*** INTERN ***

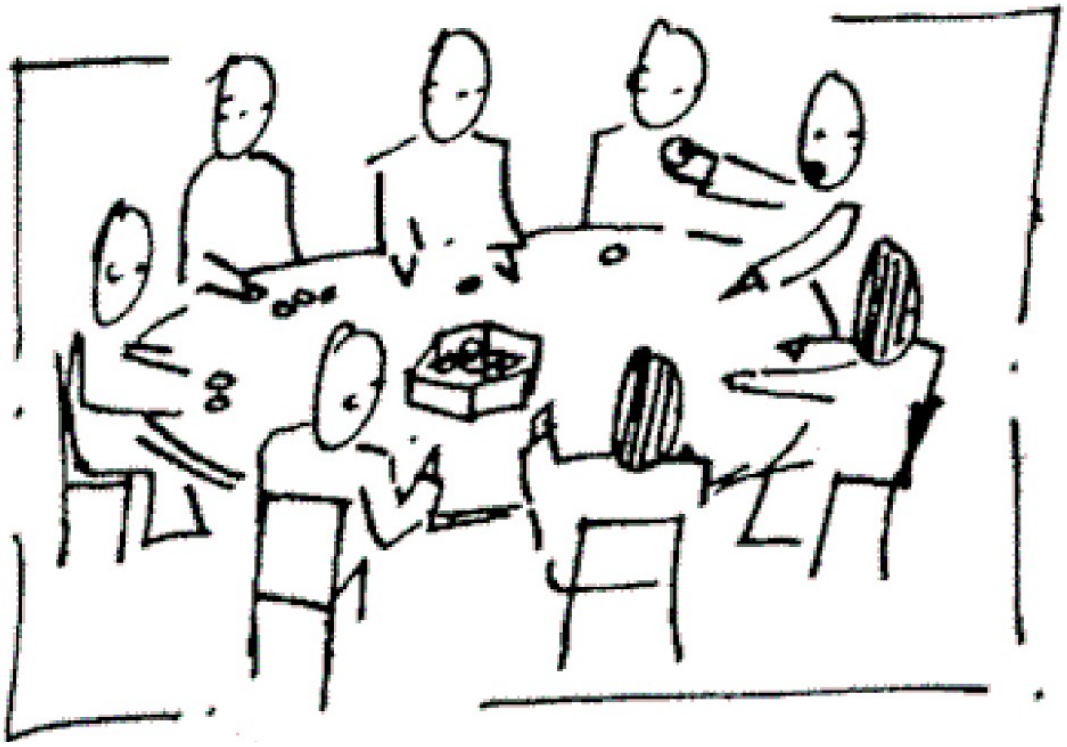
Workshop Grundlagen M1

Cyber-Sicherheit in der Produktion

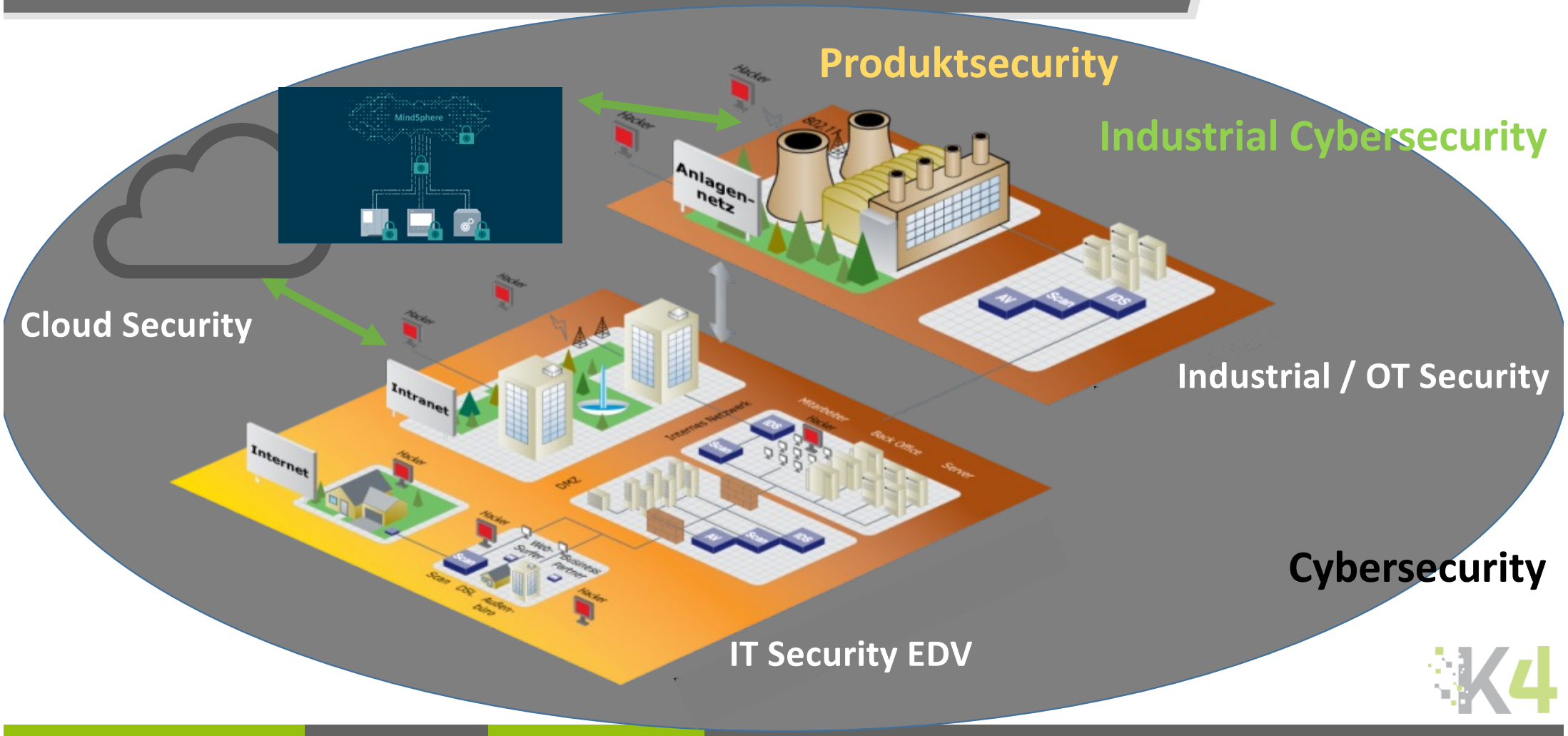
25.10.2023

Mittelstand-Digital
Zentrum
Saarbrücken

Vorstellungsrunde



Cybersecurity Perspektiven



Stillstand nach Hackerangriff bei SAF-Holland

Aurubis, **Continental** und nun auch SAF-Holland: Der Nutzfahrzeug-Zulieferer mit Sitz im bayrischen Bessenbach ist am vergangenen Wochenende Opfer eines **Cyberangriffs** geworden, wie das Unternehmen am heutigen Montagmittag mitteilt. Infolge der Attacke sie das Notfallprotokoll aktiviert und die Systeme vom Netz getrennt worden, erklärte ein Sprecher auf FINANCE-Anfrage. Teile der Produktion wurden dadurch unterbrochen.

Aktuell sei man damit beschäftigt, die Systeme nach und nach wieder hochzufahren und Übergangslösungen zu finden. Wann die Produktion wieder vollständig laufen wird, ist aktuell noch nicht abzusehen. SAF-Holland rechnet aus heutiger Sicht jedoch damit, dass sich die Unterbrechung über einen Zeitraum von sieben bis vierzehn Tagen erstrecken könne.

Nach einem Cyberangriff auf den Nutzfahrzeug-Zulieferer SAF-Holland stehen Teile von dessen Produktion still. Foto: SAF-Holland

CYBER-KRIMINALITÄT

Fleischkonzern JBS zahlte Hackern elf Millionen Dollar Lösegeld

AKTUALISIERT AM 10.06.2021 - 03:33

Vergangene Woche hatte der Angriff die Produktion in Nordamerika und Australien lahmgelegt. Die Lösegeldzahlung soll in der Kryptowährung Bitcoin erfolgt sein.

Hackerangriff auf Pipeline

USA erklären regionalen Notstand

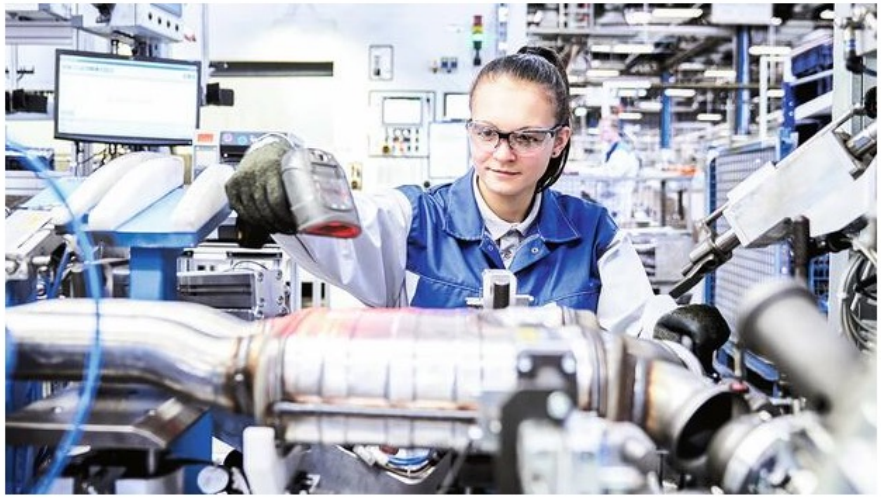
Stand: 10.05.2021 08:12 Uhr

Vergangene Woche legte ein Cyberangriff die größte Pipeline der USA lahm - das Hauptsystem ist noch immer außer Betrieb. Jetzt hat die US-Regierung den regionalen Notstand ausgerufen.

NACH HACKERANGRIFF AUF EBERSPÄCHER

Werden jetzt Heizungen und Auspuffe für Autos knapp?

von Sonja Álvarez, Thomas Kuhn und Annina Reimann
05. November 2021



Nur Notbetrieb: Beim Autozulieferer Eberspächer stockt nach dem Hackerangriff auch die Auspuffproduktion
Bild: PR

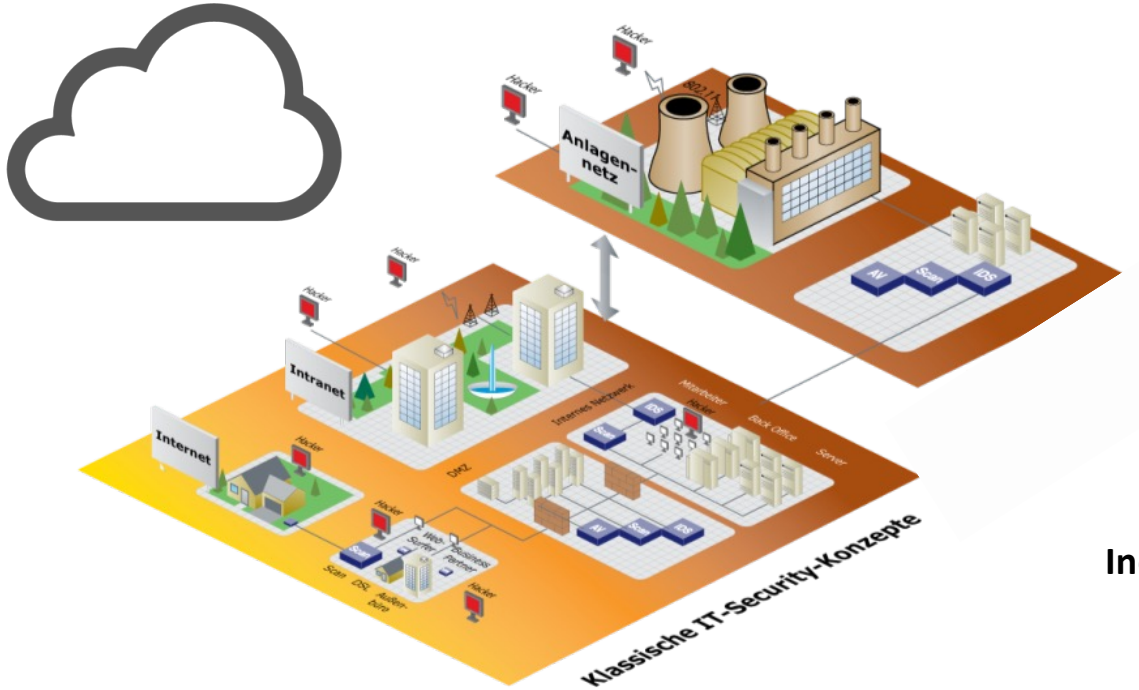
Nach dem Chipmangel bereitet der Autoindustrie nun auch der Cyberangriff auf den Zulieferer Eberspächer Sorgen. Bei einzelnen Automodellen droht die Produktion zu stocken. Für Käufer bedeutet das längere Lieferfristen.

Cyberattacke auf Metro wirkt nach

Düsseldorf · Nach mehreren Wochen sind die Probleme noch nicht gelöst. Kunden spüren dies unter anderem durch längere Wartezeiten in den Märkten. Sensible Daten von Mitarbeitern sind im Darknet aufgetaucht.

Wo stehen wir zu Zeiten Industrie 4.0 mit Industrial Security?

...Security Betrachtungsaspekte...



Business-IT:

1. Vertraulichkeit

2. Integrität

3. Verfügbarkeit

Industrie 4.0

Industrial-IT:

1. Safety

2. Verfügbarkeit

3. Integrität

4. Vertraulichkeit

Industrial-IT:

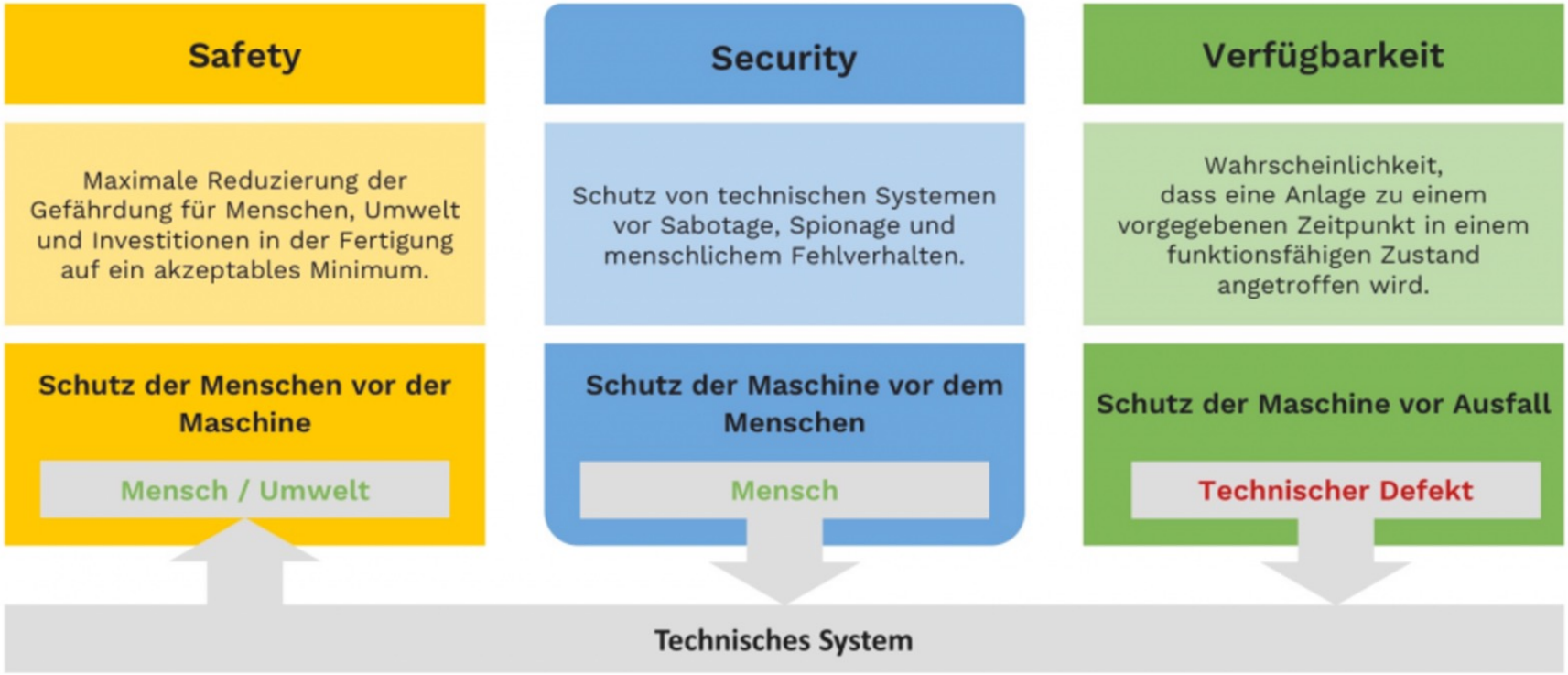
1. Safety

2. Integrität

3. Verfügbarkeit

4. Vertraulichkeit

Zusammenhang zwischen Safety, Security und Verfügbarkeit



Herausforderungen und Unterschiede dabei...

	Business IT	Industrial IT / ICS*
Virenschutz	Weit verbreitet	Kompliziert, oft unmöglich
Lebensdauer	3-5 Jahre	5-20 Jahre
Outsourcing	Weit verbreitet	Selten
Patchmanagement	Oft, täglich	Selten, benötigt Freigabe vom Anlagenhersteller
Änderungen	Häufig	Selten
Zeitabhängigkeit	Verzögerungen akzeptiert	Kritisch
Verfügbarkeit	akzeptabel	24x7
Awareness	Gut	Schlecht
Sicherheitstests	Weit verbreitet	Selten und problematisch
Physische Sicherheit	Abgesichert, bemannt	Großflächig, unbemannt

OT-Arbeitsweisen unterscheiden sich...

- In der Vergangenheit waren ICS
  - Stand-alone Systeme
  - vernetzt durch proprietäre Netzwerke
  - „eigen-Entwicklungen“ mit eigenen Standards

- Heute sind ICS
  - basierend auf state-of-the-Art Soft- und Hardware
  - vernetzt mit Ethernet-Standard
  - verantwortlich für den reibungslosen Ablauf unseres Alltags

- **Morgen...**
  - **KI....Machine Learning**

"He's the only person who knows how to program our 20 year old PLCs."

