario>: <Kurzbezeichnung>				<Bewertung des Risikos>
Beschreibung des Bedrohungsszenarios				
<kurze Beschreibung des Bedrohungsszenarios>				
Betroffene Komponenten, Anwendungen, Kommunikation				
<hier werden die betroffenen Komponenten, Netzwerksegmente etc. benannt, auf die die Bedrohung wirkt>				
Technische Auswirkung				
< in diesem Abschnitt werden die technischen Auswirkungen beschrieben, die durch die Realisierung einer Bedrohung möglich werden>				
Referenz auf IEC 62443-3-3				**Ziel-SL**
<Referenzen auf die Security Requirements des Standards, durch die der Bedrohung begegnet werden kann>				<der zu erreichende SL (Security Level), in den meisten Fällen ist SL=3>
Beschreibung der Security-Umgebung				
- <in grün werden die umgesetzten Security-Maßnahmen beschrieben> - <in rot werden Defizite/Schwachstellen beschrieben>				
Parameter zur SL Bestimmung (die Bedeutung und möglichen Werte der Parameter sind im Sicherheitskonzept beschrieben)				**Erreichter-SL**
Skills	*Ressourcen (Zeit)*	*Ressourcen (Ausrüstung)*	*Zeitfenster*	<Abschätzung für den erreichten SL gemäß den Bewertungen der Parameter zur SL Bestimmung, siehe Sicherheitskonzept>
<Wert>	<Wert>	<Wert>	<Wert>	
Auswirkung (bzgl. Handlungsfelder)				
<hier wird die maximale Auswirkung bzgl. der Handlungsfelder beschrieben. Die Beschreibung wird mit einer Gesamtbewertung des Schadens gemäß den Schadensklassen vorgenommen, z.B. Schaden: gravierend>				
Abgeleitete Security-Maßnahmen				
<hier werden die Security-Maßnahmen empfohlen, die als notwendig erachtet werden, um dem zu hohen Risiko angemessen zu begegnen. In der Regel ist der zu erreichende SL anzustreben>				

Parameter	Wertebereich	Definition	SL
keine	**keine**	Beiläufige oder zufällige Verletzung der Informationssicherheit.	1
Wissen	generisch	Detailliertes Wissen über die Sicherheit, der Domäne oder dem spezifischen System ist nicht notwendig	2
	spezifisch	Spezifisches Wissen über die Sicherheit (z.B. Brechen von kryptographischen Verfahren, Reverse Engineering), der Domäne oder dem spezifischen System ist erforderlich.	3,4
Ressource (Zeit)	Niedrig	Minuten bis Stunden	2
	Mittel	Tage	3
	Hoch	Monate	4
Ressource (Ausrüstung)	Niedrig	Keine besondere Ausrüstung notwendig.	2
	Mittel	Der Angreifer greift auf Exploits im Betriebssystem zurück, welche nicht weitreichend bekannt sind. Er nutz Cracking-Tools für Passwörter und Schlüssel und kann auf Hash-Tables zurückgreifen.	3
	Hoch	Hochleistungsrechner, Botnetze und Supercomputer werden benutzt.	4
Zeitfenster (notwendige Zeit zur Erkennung eines Angriffs)	Niedrig	Stunden	4
	Mittel	Einige Tage	3
	Hoch	Tage - Wochen	2

