INDUSTRIE DIGITAL 2025

VORTRAG

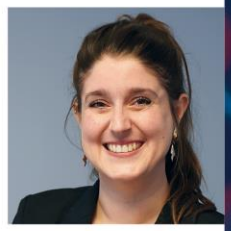
FORUM 5
IT-Security in Produktionssystemen – von der Achillesferse zum Schutzschild

d:e

Dr.-Ing. Karl Doreth
Berater & Entwickler digitaler Lösungen,
doreth:engineering

Dr.-Ing. Jan Brinkhaus
Berater für Industrie-Software & Dienste,
Brinkhaus GmbH

X4B



Dr.-Ing.
Sarah Majid Ansari,
Geschäftsführerin,
X4B Serviceagentur für die Wirtschaft GmbH

Maschinen gibt es nicht bei Mediamarkt!

IT-Security in Produktionssystemen

Dr.-Ing. Karl Doreth

d:e

Digitalisierung für Ihre Prozesse und Produkte!

Dr.-Ing. Karl Doreth

Berater für Software- und Digitalstrategien
im Maschinenbau

Kunden:

- Maschinenbauer & Produktionsbetriebe
- Hardware- & Softwarelieferanten
- Dienstleister im Maschinenbau

Zuvor:

- Leiter des digitalen Produktmanagements und der digitalen Vorentwicklung bei DMG MORI

- Gründer und Geschäftsführer des Mittelstand 4.0 Kompetenzzentrums für Niedersachsen und Bremen

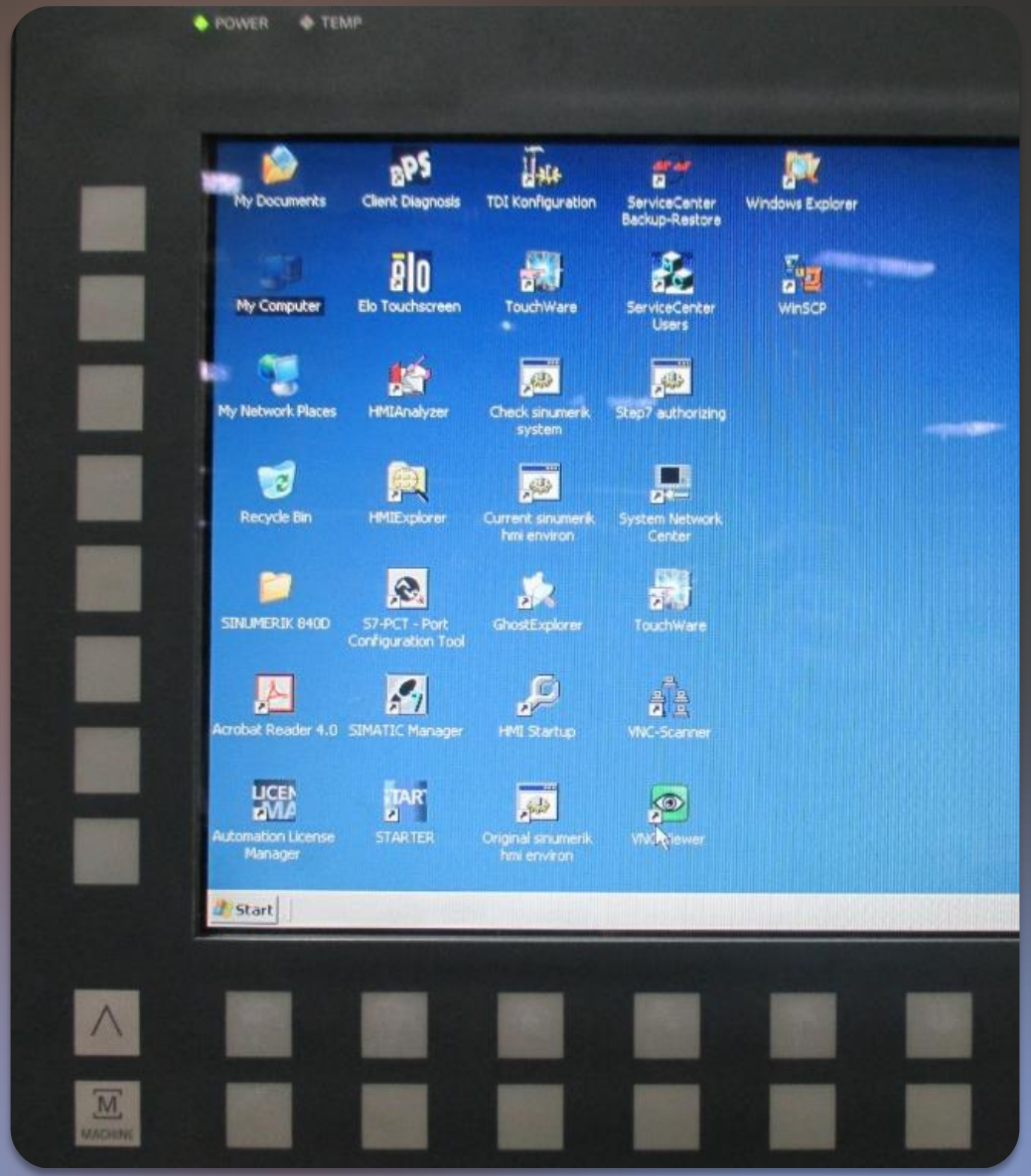
Warum reden wir überhaupt gesondert über die Produktion?