Menschen & Systeme sind oft noch nicht vorbereitet für die Digitalisierung

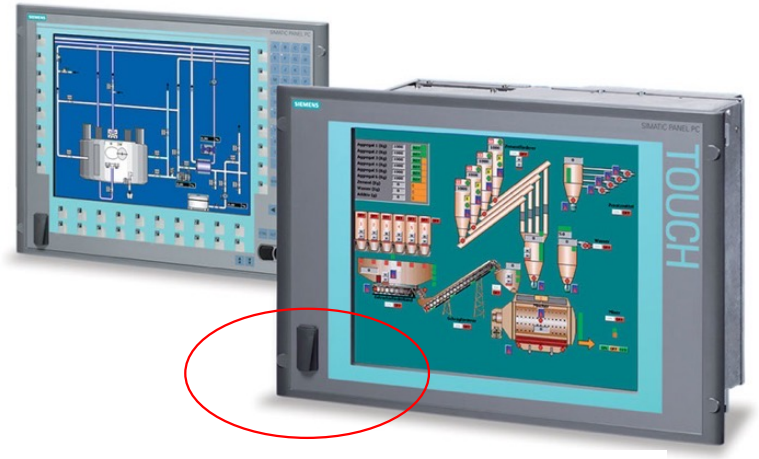
- Mischverhältnis „älterer“ Automatisierungs-technik und neuen Infrastruktur-Technologien

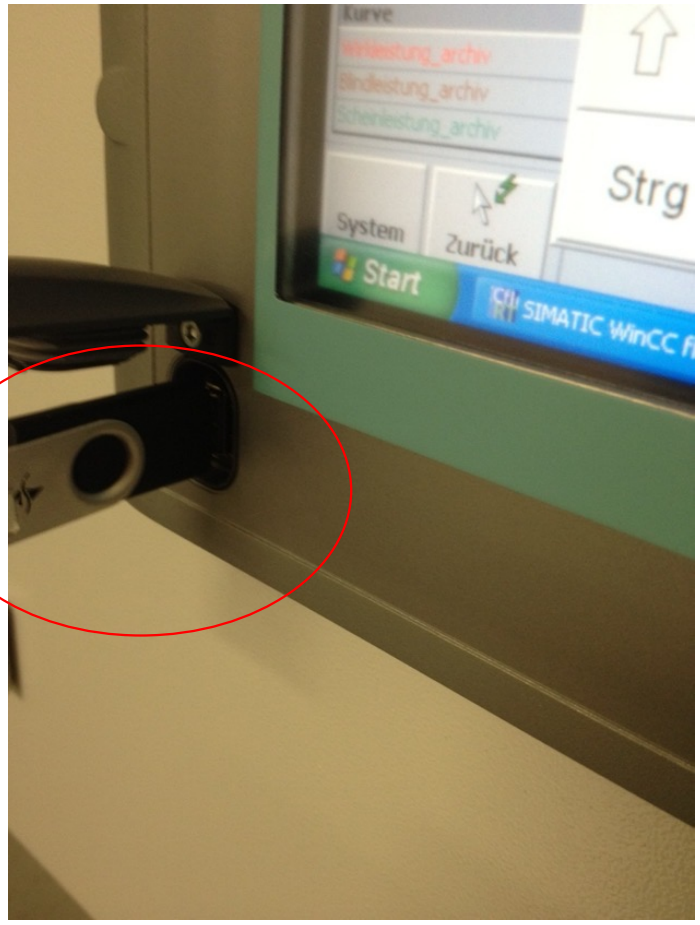
- Früher
  - „security through obscurity“
- Heute
  - gleiche Risiken wie im Office-Umfeld (TCP/IP, Windows, Hardware, WWW & Mail,….)
  - gleiche Angreifer wie im Office-Umfeld

- **Morgen neue Risiken...**
  - **KI ....Machine Learning**

Real World Findings

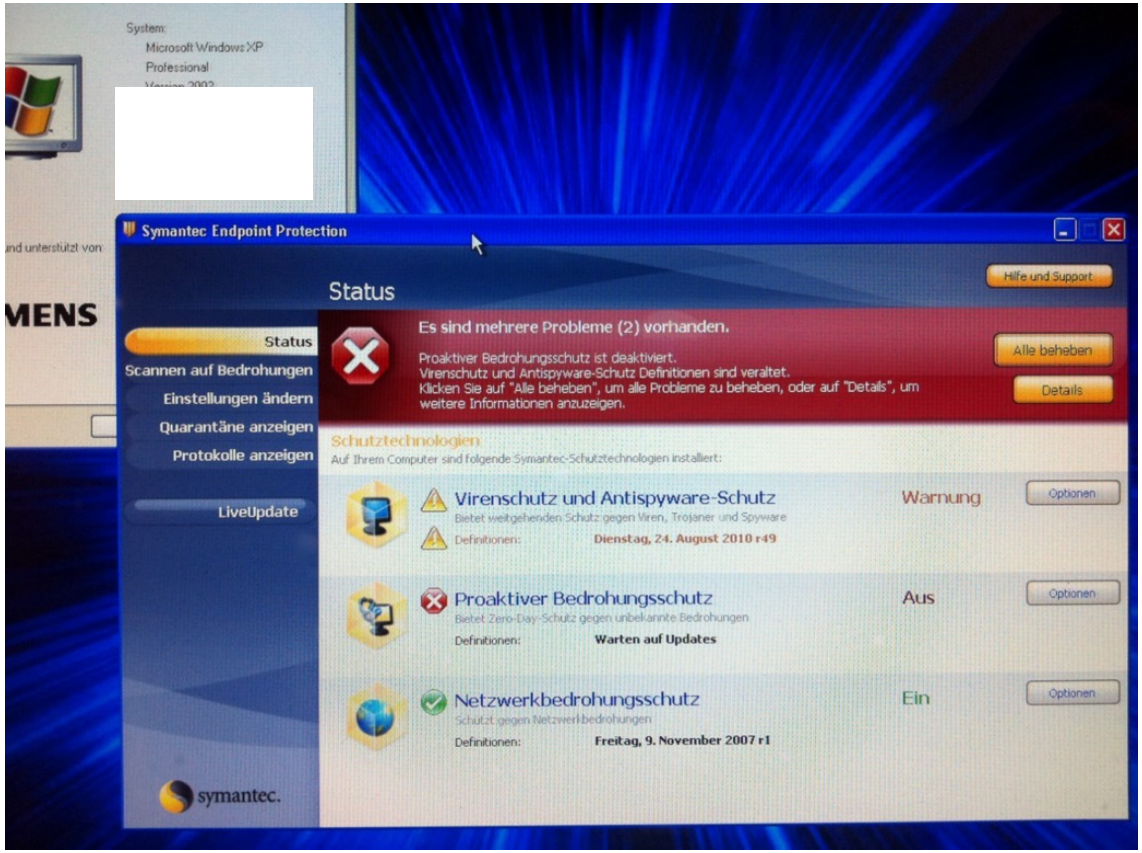
Real World Findings





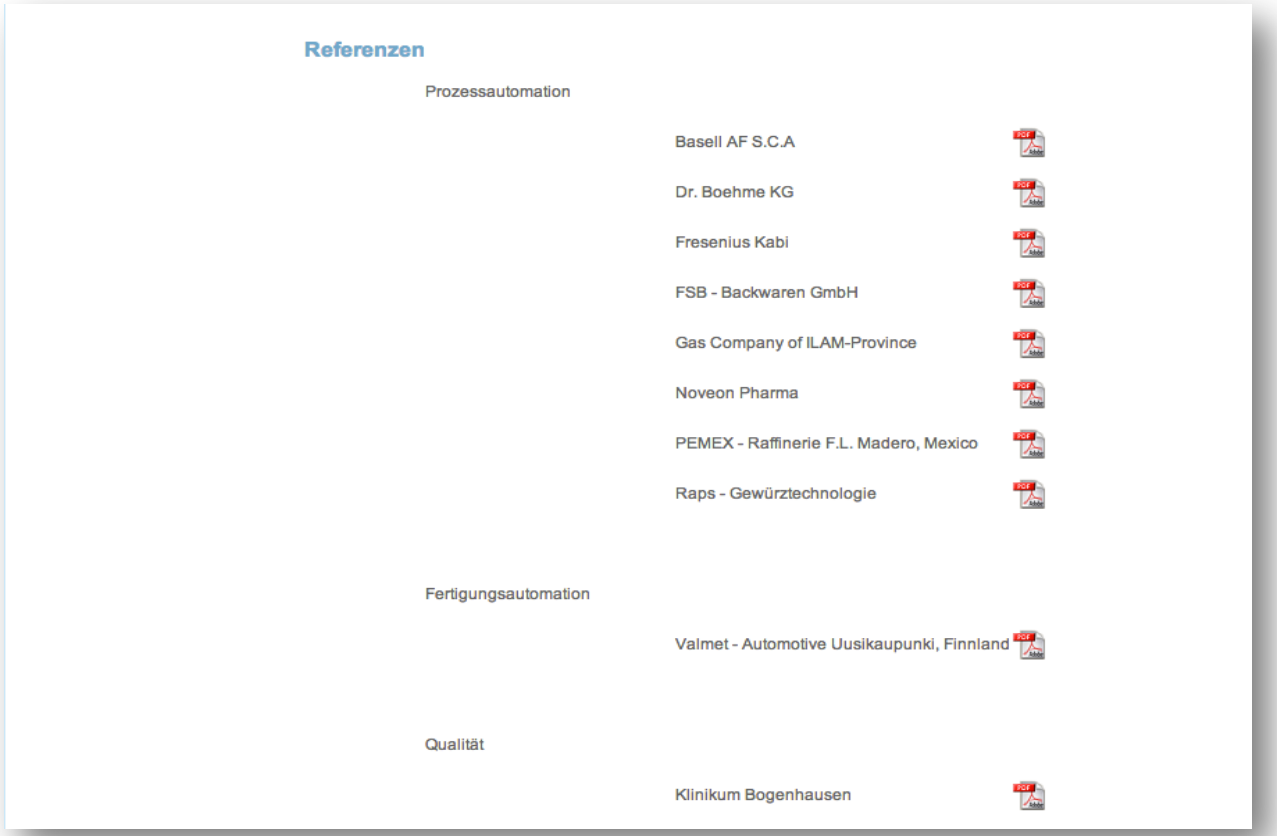
Real World Findings

Real World Findings



Real World Findings

WarGoogleling 2.0



Referenzen

Prozessautomation

- Basell AF S.C.A
- Dr. Boehme KG
- Fresenius Kabi
- FSB - Backwaren GmbH
- Gas Company of ILAM-Province
- Noveon Pharma
- PEMEX - Raffinerie F.L. Madero, Mexico
- Raps - Gewürztechnologie