Risikomatrix

Schaden

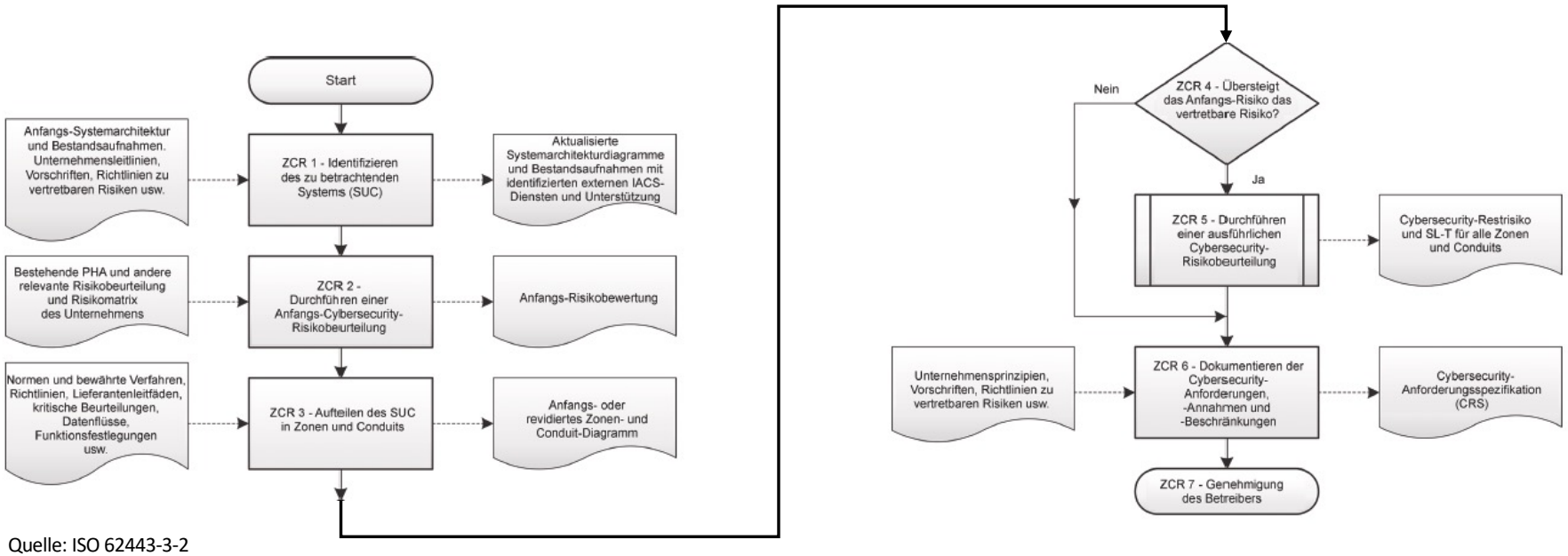
Eintrittswahrscheinlichkeit	Security Level	1 Unwesentlich	2 Mäßig	3 Hoch	4 Kritisch
unwahrscheinlich	4				
möglich	3				
wahrscheinlich	2				
fast sicher	1				

Darstellung kritischer Risiken, zwingender Handlungsbedarf

Darstellung wesentlicher Risiken, Handlungsbedarf nach Ermessen

Darstellung unwesentlicher Risiken, kein Handlungsbedarf

Anforderungen an Zonen, Conduits und Risikobeurteilungen



Quelle: ISO 62443-3-2

Bsp. Risiko-Analyse

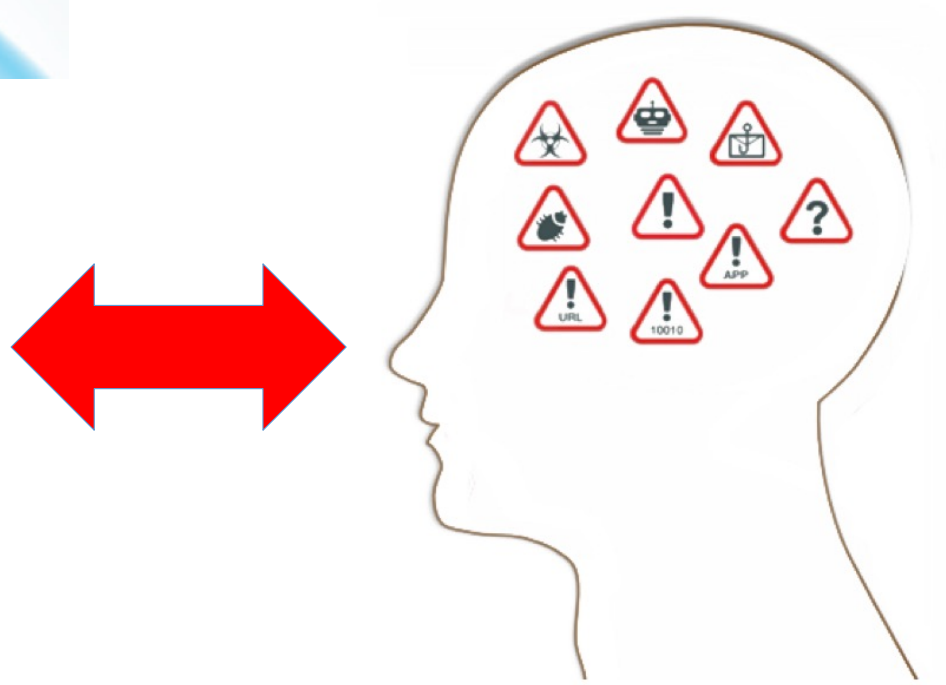
DC	Kurztitel Bedrohung			Risiko
Beschreibung des Bedrohungsszenarios				
Kurbeschreibung der Bedrohung auf Basis des Bedrohungskataloges.				
Betroffene Komponenten, Anwendungen, Kommunikation				
Beschreibung der betroffenen Systeme und Komponenten.				
Technische Auswirkungen				
Kurzbeschreibung der technischen Auswirkungen bei Auftreten der Bedrohung.				
Referenz auf IEC 62443-3-3				Erreichter-SL
Angabe der „Fundamental Requirement" der ISO 62443, die bei Einwirken der Bedrohung angewendet wird.				Erreichter Security Level
Beschreibung der Security-Umgebung				
Angabe der bereits umgesetzten Sicherheitsmaßnahmen auf Basis der Anforderungen.				
Auswirkung (bzgl. Handlungsfelder)				Schaden
Auswirkungen auf die Informationssicherheit bei Eintreten der Verletzung einer oder mehrere Schutzziele.				Anzunehmender Schaden
Parameter zur SL-Bestimmung				Ziel-SL
Skills	Ressourcen (Zeit)	Ressourcen (Ausrüstung)	Zeitfenster	Notwendiger Security Level
Bewertung umgesetzte Maßnahmen				
Zusammenfassung und Bewertung der umgesetzten Maßnahmen auf Basis der ISO 62443 und Aggregierung des erreichten Security Level				
Abgeleitete Security-Maßnahmen				
Zusätzliche Maßnahmen zur Erreichung eines höheren Security Level oder Verbesserung bestehender Maßnahmen.				