d:e

Windows 10 Umstellung steht an!

Was steckt in Maschinen?

Was steckt in Maschinen?



Was steckt in Maschinen?

Maschinenbeispiele:

- Heller H5000
  Baujahr 2006
  Windows NT 4.0 SP 2
- Sauer Ultrasonic 10
  Baujahr 2011
  Window XP (ohne SP)
- Gildemeister NEF 400
  Baujahr 2015
  Window 7 SP1
- Derzeit geliefertes Betriebssystem
  Windows 10 (seit ~ 2018)

Beitragstyp: **Produktmitteilung** Beitrags-ID: **109978320**, Beitragsdatum: **04.09.2025**

★★★½☆ (3)
> Bewerten

SIMATIC IPC Operating System Packages mit Windows 11 IoT Enterprise 2024 LTSC

Beitrag | Betrifft Produkt(e)

Für die SIMATIC IPCs werden nun auch Betriebssystempakete mit Windows 11 IoT Enterprise 2024 LTSC bereitgestellt.

SIMATIC IPC mit vorinstalliertem Windows 11 Betriebssystem ab Werk benötigen keine Aktivierung.
Alle Funktionen sind freigeschaltet wie bei einem aktivierten System.
Die SIMATIC IPC Operating System Packages erfordern eine Aktivierung (Online oder per Telefon).

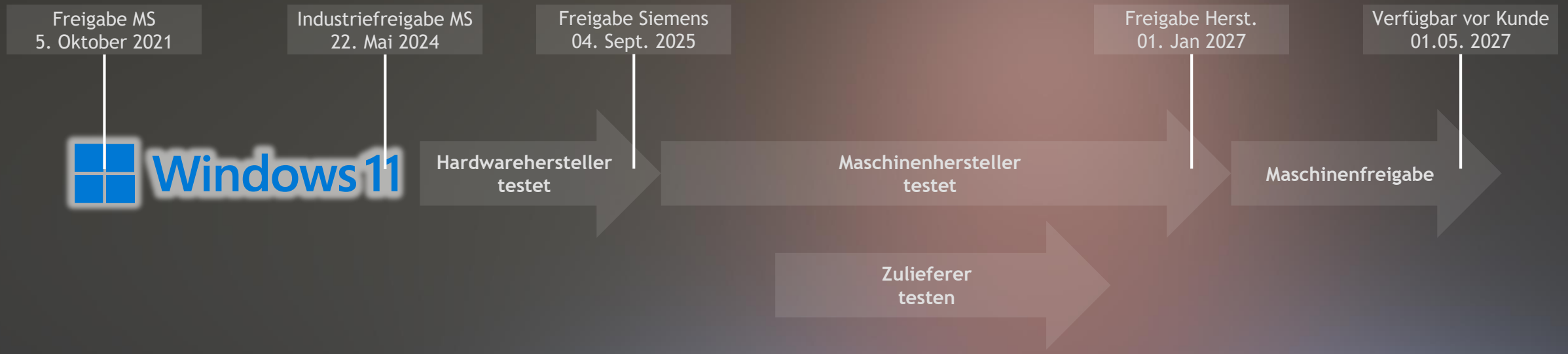
Der Preis eines Packages (mit USB Flash Drive) entspricht der einer Bestellung des Betriebssystems über den Konfigurator.
Die Lizenz deckt immer die für den jeweiligen IPC verfügbare leistungsstärkste CPU ab.

Die Lieferung erfolgt in einem Folienumschlag.
Das reduziert Verpackungsmaterial und die Größe der Versandverpackung (speziell bei der Bestellung von mehreren Packages).
Der COL ist nicht von außen sichtbar und nur über ein Öffnen des Umschlages erreichbar.