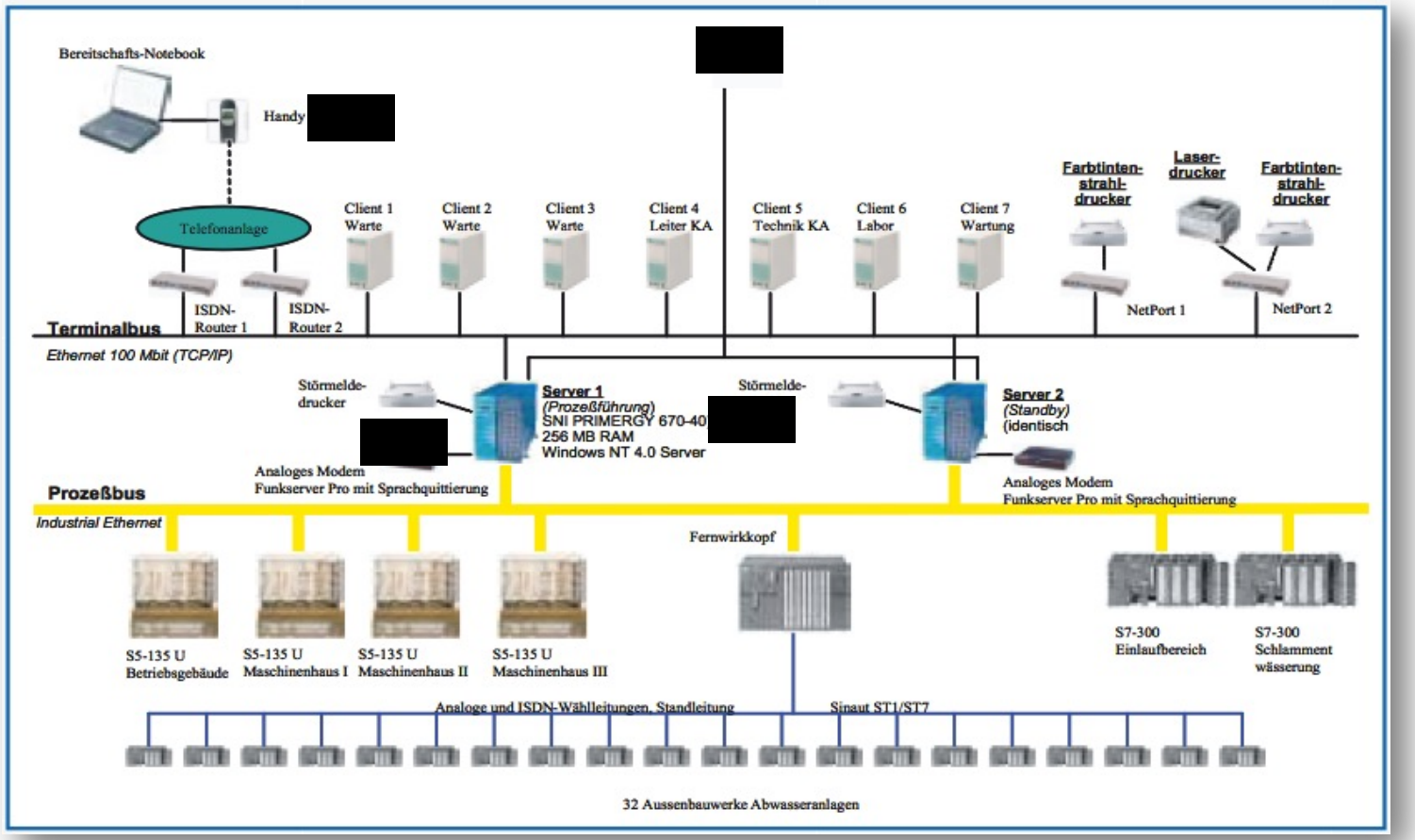
Fertigungsautomation

- Valmet - Automotive Uusikaupunki, Finnland

Qualität

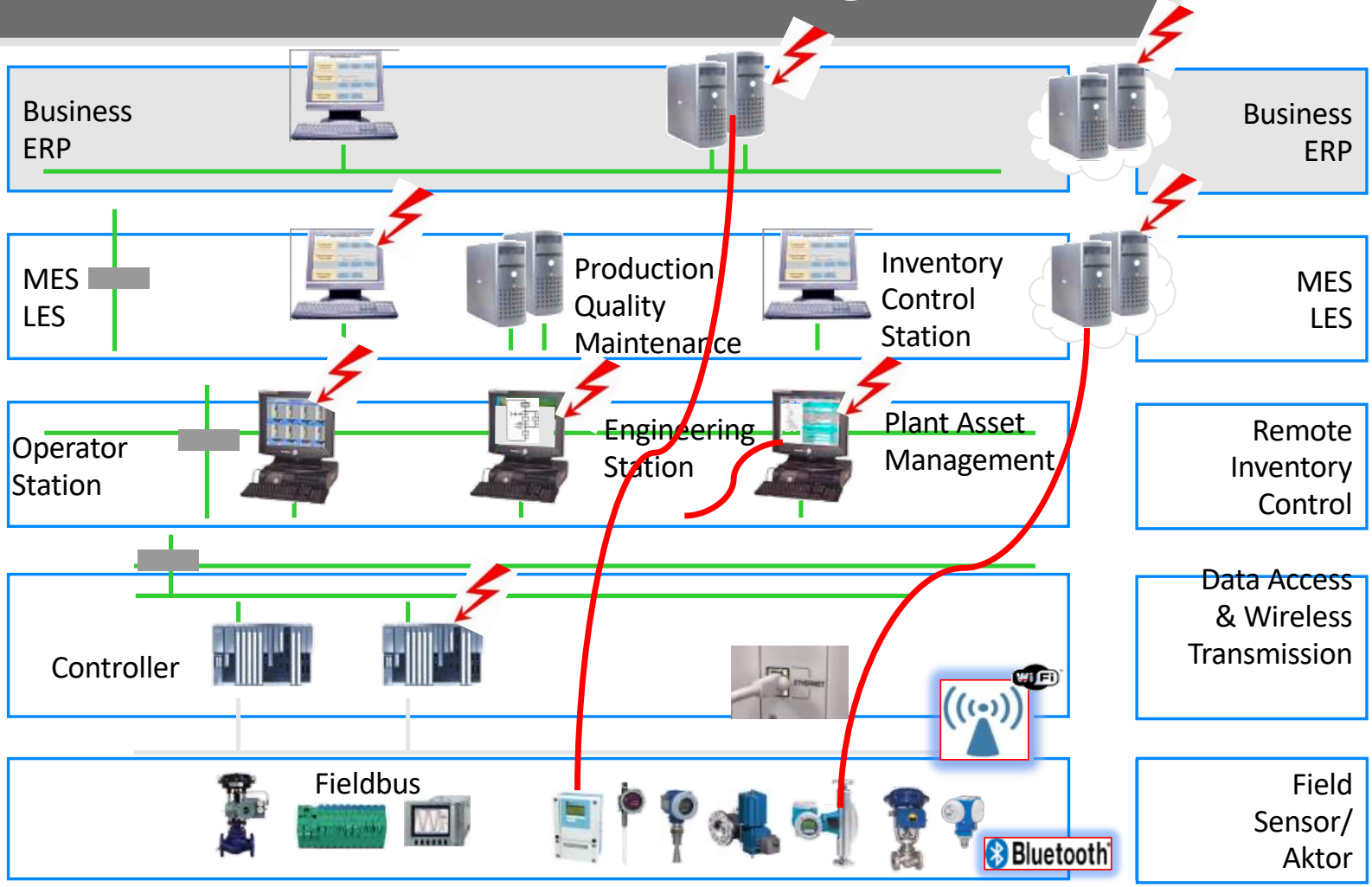
- Klinikum Bogenhausen

WarGoogleling 2.0



Neue Technik – neue Herausforderungen

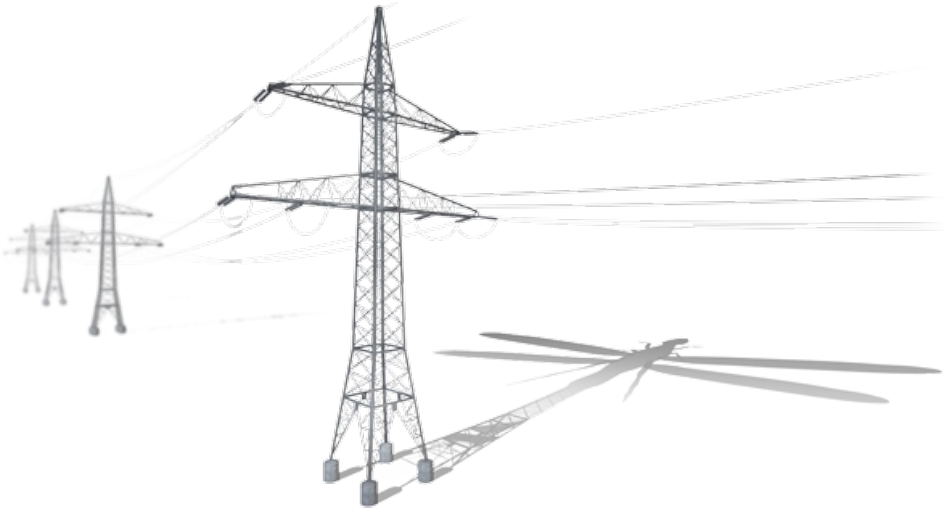
Neue Technik – neue Herausforderungen



Beispiel an Hand einer Schadsoftware

Havex / Dragonfly

- Entdeckt: Juni 2014
- Erste Aktivitäten: 2010
- Weitere Aktivitäten: 2019



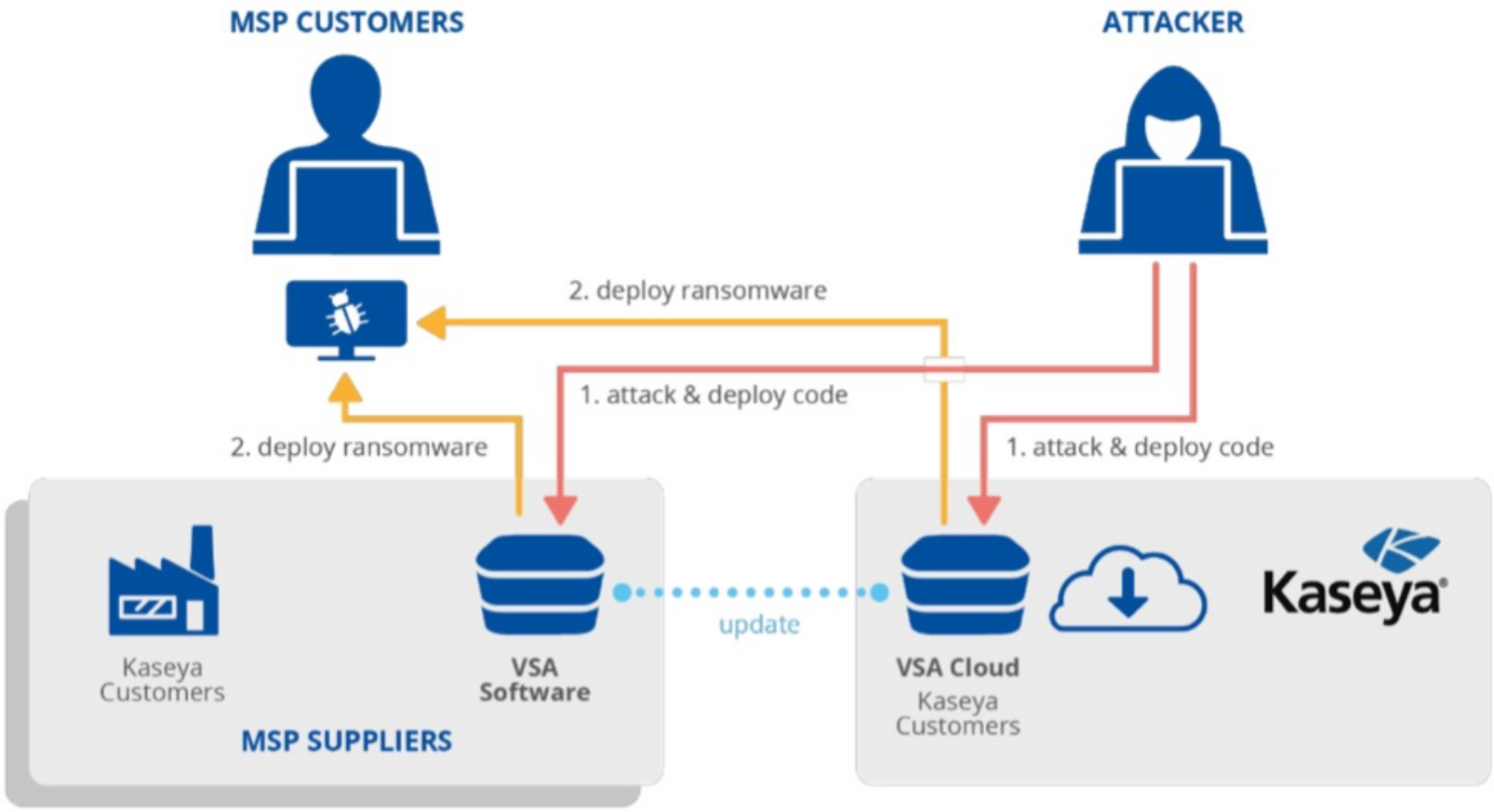
- RAT = Remote Access Trojaner
  - Watering Hole Attack
    - Angriff über Hersteller Website
    - Hersteller-Software wurde kompromittiert
    - Nach Installation Backdoor geöffnet

Havex / Dragonfly

- sammelt Daten über OPC, Modbus, EtherNet/IP, S7/Profinet und weitere Protokolle
- speziell ausgelegt für europäische Energie- & produzierende Industrie
  - Stromnetze, Piplines, Windparks, Produktionsunternehmen etc.

- Analyse der Schadsoftware zeigt Aktivitäten von Montag bis Freitag in der Zeitzone UTC+4 auf.

Supply Chain Angriffe steigen

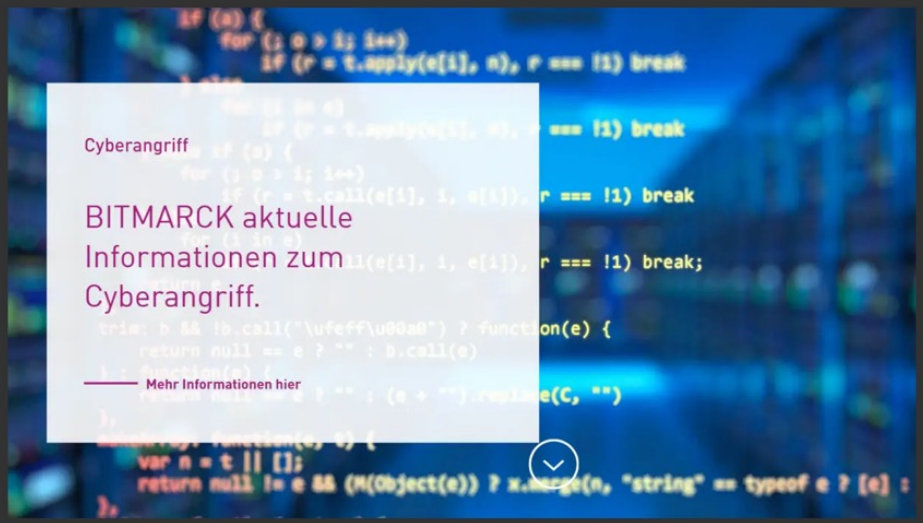


Supply Chain Angriffe steigen

Nach Cyberangriff: Millionen Versicherte können Krankenkassen-Apps nicht nutzen

Nachdem der IT-Dienstleister Bitmarck von Cyberkriminellen angegriffen wurde, haben Millionen Krankenversicherte weiterhin mit massiven Störungen zu kämpfen.

Lesezeit: **5 Min.** In Pocket speichern 107



(Bild: Bitmarck)

Supply Chain Angriffe steigen

Adesso Deutschland verschwieg Cyberangriff lange

Von Philipp Anz, 20. April 2023 um 13:37

SECURITY CYBERANGRIFF DEUTSCHLAND ADESSO

Foto: Engyn Arkut / Unsplash

Kunden wurden nicht über die gefährliche Situation informiert. Erst ein Whistleblower machte Medien und Security-Behörden auf den Fall aufmerksam.

Gefahr durch VPN-Verbindungen

Adessos Sicherheitsteam entdeckte den Angriff erst am 11. Januar. Zwar seien danach laut 'SZ' ein Microsoft-Ermittlerteam informiert und einige kompromittierte Nutzerkonten geschlossen worden. Doch Behörden oder Kunden erfuhren nicht, dass sie in Gefahr sind. In Deutschland zählen zu diesem Kreis grosse Konzerne wie BMW, RWE und EON, das Bundeskriminalamt, die Finanzaufsicht Bafin und die Bundesbank. Zu vielen Firmen unterhält Adesso VPN-Verbindungen, die durch einen Angriff zum Problem werden können.

Grundrauschen - Statistiken

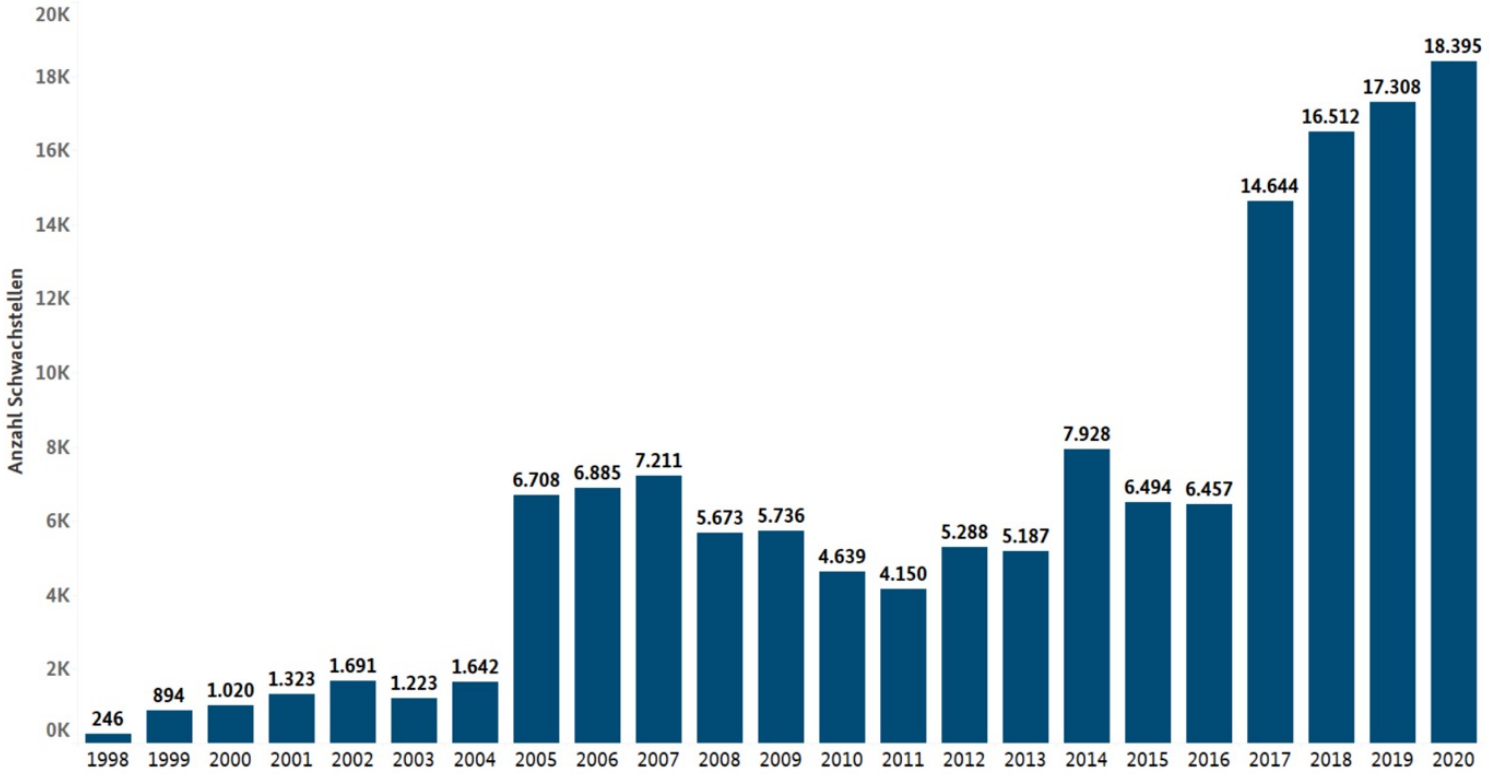


Abbildung 14: Anzahl an veröffentlichten Software-Schwachstellen basierend auf zugewiesenen CVE-Nummern (Common Vulnerabilities and Exposures; Standard zur Benennung von Sicherheitslücken in Computersystemen; Quelle der Grafik siehe Fußnote 8)

VDE CERT


VDE CERT
Suche
Nachrichten
Advisories
CNA
Bulletins
Termine
Weiteres
Über uns
CERT@VDE ist die erste IT-Sicherheitsplattform in Deutschland für kleine und mittelständische Unternehmen (KMU) im Bereich der Automatisierung.
Mit der fortschreitenden Vernetzung von Produktionssystemen steigt auch das Risiko von Sicherheitslücken und dadurch von Angriffen auf Ihre Systeme.
CERT@VDE hilft dabei auf digitale Bedrohungen angemessen zu reagieren und Sicherheitslücken zu kommunizieren. Auf unserer Seite finden Sie aktuelle Sicherheitswarnungen, Vernetzungsmöglichkeiten und weitere wichtige Informationen, um Ihr Unternehmen vor Angriffen/Sicherheitslücken zu schützen.
Was das einzelne KMU nicht leisten kann, bietet CERT@VDE durch Kooperation, Vernetzung und Kompetenz. Wir unterstützen betroffene KMU bei den notwendigen Analysen und Entscheidungen und koordinieren die Reaktion auf Sicherheitsschwachstellen über

Industrial Control System Security 2022

Top 10 Bedrohungen	Trend seit 2019
Einschleusen von Schadsoftware über Wechseldatenträger und mobile Systeme	→
Infektion mit Schadsoftware über Internet und Intranet	↑
Menschliches Fehlverhalten und Sabotage	→
Kompromittierung von Extranet und Cloud-Komponenten	↗
Social Engineering und Phishing	→
(D)DoS Angriffe	→
Internet-verbundene Steuerungskomponenten	↗
Einbruch über Fernwartungszugänge	↗
Technisches Fehlverhalten und höhere Gewalt	→
Soft- und Hardwareschwachstellen in der Lieferkette	↑

Live Szenarien

*** INTERN ***

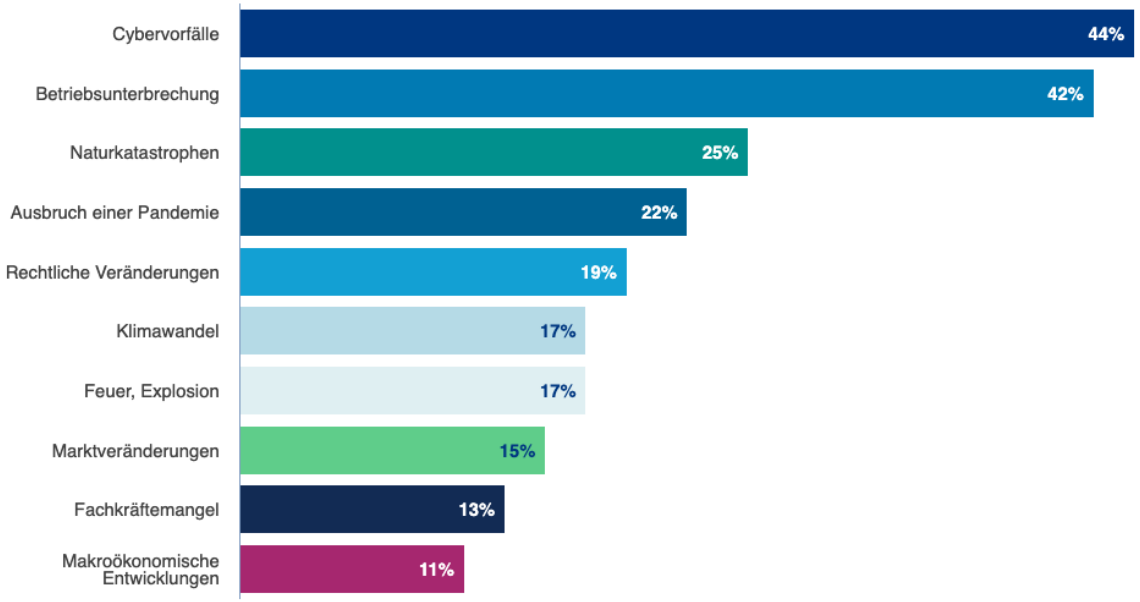
Top 10 Geschäftsrisiken weltweit in 2022

Allianz

Top 10 Geschäftsrisiken weltweit in 2022

Allianz Risk Barometer 2022

Basierend auf den Antworten von 2.650 Risikomanagement-Experten aus 89 Ländern und Gebieten (% der Antworten). Die Zahlen ergeben nicht 100%, da jeweils bis zu drei Risiken ausgewählt werden konnten.



AGCS News & Insights

Source: Allianz Global Corporate & Specialty

202 Milliarden Euro Schaden pro Jahr

Wodurch sind Ihrem Unternehmen innerhalb der letzten 12 Monate Schäden im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden?