Cybersecurity is a Foundation for Digital Business

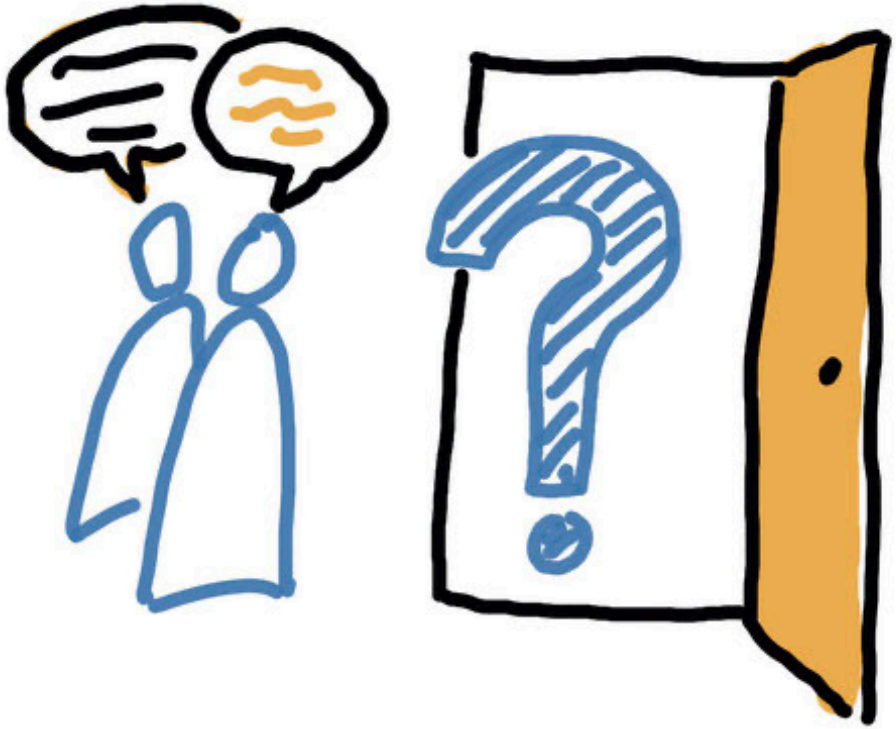
Gartner

Gartner Webinars

- Gesetzliche Vorgaben wie das IT Sicherheitsgesetz
- Normen-Vorgaben
- Business-Vorgaben
- Haftungsaspekte steigen
- Management „Stand der Technik“
- Versicherungsanforderungen steigen
- Industrie 4.0 Migrationsprojekte



Fragen



Für Fragen
und Informationen:

K4 DIGITAL

Alfred-Nobel-Allee 38
66793 Saarwellingen

+49 (0)6831 6879-0
info@k4.digital