Die SIMATIC IPCs sind ab Werk mit verschiedenen vorinstallierten und einschaltfertigen Betriebssystemen bestellbar.

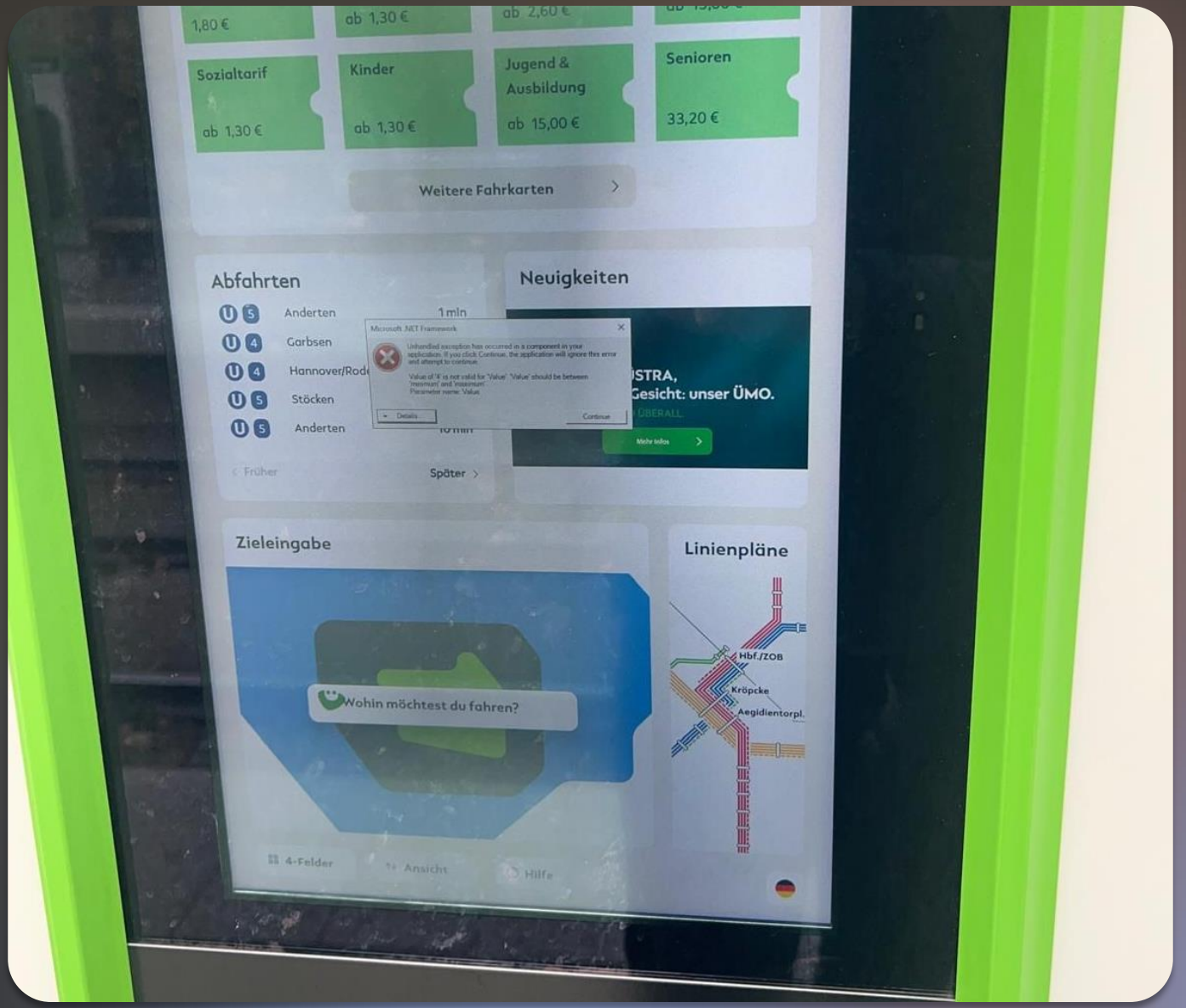
Für die aktuellen Geräte steht unter anderem Windows 10 IoT Enterprise 2016 LTSB, Windows 10 IoT Enterprise 2019 LTSC und auch Windows 10 IoT Enterprise 2021 LTSC zur Verfügung.