Schaden durch...	Schadenssummen in Mrd. Euro (2022)	Schadenssummen in Mrd. Euro (2021)	Schadenssummen in Mrd. Euro (2019)	Schadenssummen in Mrd. Euro (2017)
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	41,5	61,9	13,5	5,3
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	10,7	24,3	5,3	0,7
Datenschutzrechtliche Maßnahmen (z.B. Information von Kunden)	18,3	17,1	4,4	3,2
Patentrechtsverletzungen (auch schon vor der Anmeldung)	18,8	30,5	14,3	7,7
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	41,5	29	11,1	8,6
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	21,1	22,7	11,1	3,5
Imageschaden bei Kunden oder Lieferanten/ Negative Medienberichterstattung	23,6	12,3	9,3	7,7
Kosten für Ermittlungen und Ersatzmaßnahmen	10,1	13,3	18,3	10,6
Kosten für Rechtsstreitigkeiten	16,2	12,4	15,6	5,5
Höhere Mitarbeiterfluktuation/Abwerben von Mitarbeitern	-	-	-	2,2
Sonstige Schäden	0,9	0	<0,1	<0,1
Gesamtschaden pro Jahr	**202,7**	**223,5**	**102,9**	**54,8**

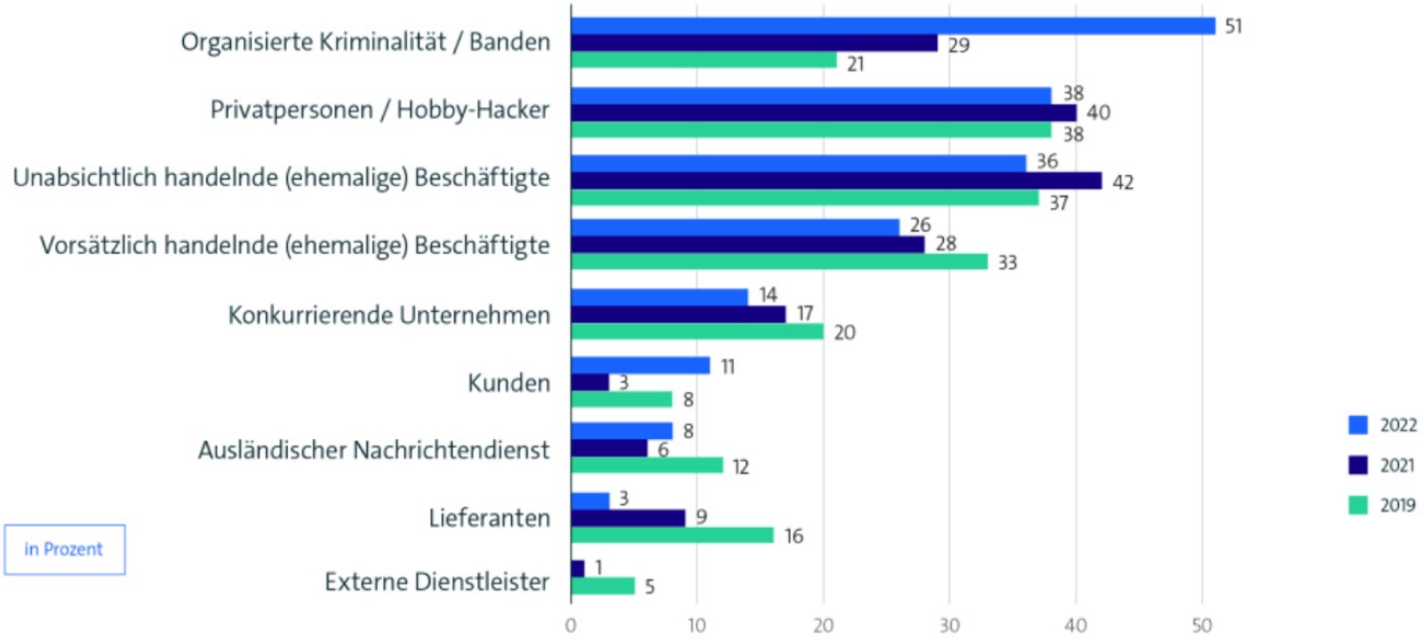
Basis: Alle befragten Unternehmen, die in den letzten 12 Monaten (2019 und 2017: 2 Jahren) von Diebstahl von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (2022: n=899; 2021: n=935; 2019: n=801; 2017: n=571) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2022

bitkom

K4

Attacken auf die Wirtschaft werden professioneller

Von welchem Täterkreis gingen Handlungen in den letzten 12 Monaten aus?

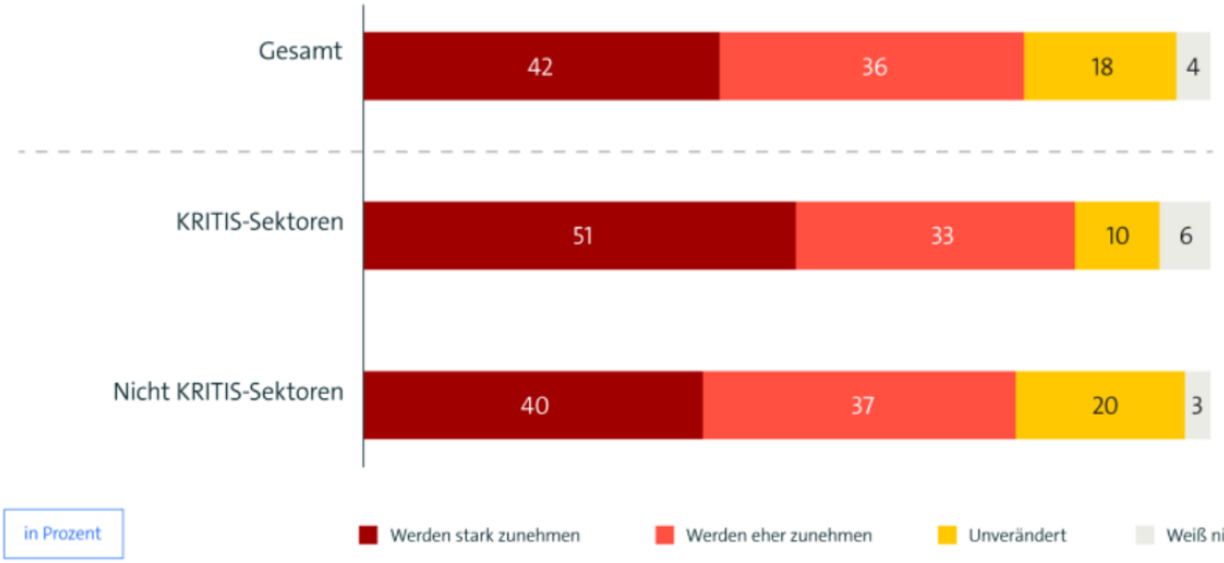


Basis: Alle befragten Unternehmen, die in den letzten 12 Monaten (2019: 2 Jahren) von Diebstahl von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (2022: n=899; 2021: n=935; 2019: n=801) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2022

bitkom

Wirtschaft rechnet mit verstärkten Cyberangriffen

Wie wird sich die Anzahl der Cyberattacken auf Ihr Unternehmen in den nächsten 12 Monaten im Vergleich zu den letzten 12 Monaten voraussichtlich entwickeln?

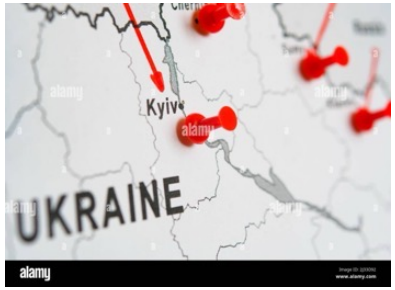


Basis: Alle befragten Unternehmen (n=1.066) | Quelle: Bitkom Research 2022

bitkom

*** INTERN ***

…Rahmenbedingungen & Kennzeichen der Digitalisierung…

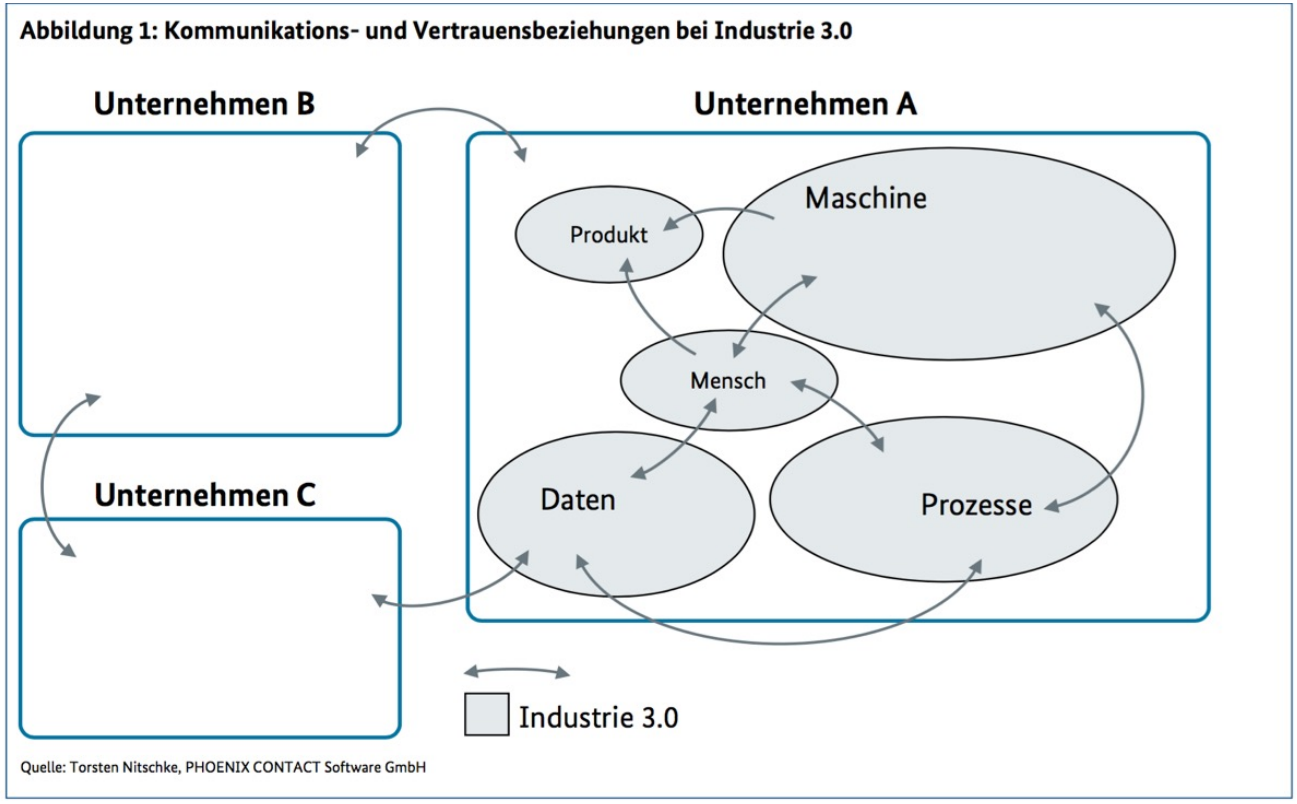


GEN
Y & Z

Ambidextrie

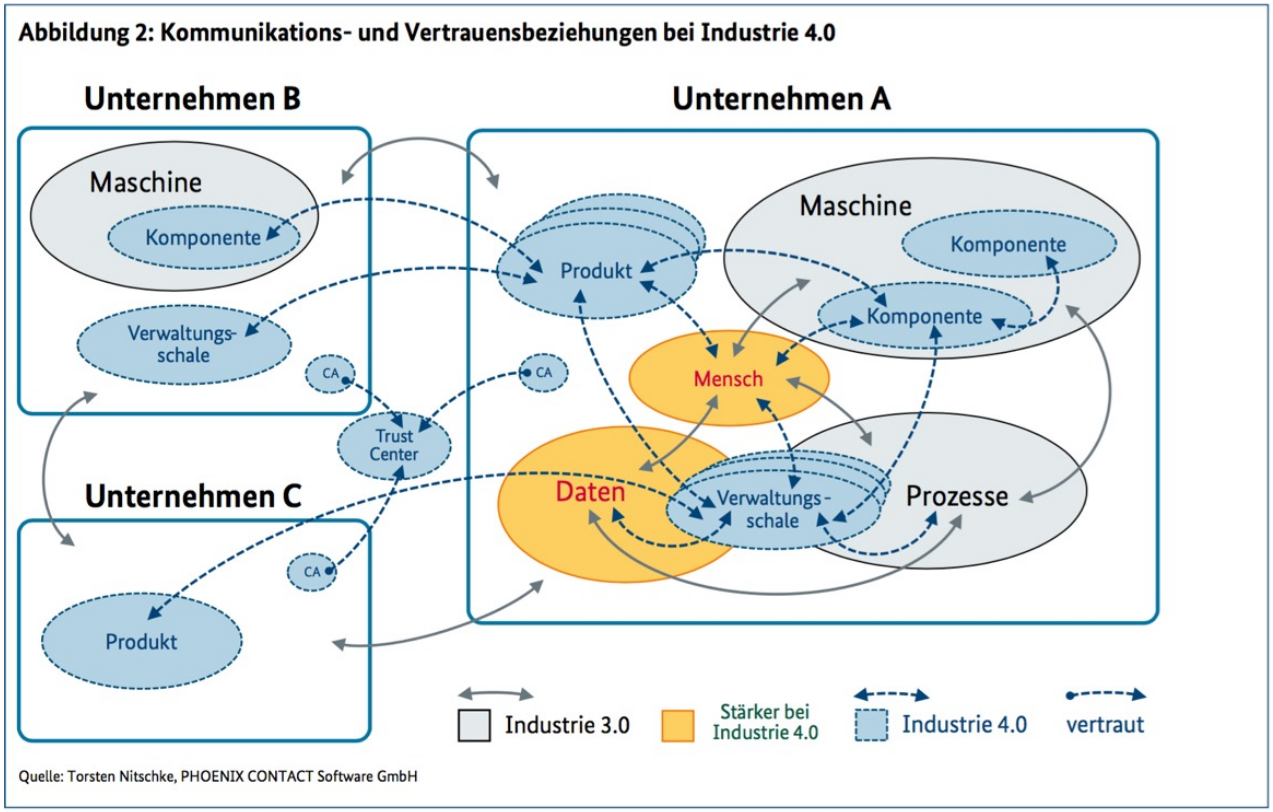
Denken & Handeln in ECO Systemen!

Industrie 3.0



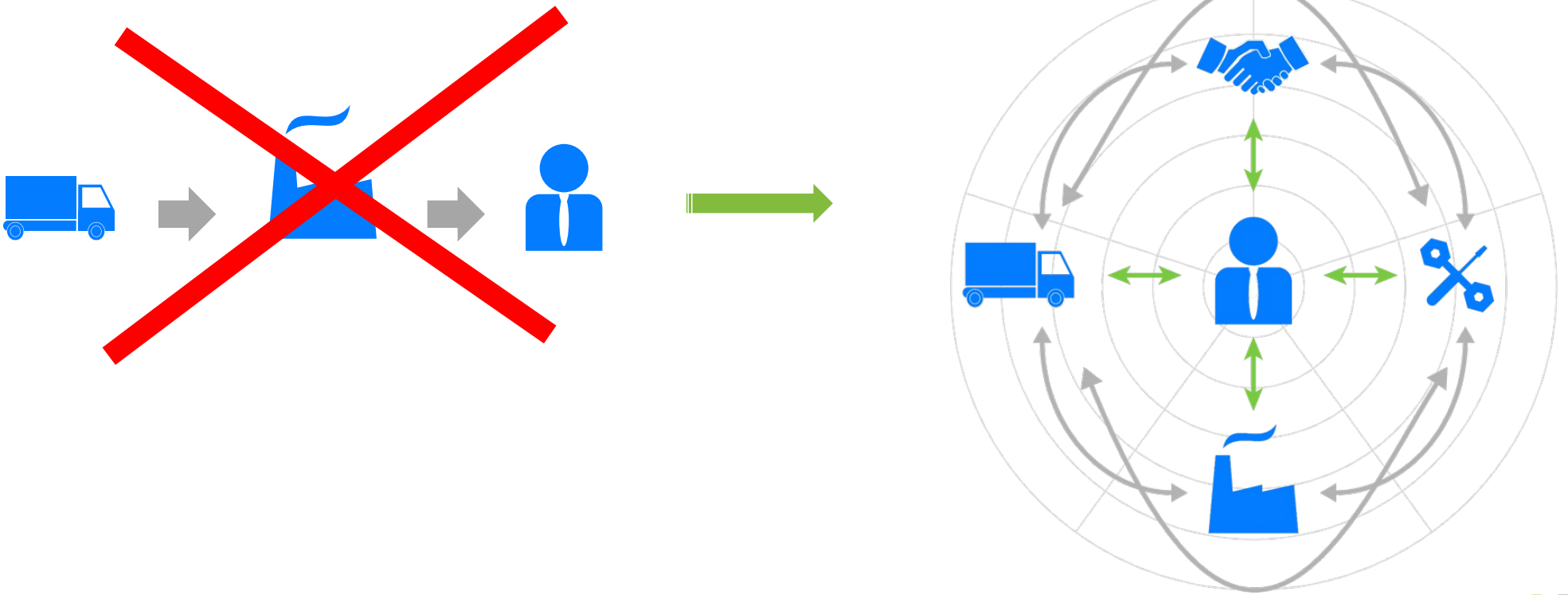
Wechsel von festen & bewährten Vertrauensbeziehungen zu

Industrie 4.0

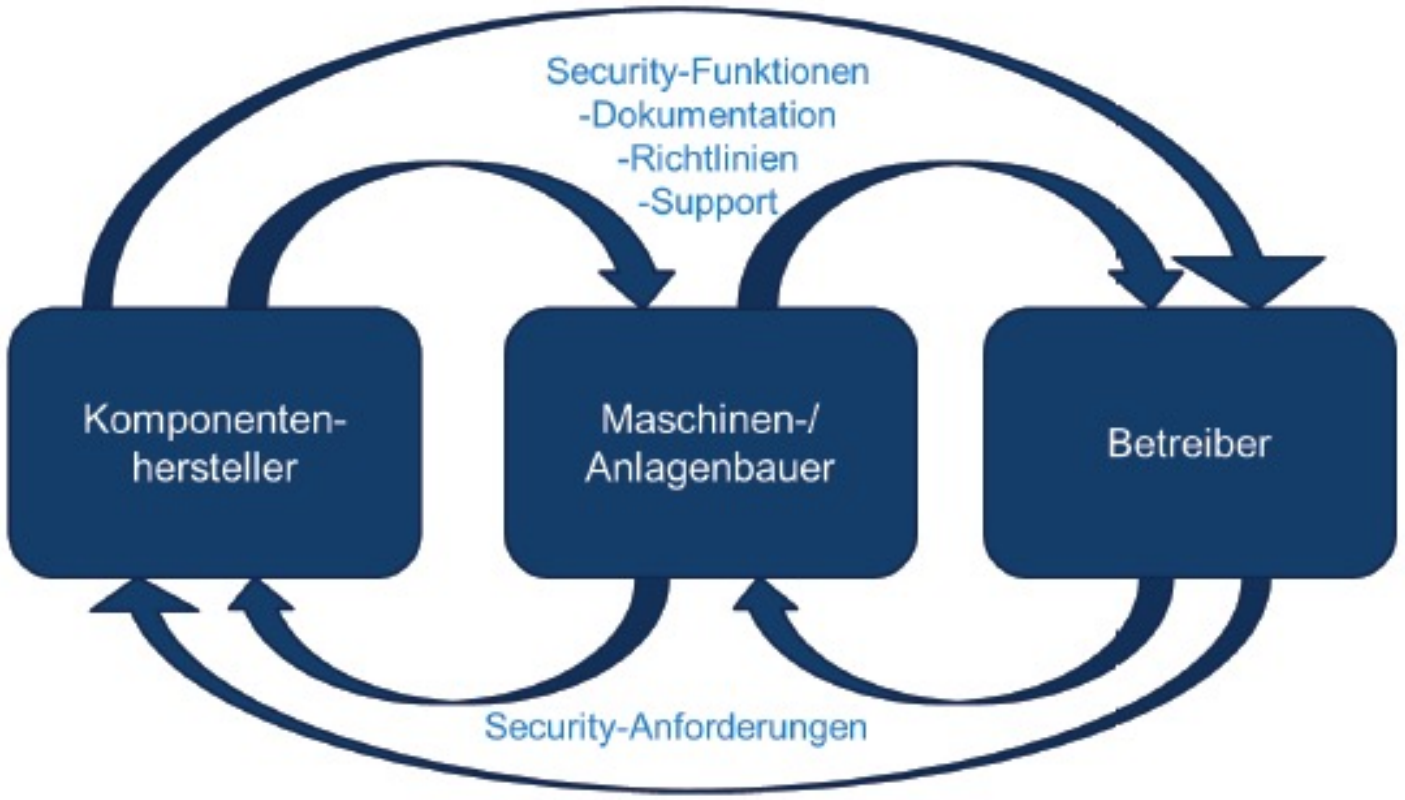


flexiblen, teils noch wenig bekannten Kommunikationsbeziehungen

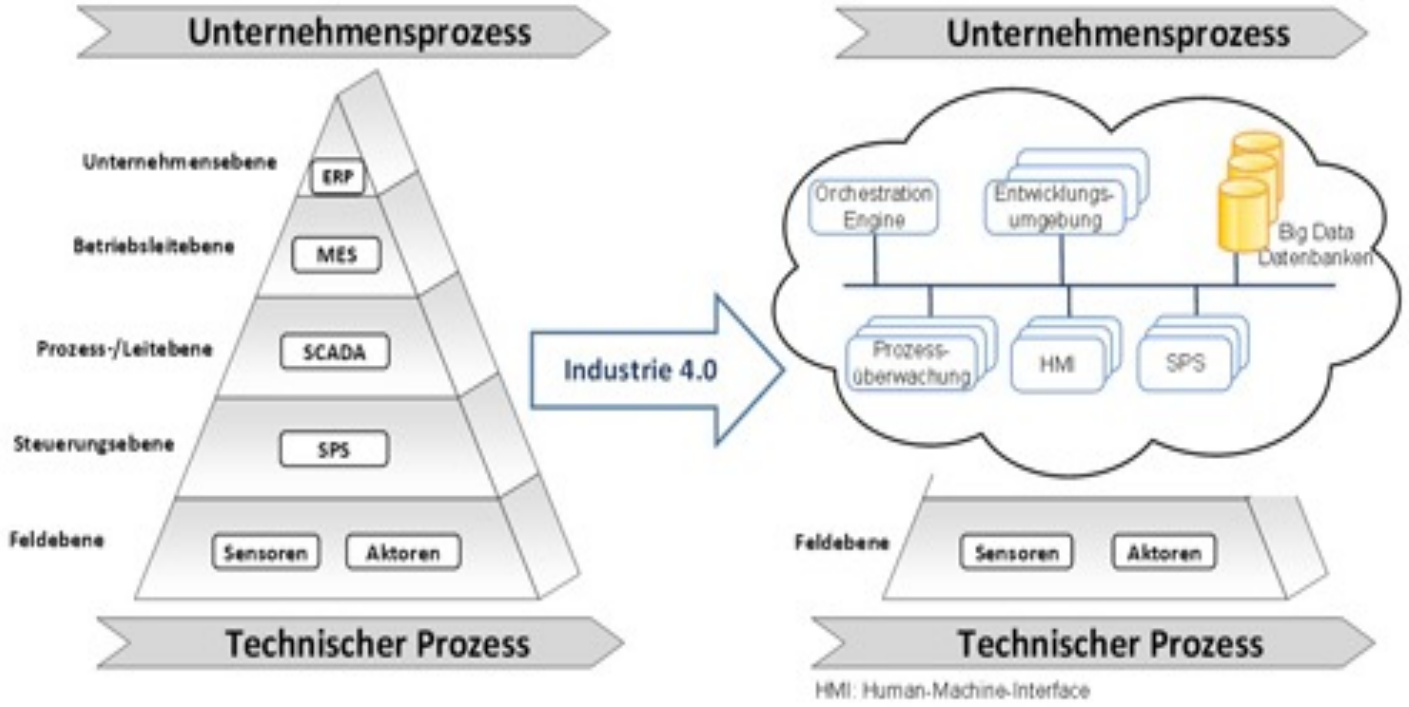
Veränderung der Wertschöpfungskette



Lieferketten – Anforderungen steigen



einhergehende Auflösung der Automatisierungspyramide



HMI: Human-Machine-Interface

Big Picture

Analyse Geschäftsprozesse

Teilprozess 1 | Teilprozess 2 | Teilprozess 3 | Teilprozess 4 | Teilprozess 5 | Teilprozess 6

Verfahrensprozess Produktionsprozess

Ermitteln Maximum tolerable period of disruption (MTPD)

Ermitteln Recovery Time Objective (RTO)

Identifikation notwendiger Services

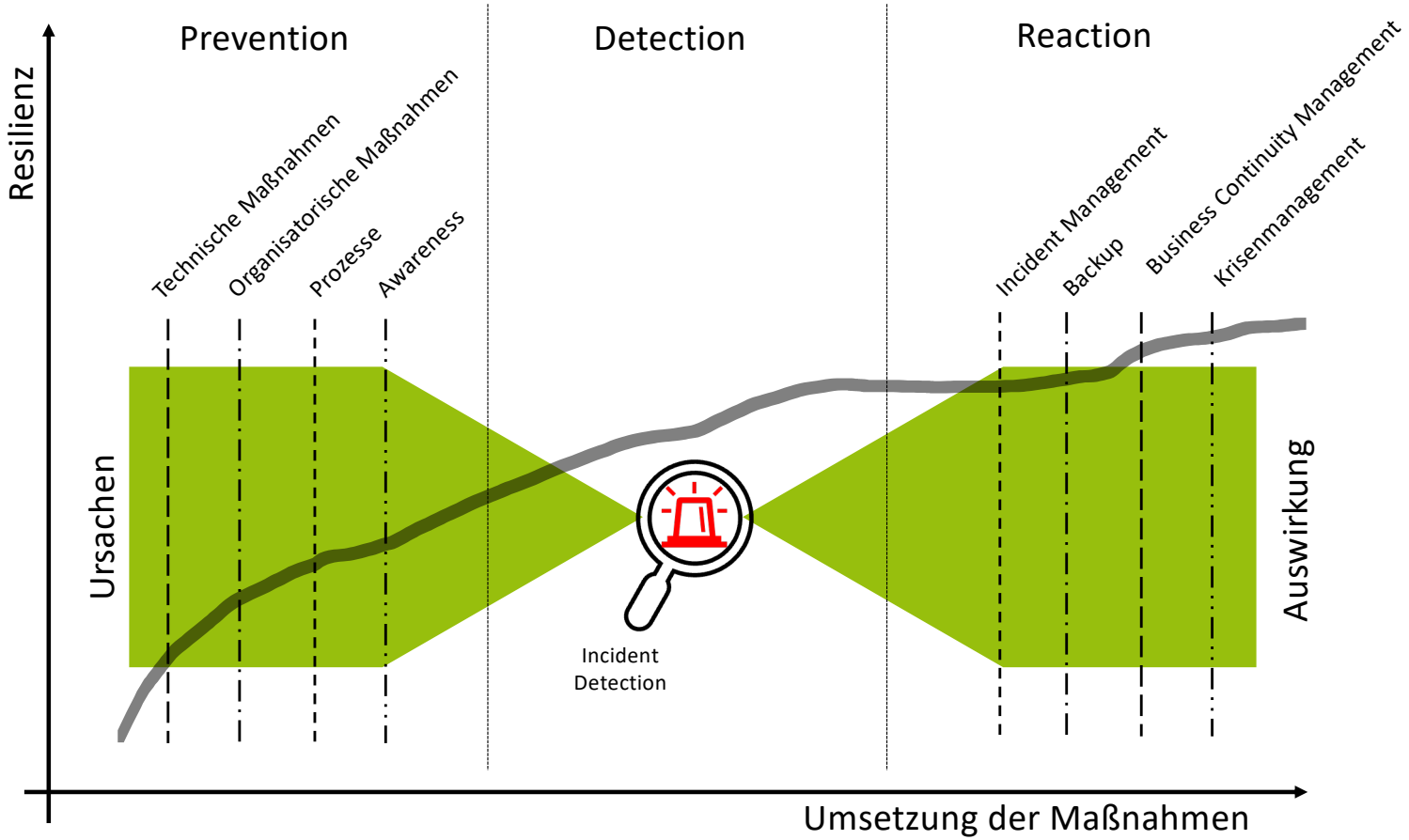
z.B. Hosting Services | z.B. Entwicklung | z.B. Support | z.B. Cloud-Services

Service- und Funktionsebene

Zuordnung IT- und OT Systeme

Systemebene

Cybersecurity - Resilienzmodell



Reaction

Mit dem Cyber-Sicherheitsnetzwerk soll

eine flächendeckende dezentrale Struktur aufgebaut werden,

die effizient und kostengünstig

KMU und Bürger bei

IT-Sicherheitsvorfällen Unterstützung anbietet.

…Rahmenbedingungen…Beispiele

ISO/IEC 27001

BSI-Grundschutz

IEC 62443

NIST

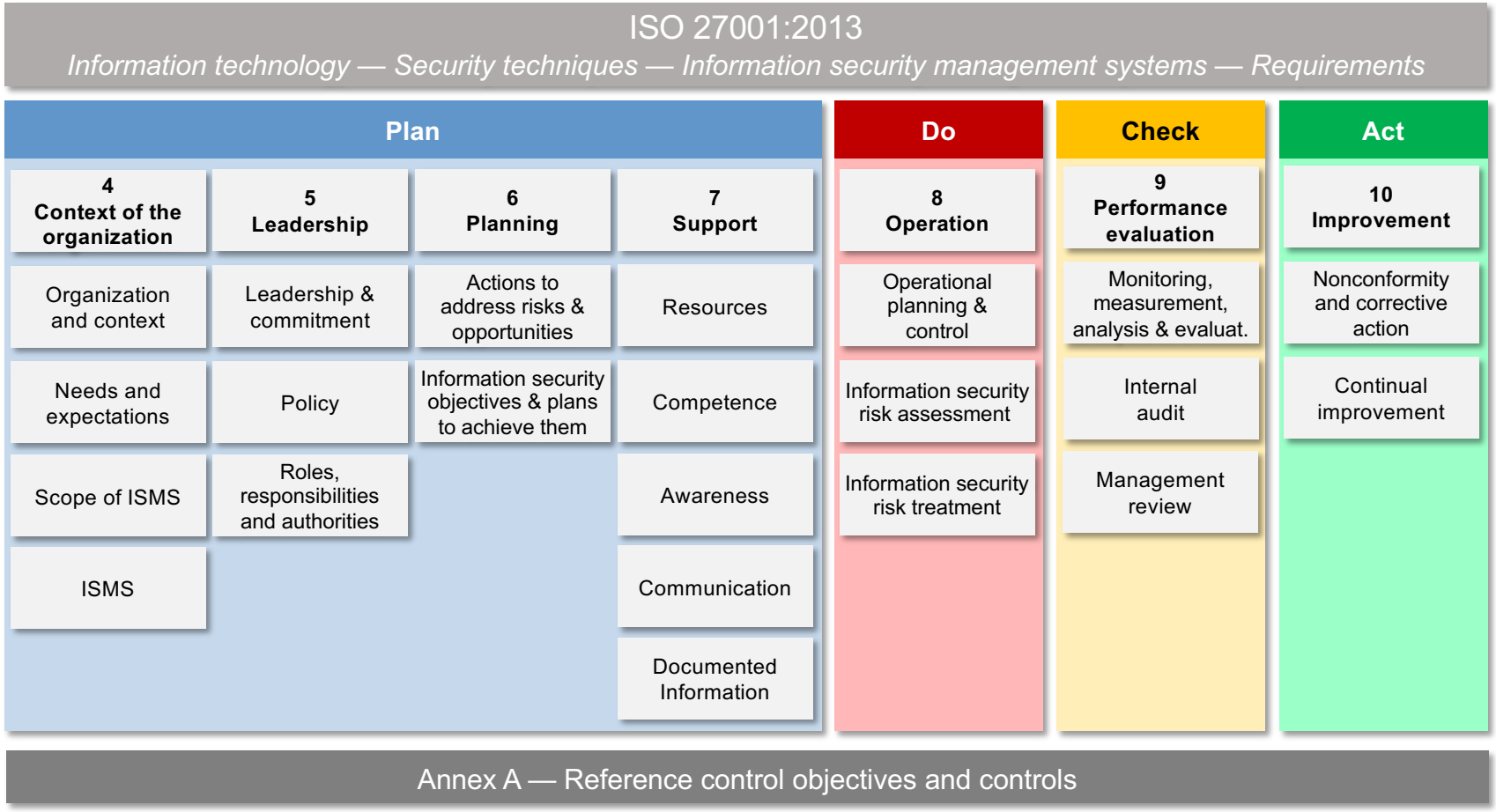
Branchenstandards

- DSGVO – Datenschutz-Grundverordnung
- IT-Sicherheitsgesetz 2.0
- KAS 51 Störfallverordnung Kommission für Anlagensicherheit

- Dienstleister & Lieferantenqualifizierung TISAX und individuelle Betreiber-Anforderungen
- EU NIS2 Cyber Security
- Cyber Resilienz Act

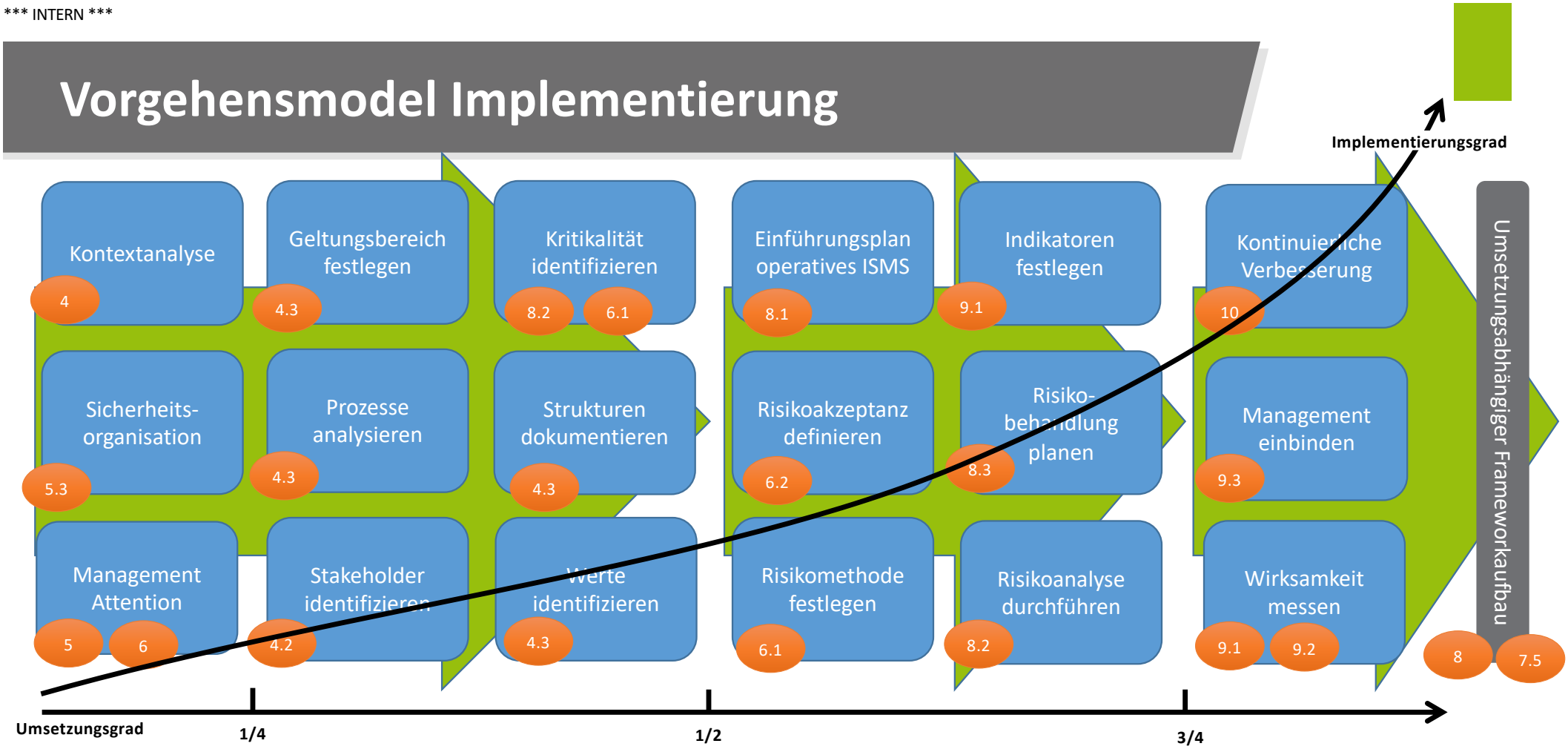
- Haftungsaspekte „Stand der Technik“
- Versicherungsanforderungen
- Gesetz zur Kontrolle & Transparenz im Unternehmen (KonTraG) internes Kontrollsystem aufzubauen.
- GmbH Gesetz