Dauer der Einführung eines neuen Betriebssystems (Prognose)



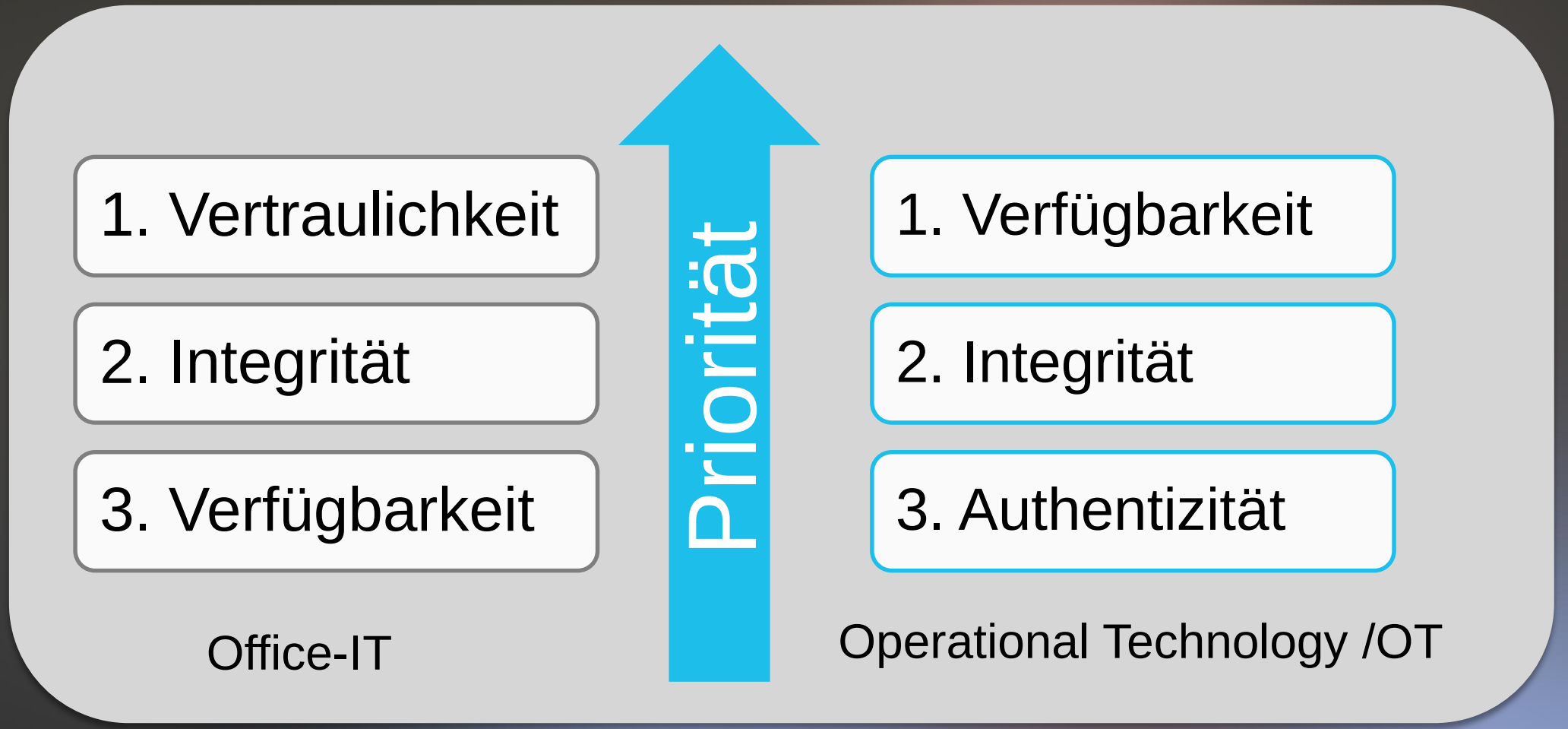
Zu wiederholen für jedes Update?