ISO 27001: 2013: PDCA-cycle Mapping



*** INTERN ***

Vorgehensmodel Implementierung



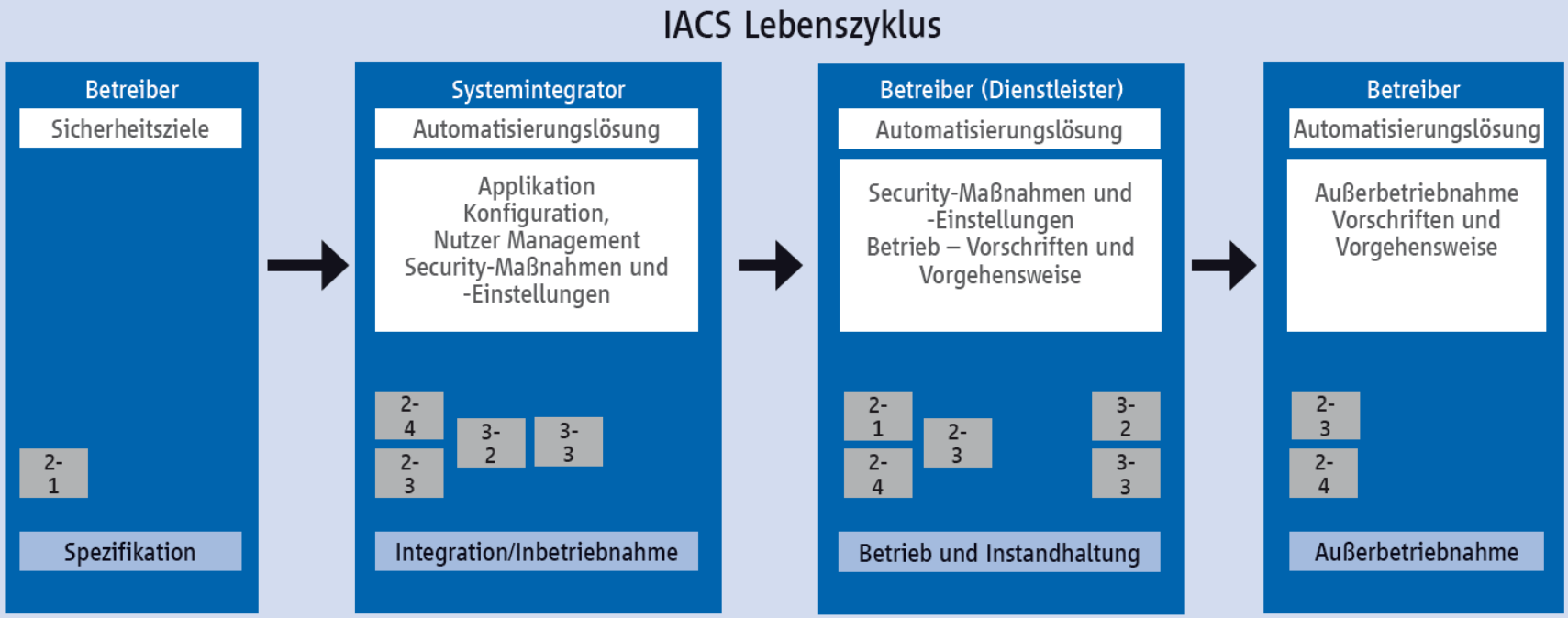
IEC 62443

IEC 62443
Industrial communication networks – Network and system security

General		Policies & Procedures		System		Component / Product	
1-1	Terminology, concepts and models	2-1	Requirements for an IACS security management system	3-1	Security technologies for IACS	4-1	Secure Product Development Lifecycle Requirements
1-2	Master glossary of terms and abbreviations	2-2	Implementation guidance for an IACS security management system	3-2	Security Risk Assessment and System Design	4-2	Technical security requirements for IACS components
1-3	System security compliance metrics	2-3	Patch management in the IACS environment	3-3	System security requirements and security levels		
1-4	IACS security lifecycle and use-case	2-4	Security program requirements for IACS service providers				

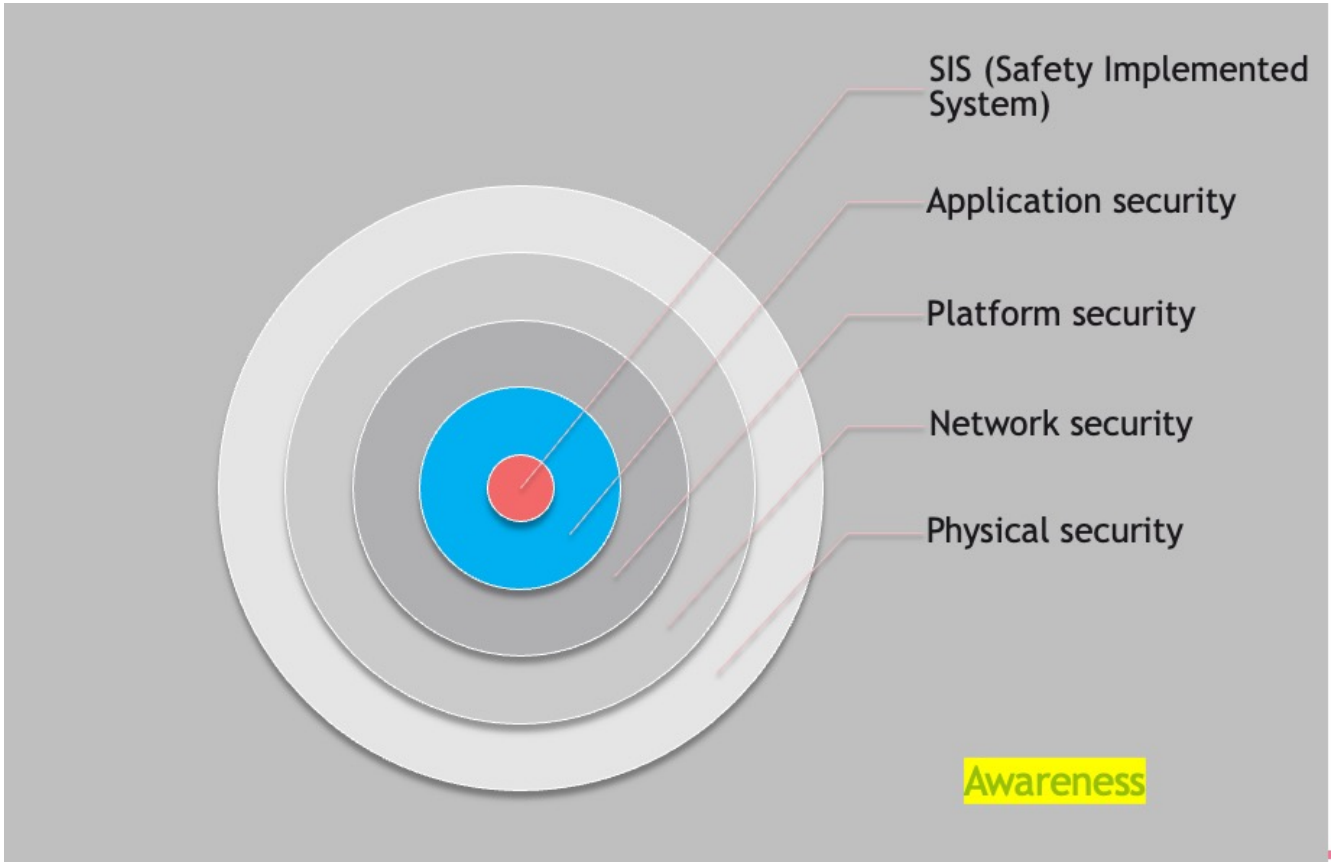
IEC 62443

Abbildung 4: Lebenszyklus und seine Zusammenhänge gemäß IEC 62443

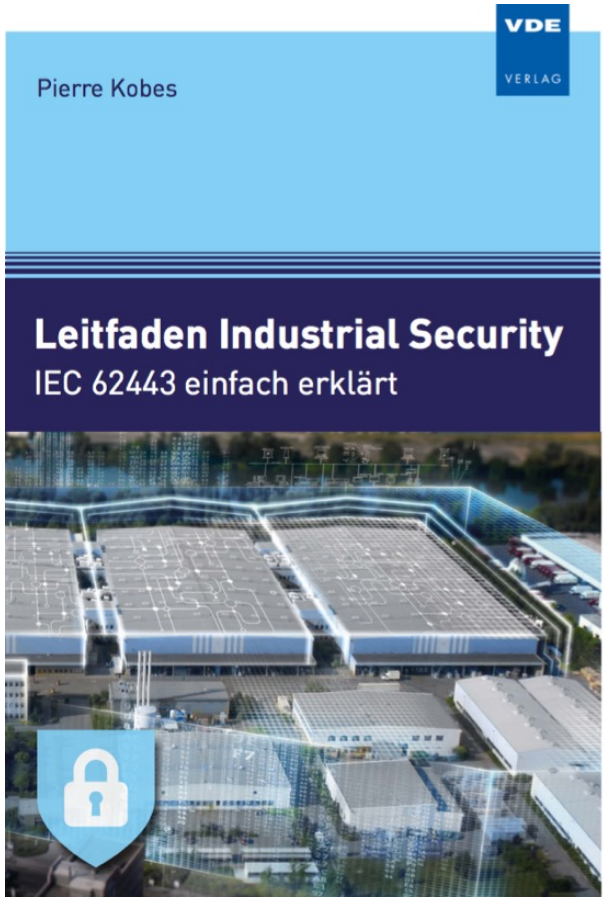


Quelle: ZVEI

IEC 62443 Defense in Depth Modell



IEC 62443



EU NIS2 Cyber Security

NIS 2 – Annex I und II

VDMA

Essential Entities

- Energy
  - electricity
  - district heating and cooling
  - oil
  - gas
  - hydrogen
- Transport
  - air
  - rail
  - water
  - road
- Banking
- Financial Market Infrastructures
- Health
- Drinking Water
- Waste Water
- Digital Infrastructure
- Public Administration
- Space

Important Entities

- postal and courier services
- waste management
- manufacture, production and distribution of chemicals
- food production, processing and distribution
- manufacturing
  - medical devices and in vitro diagnostic medical devices
  - computer, electronic and optical products
  - electrical equipment
  - machinery and equipment
  - motor vehicles, trailers and semi-trailers
  - transport equipment
- digital providers
  - online marketplaces
  - online search engines
  - social networking services platforms

size-cap rule: all medium & large enterprises that operate within these sectors / offer these services affected

Micro and Small Entities

in general:
- **excluded** from the scope of the Directive

exceptions:
- providers of electronic communications networks
- providers of publicly available electronic communications services
- trust service providers
- Top-level domain name (TLD) name registries
- public administration
- certain other entities

EU NIS2 Cyber Security

NIS 2 – die wichtigsten Punkte

VDMA

- Wichtige Unternehmen gem. Anhang II („Important Entities“)
- Betriebsgröße: ab 50 Mitarbeitern gem. Artikel 2
- Security „interner“ Systeme
  - Eigene IT-Systeme
  - Systeme für Dienstleitungen gegenüber Dritten
- Gewährleistung eines dem bestehenden Risiko angemessenen Sicherheitsniveaus (Stand der Technik) gem. Artikel 18
- Meldepflicht an Behörden innerhalb von 24 72 Stunden
- Cybersecurity-Schulung der Geschäftsführung gem. Artikel 17

EU NIS2 Cyber Security

NIS 2 – Artikel 18: Risikomanagement

VDMA

a) Risikoanalyse- und Sicherheitskonzepte für Informationssysteme;

b) Bewältigung von Sicherheitsvorfällen (Prävention und Erkennung von Sicherheitsvorfällen und Reaktion auf Sicherheitsvorfälle);

c) Aufrechterhaltung des Betriebs und Krisenmanagement;

d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren Anbietern oder Diensteanbietern beispielsweise Anbietern von Datenspeicher- und Datenverarbeitungsdiensten oder verwalteten Sicherheitsdiensten (MSS);

e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;

f) Konzepte und Verfahren (Erprobung und Prüfung) zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;

g) Einsatz von Kryptografie und Verschlüsselung.

K4

Cyber Resilience Act (CRA)

Der Cyber Resilience Act ist die erste EU-weite Rechtsvorschrift zur Cyberresilienz von Produkten mit digitalen Elementen. Die Erforderlichkeit begründet die Kommission mit den weltweit zunehmenden enormen Sicherheitsrisiken im IT-Bereich. So wird laut EU alle 11 Sekunden ein Ransomware-Angriff registriert.18.10.2022

Die neuen Regelungen betreffen alle Unternehmen, die Produkte mit digitalen Elementen herstellen. Darüber hinaus gibt es Verpflichtungen für Händler und Einführer. Größenbezogene Ausnahmen gibt es nicht.

Der am 15. September 2022 veröffentlichte Entwurf liegt derzeit dem Ministerrat und dem Europäischen Parlament zur Prüfung vor. Nach der Verabschiedung und Veröffentlichung im Amtsblatt der Europäischen Union wird der Cyber Resilience Act mit Übergangsfristen von 12 bzw. 24 Monaten in Kraft treten.

EU NIS2 & CRA

Bereich	IT	OT	Produkt
	NIS 2 Richtlinie		Cyber Resilience Act RED Delegated Act, MVO
Anwendungsbereich	Eigene IT-Umgebung	Eigene Fertigung	Zu verkaufende Produkte
Verantwortung	IT Abteilung	Betriebsleitung	Produktentwicklung
Systeme	Laptop, E-Mail, Webseite	MES, SPS, Fernwartung	„Vernetztes Produkt“, IoT-Dienste, Maschinen-Cloud
Betriebsprozesse	Eigene Prozesse		Kundenprozesse
Regulierungsrolle	Verwender, Nutzer		Hersteller, Diensteanbieter

NIST Framework

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?

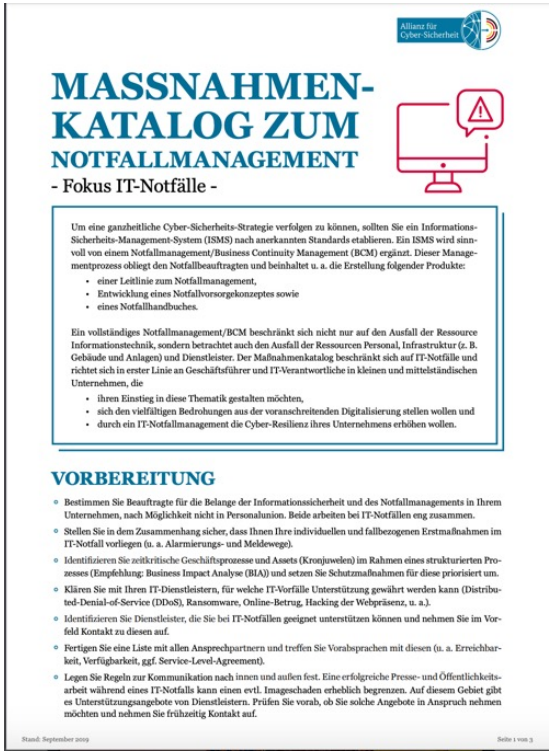
Wann ist das Ereignis eingetreten?

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:

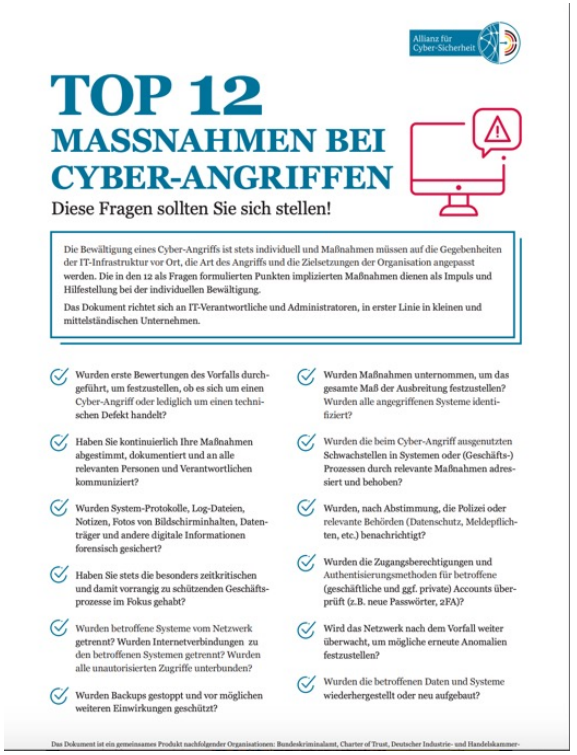
- einer Leitlinie zum Notfallmanagement,
- Entwicklung eines Notfallvorsorgekonzeptes sowie
- eines Notfallhandbuches.

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

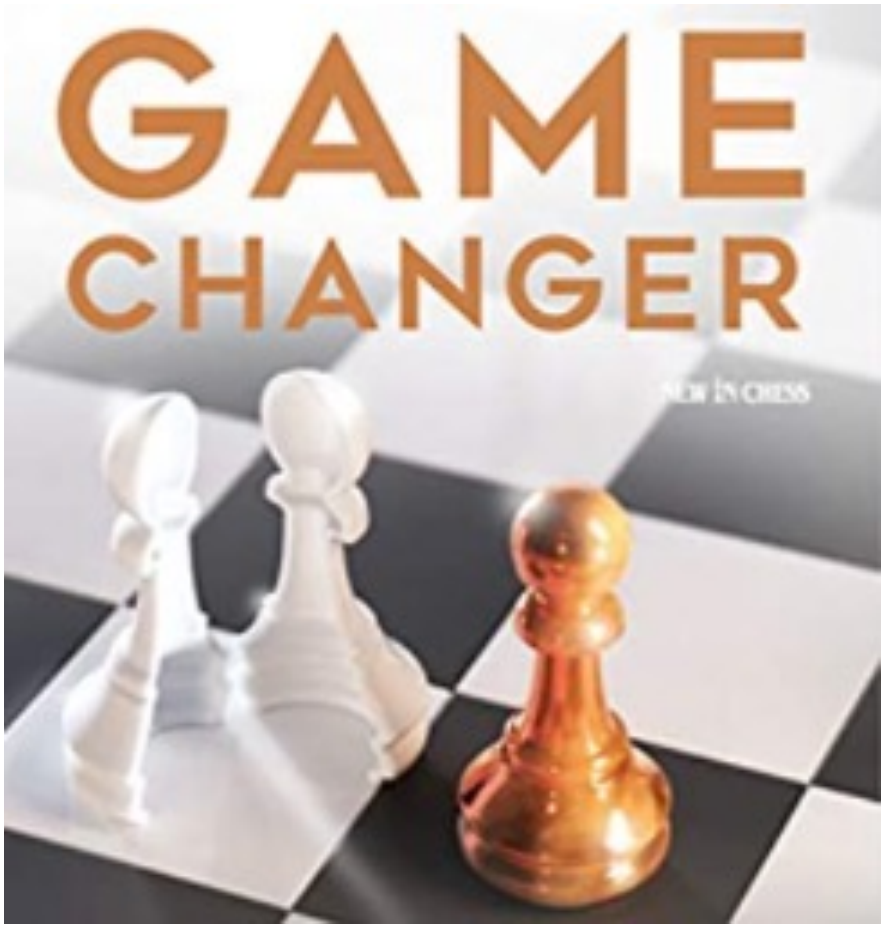
Diese Fragen sollten Sie sich stellen!

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?

…es braucht eine andere Qualität der Security…



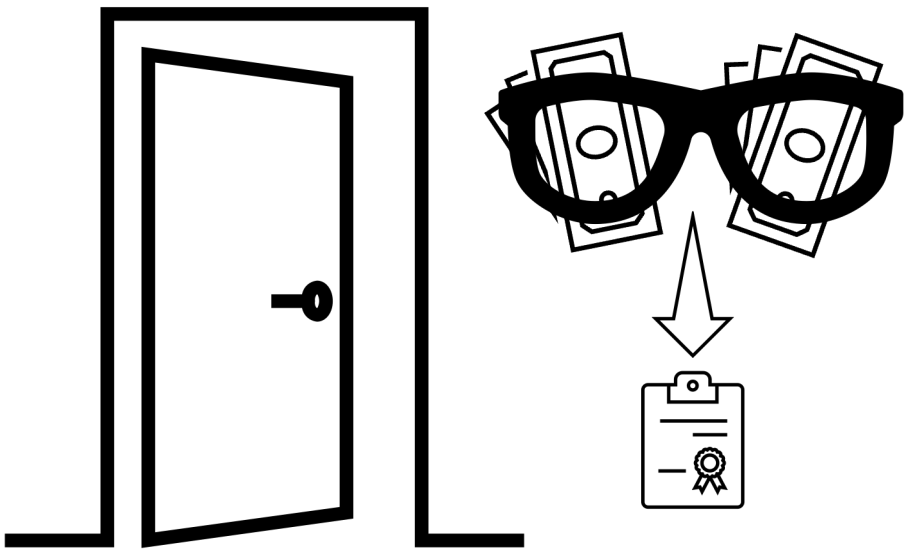
Analogie – Qualität Spaltmaß vers. Betriebssystem

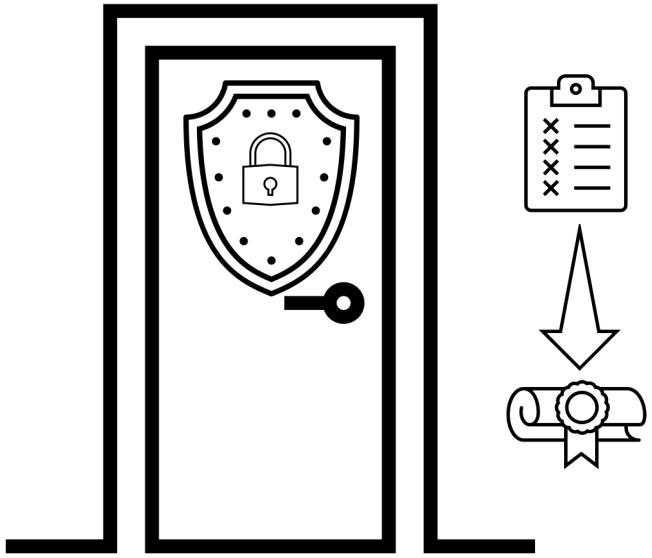
„Ich habe die miserablen Spaltmaße satt. Sie haben sechs Wochen, um Spaltmaße auf Weltklasse-Niveau zu entwickeln. Ich kenne die Namen von Ihnen allen. Wenn wir in sechs Wochen keine guten Spaltmaße haben, werde ich Sie alle ersetzen. Vielen Dank für Ihre Zeit.“ -Ferdinand Piëch

TESLA

Qualität wird neu definiert!

Scheinsicherheit vs. Sicherheit





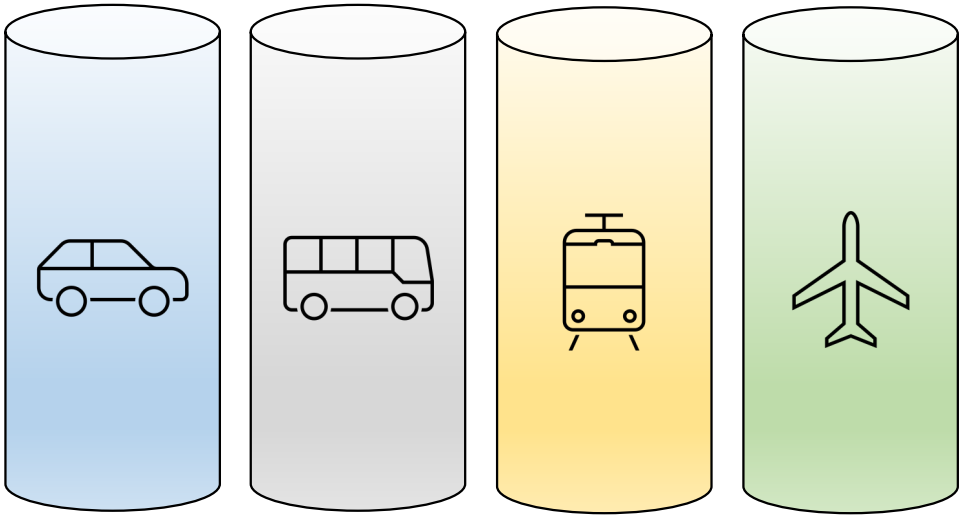
Scheinsicherheit vs. Sicherheit

Plattform Ökonomie, ECO-Systeme, Komplexität Prozesse & Dynamik, VUCA

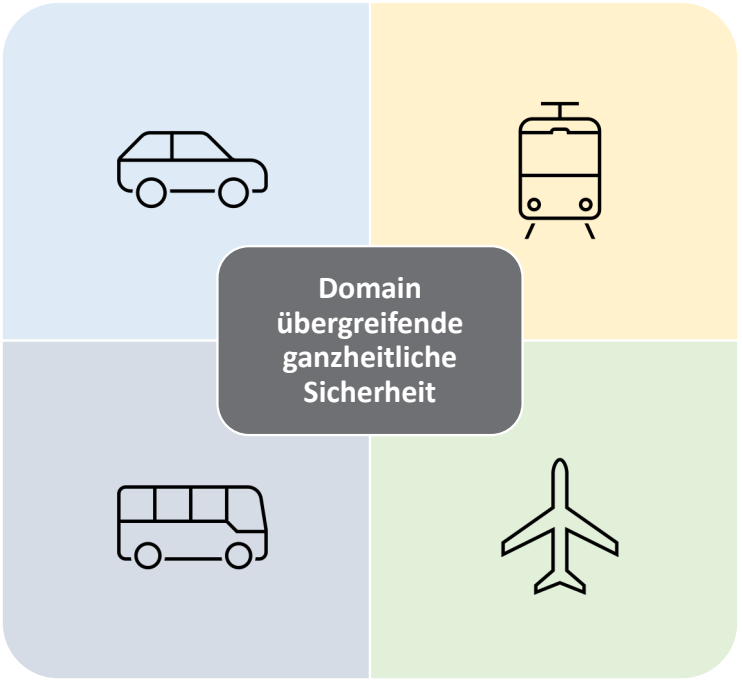
stärkere Automatisierung von Security

Sophisticated Sicherheit

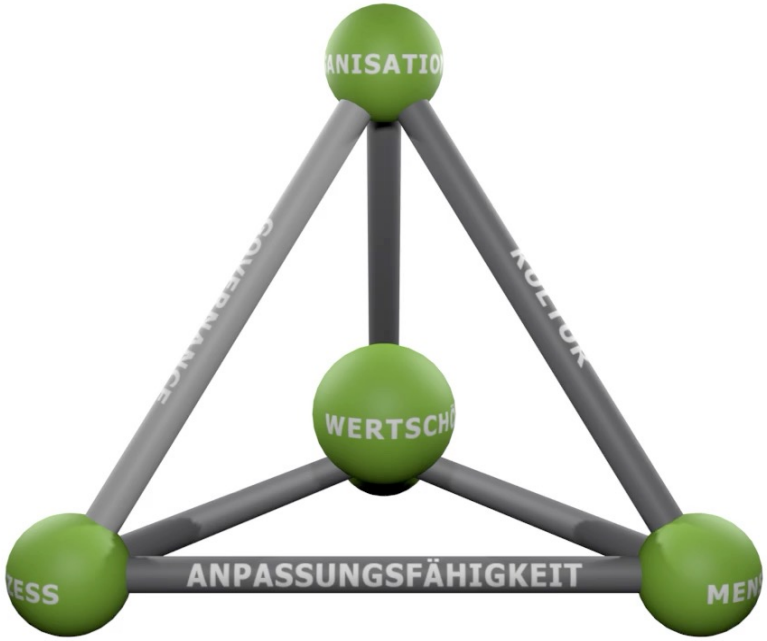
Domainspezifische Sicherheit



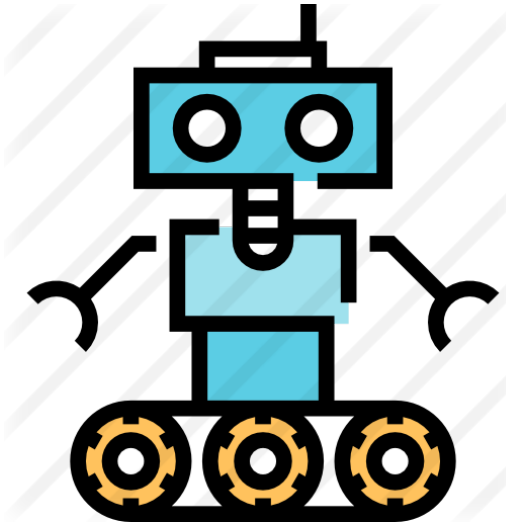
Mobilitätskonzept

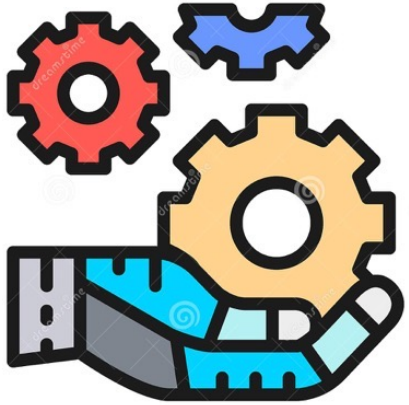


Ganzheitliche Betrachtung über die Wertschöpfungskette
Mensch – Organisation – Prozesse – Technologie



…wir scheitern aktuell nicht technologisch…

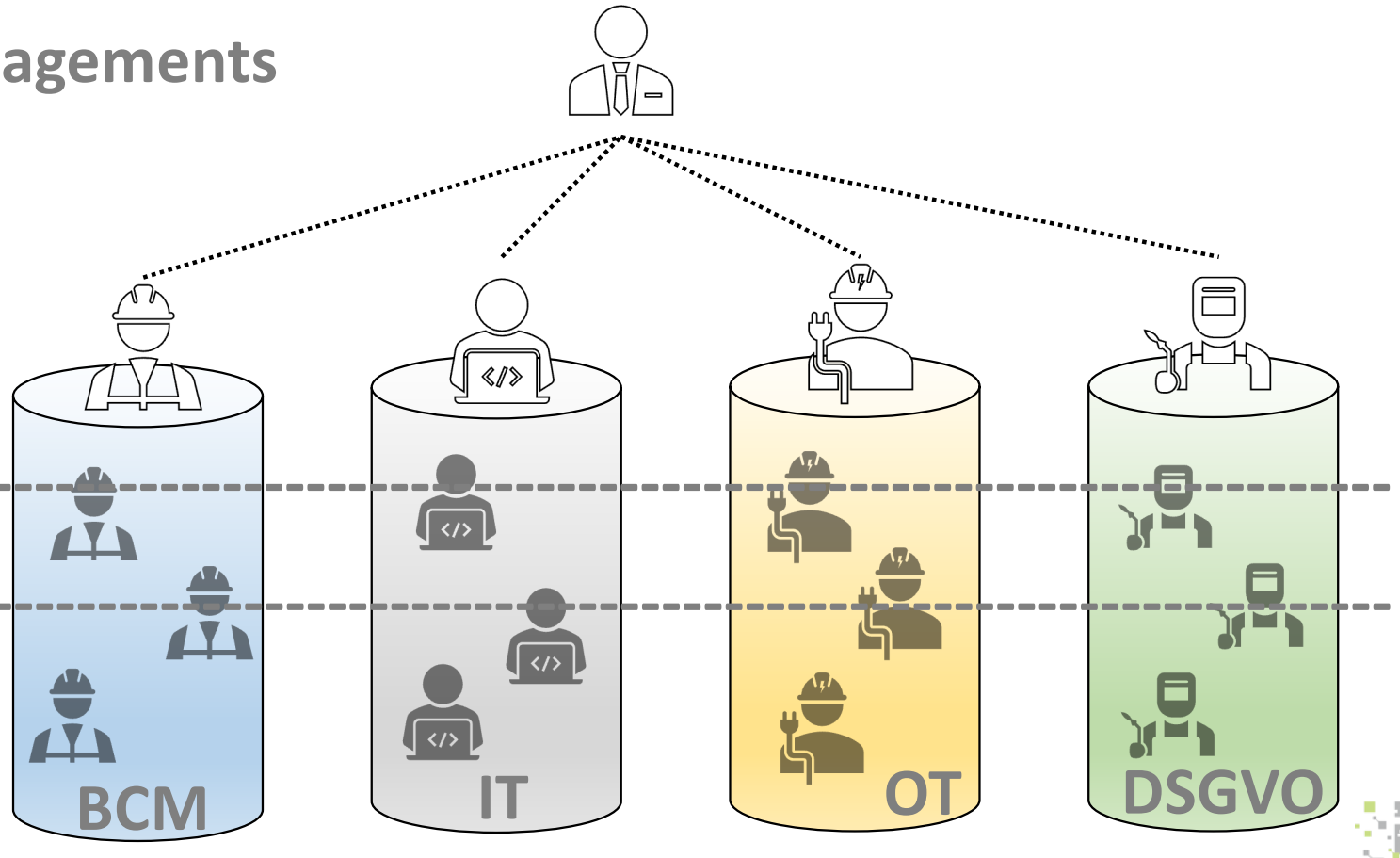




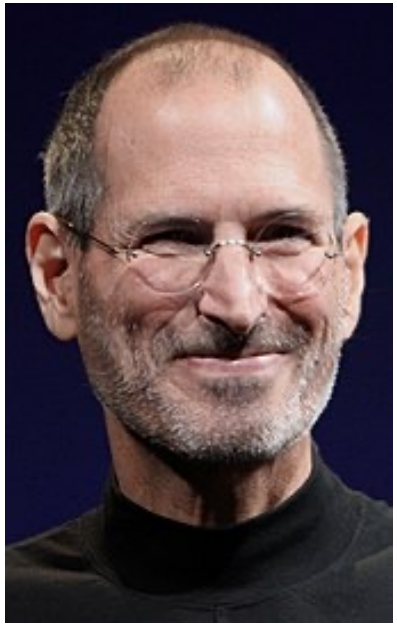
sondern in den Organisationen und weil das Management oft nicht dahinter steht!

raus aus den Silos!

Aufgabe des Managements

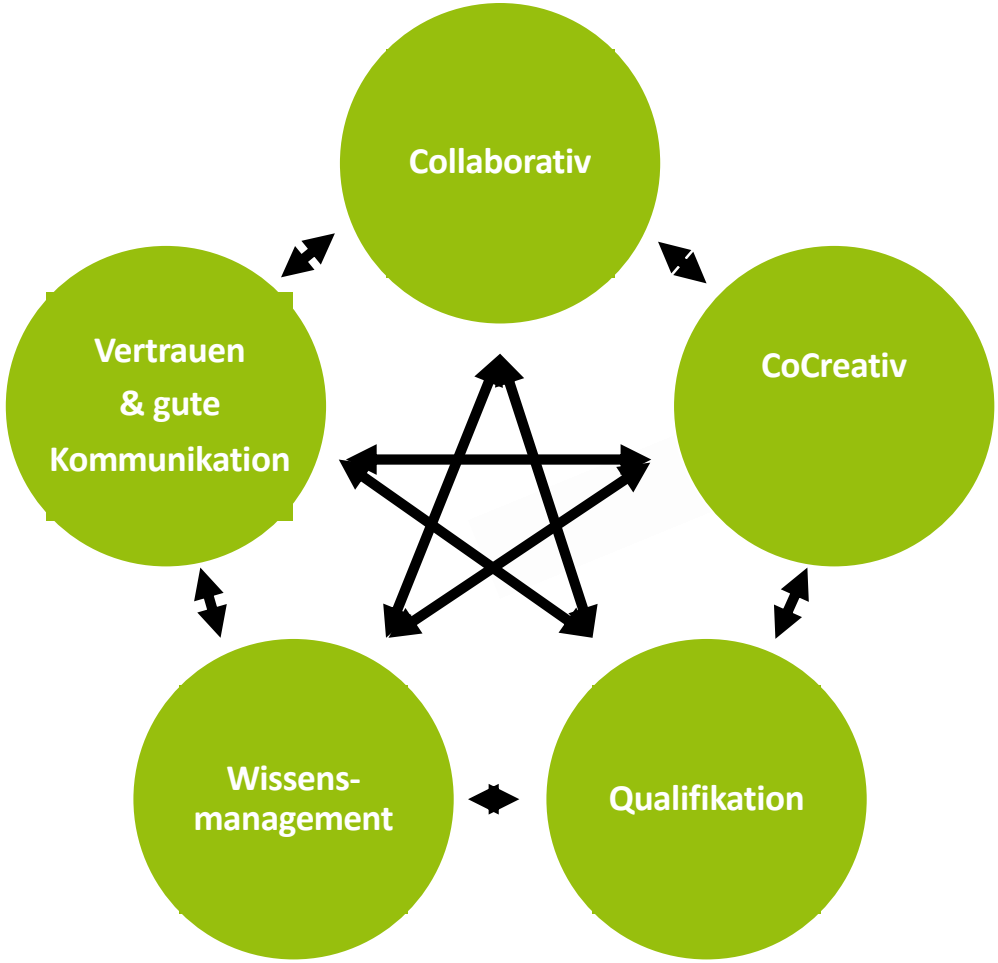


Was ist c(k)reativ?

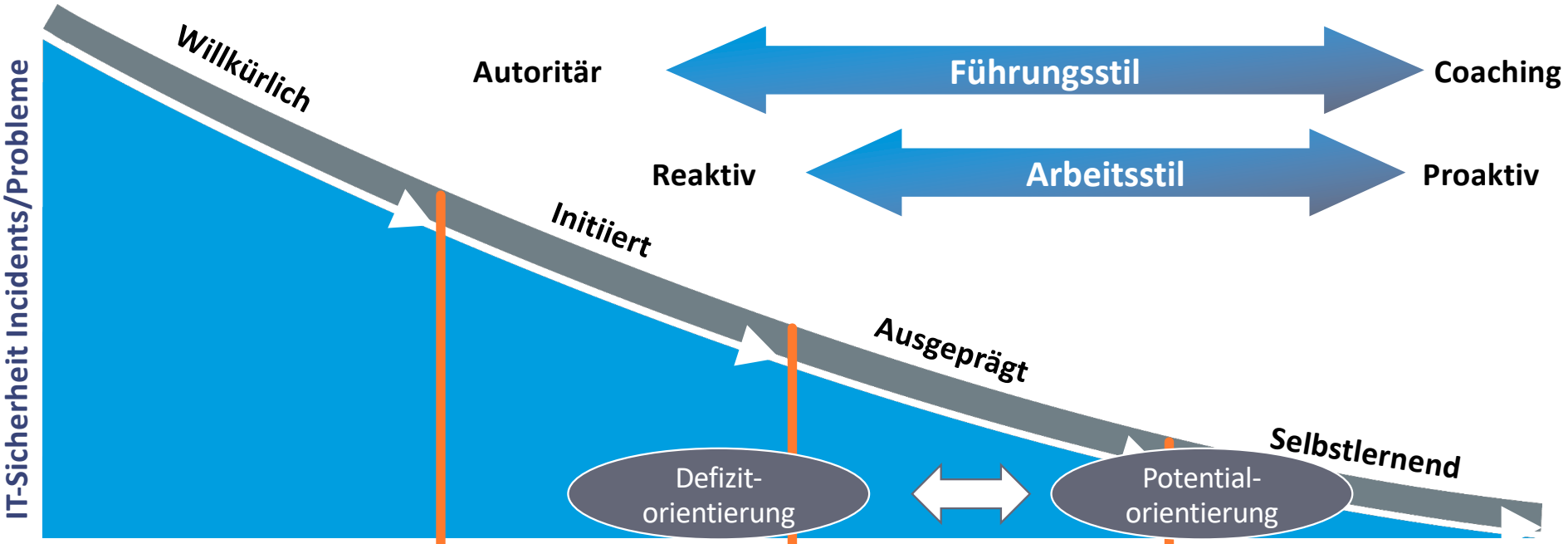


„Dinge miteinander zu verbinden“

Entscheidende Merkmale für eine neue Qualität von Cybersecurity!



Schlüsselfaktor Unternehmenskultur



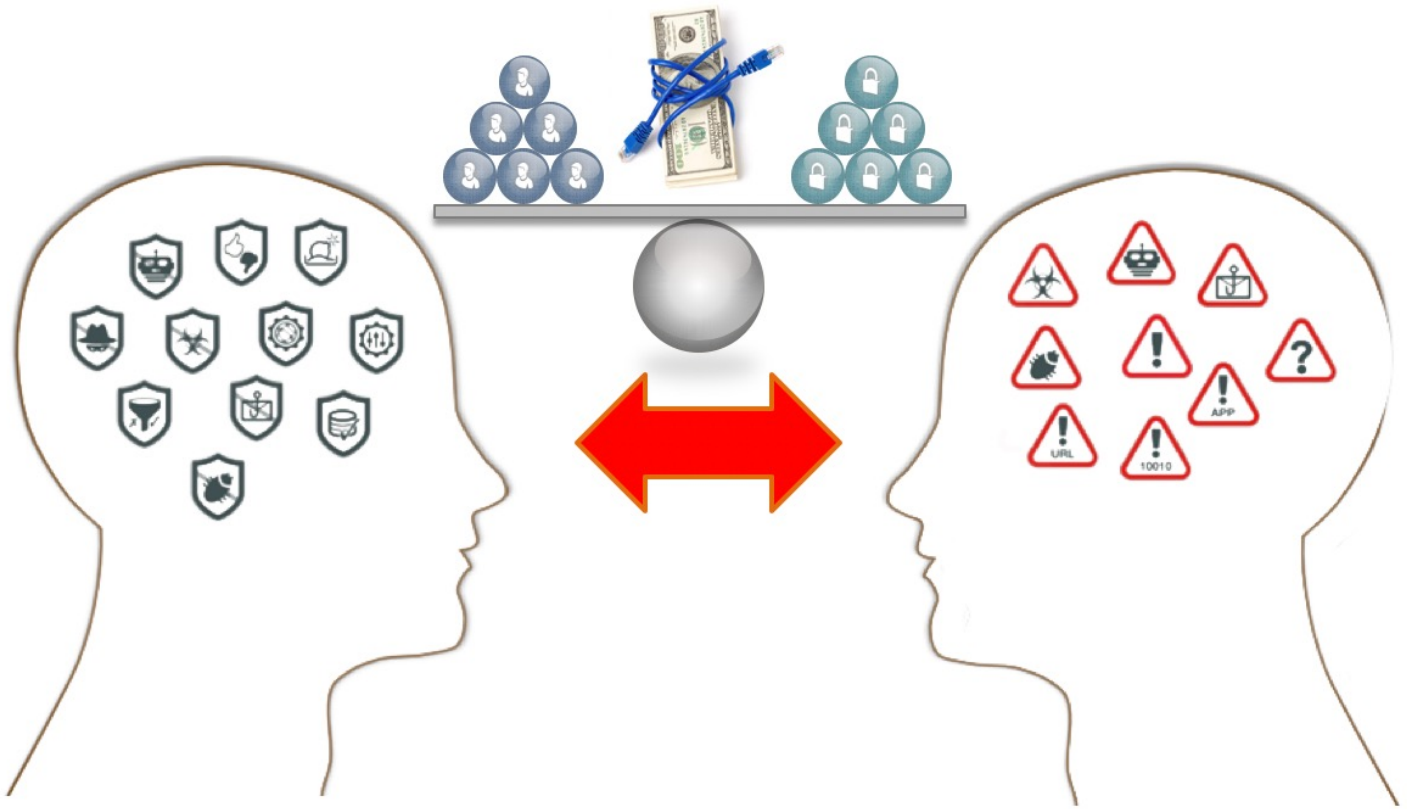
- Fehlendes Bewusstsein für ITS in der Organisation.
- ITS ist nicht definiert.
- Willkürliche Behandlung von IS-Vorfällen.
- Verantwortungen sind verwaist und Prozesse willkürlich gestaltet.
- ITS-Bewusstsein individuell.

- 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

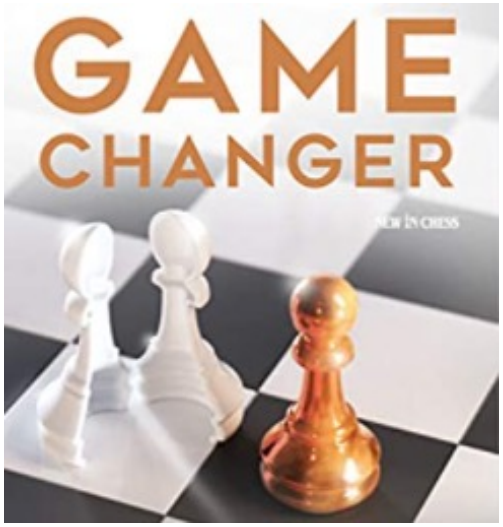
- Die Organisation lebt ITS.
- Externe sind nahtlos ins ISMS integriert.
- Resilienz stark ausgeprägt.
- Autonomes Anpassen an neue Gegebenheiten.
- Zukunftsorientierte Gestaltung.

Balance Security & Wirtschaftlichkeit

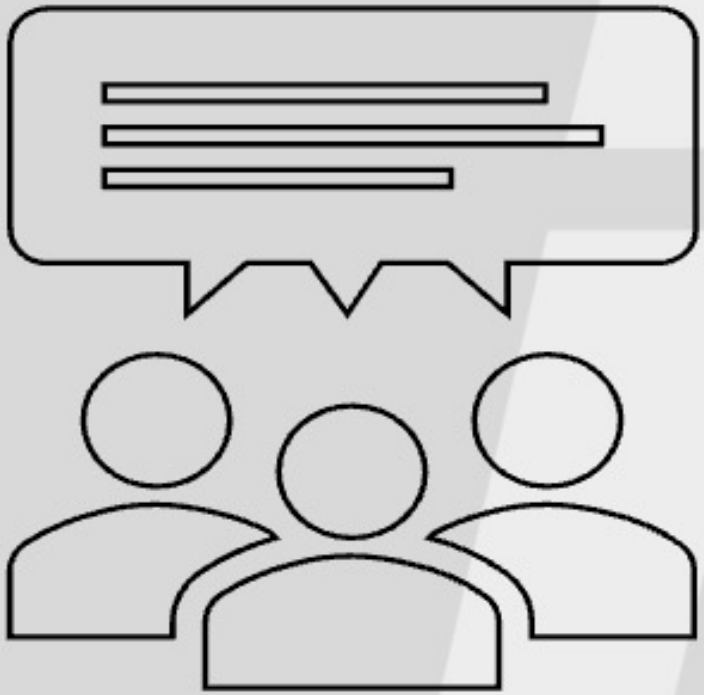


5 Empfehlungen im Kontext GAME CHANGER

- Schaffen Sie Organisationsverständnis – Kommunikation – Management & Kommittment!
- Gemeinsam den Weg beschreiten...
- Ganzheitlicher Ansatz Big Picture
  Fokus Mensch - Organisation – Prozesse – Technology
- Best Practices
- Konzept Ambidextrie



saaris
saarland.innovation&standort e.V.



Start September 2017

ca. 6 Termine / Jahr

AK Industrial IT-Security wird durchgeführt von

saarland.innovation&standort e. V., in Kooperation mit K4 DIGITAL GmbH

Staatskanzlei SAARLAND

Europäische Union
EUROPÄISCHER FONDS FÜR REGIONALE ENTWICKLUNG

Warum tun wir das?

Learning from Experts

Wir möchten Wissen teilen

1 + 1 = > 2

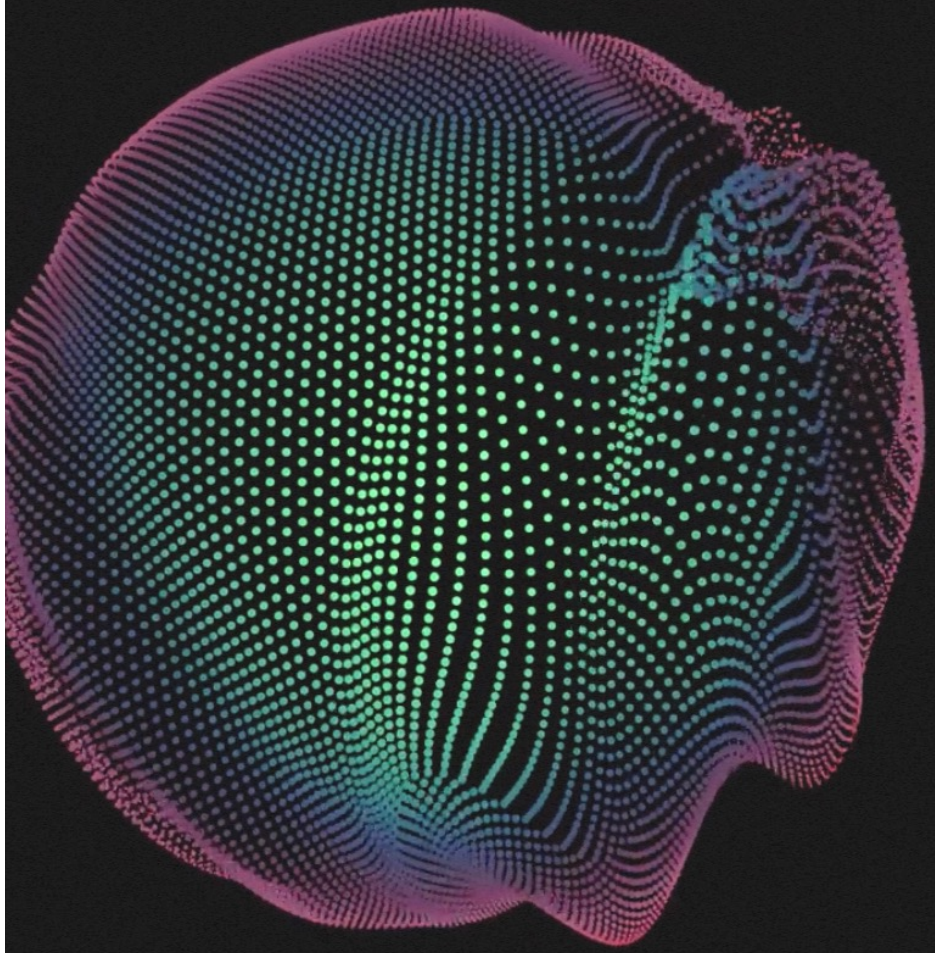
Entwicklung von Best Practices

Transfermaßnahmen & Handlungsempfehlungen

Arbeitskreis Industrial IT-Security

saarland.innovation&standort e. V.
Franz-Josef-Röder-Straße 9 | 66119 Saarbrücken

Telefon: 0681 9520-474
Fax: 0681 5846125
E-Mail: sabine.betzholz-schlueter@saaris.de
Internet: www.saaris.de



CYBR360.

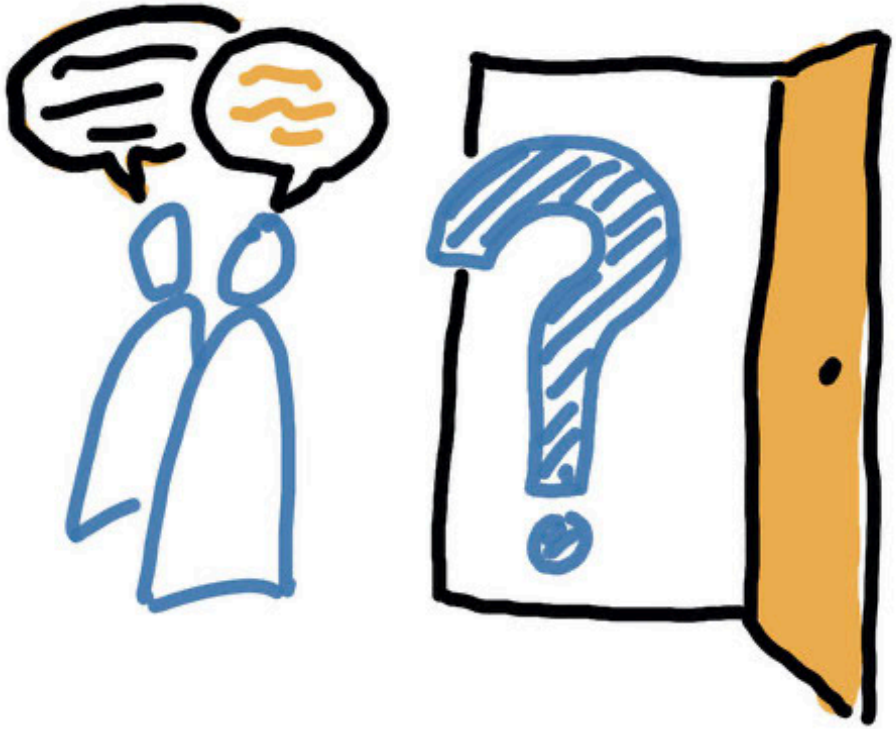
Die Initiative für digitale Sicherheit

Netzwerke schützen Netzwerke. Wir Saarländer wissen das. Mit dem Netzwerk CYBR360 schließen sich Fachexpert:innen aus Forschung, Beratung und Anwendung zusammen, um gemeinsam Präventionsangebote, Weiterbildungen und Lösungen vor allem für kleine und mittlere Unternehmen zu erarbeiten. Gemeinsam mit dem Bundesamt für SIcherheit in der Informationstechnik (BSI) und unseren Partner:innen aus der Großregion entwickeln wir außerdem geeignete Prozesse und Wege, um schnelle Hilfe zu vermitteln und die Schäden im Falle einer Cyberattacke zu minimieren.

CYBR360 geht auf die Initiative der Netzwerkstelle Digitalisierung (DiNet) der Landesregierung zurück. Als Netzwerk sind wir offen für Beratende, für Start-Ups und Forschende, für Unternehmen aus der Anwendung gleichermaßen wie aus der Entwicklung.

Ministerium für Wirtschaft, Innovation, Digitales und Energie
SAARLAND

Fragen



*** INTERN ***

Für Fragen
und Informationen:

K4 DIGITAL

Alfred-Nobel-Allee 38
66793 Saarwellingen

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