Alte Betriebssysteme in vielen „Geräten“



Alte Betriebssysteme in vielen „Geräten“

Priorisierung Schutzziele im Büro- und Produktionsbereich



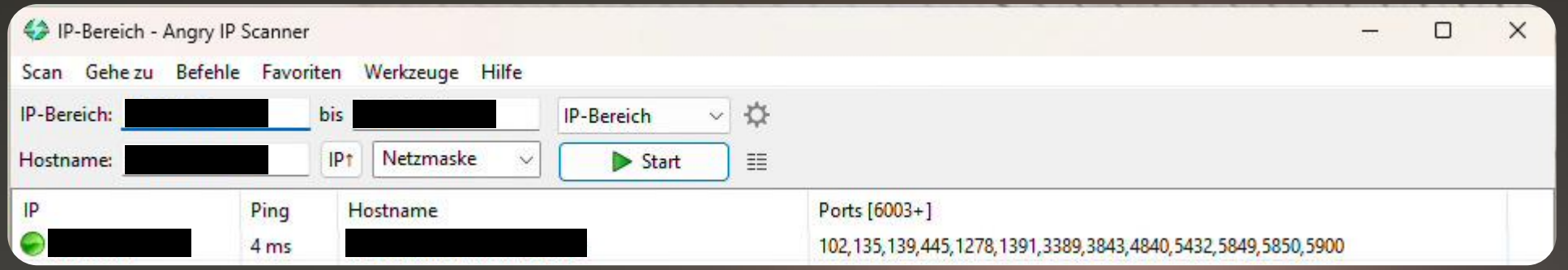
Quelle: Prof. Dr.-Ing. Karl-Heinz Niemann, HSH

Never

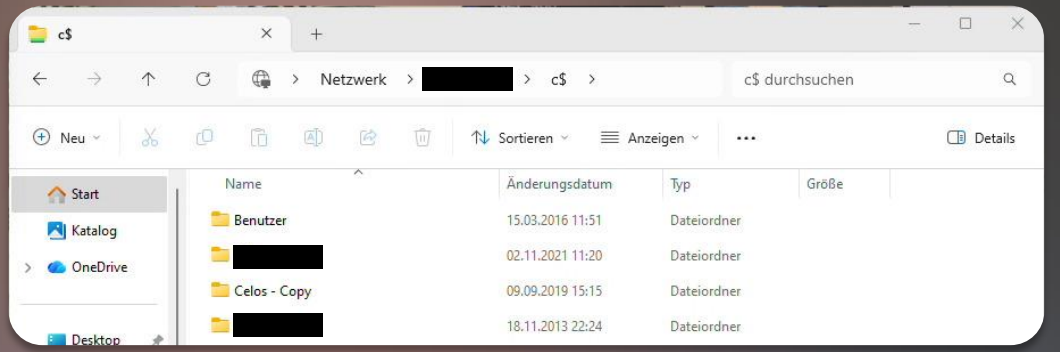
Never

Never change a running system!

Nahezu keine Sicherheitsmechanismen in Maschinen

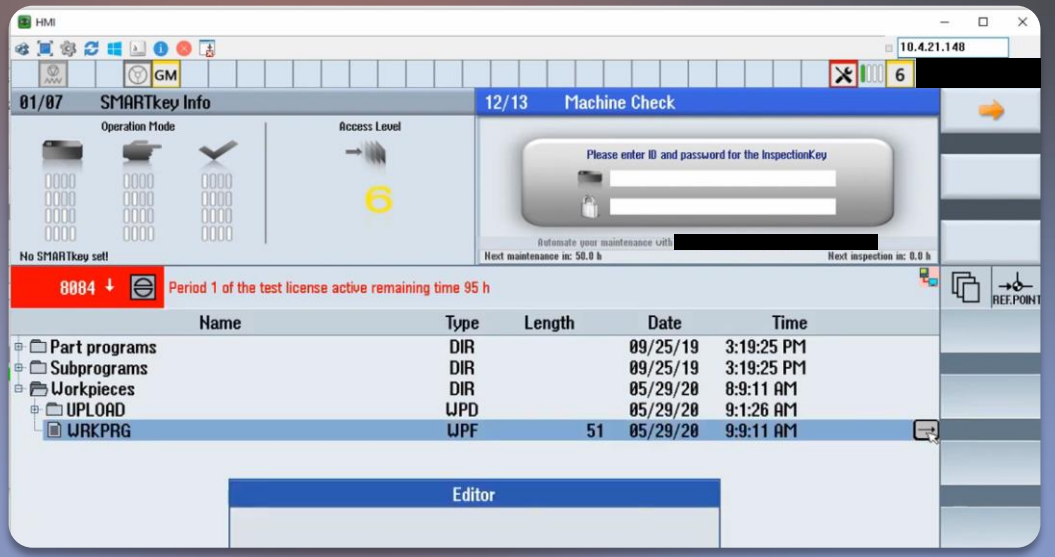


102
Siemens S7 (ISO-TSAP/COTP)
Keine Authentifizierung nötig!



139 + 445
Windows Datei- und Druckerfreigabe
Standardpasswort: XXXXXXX

5900
VNC (Virtual Network Computing) – remote desktop access
Standardpasswort: XXXXXXX

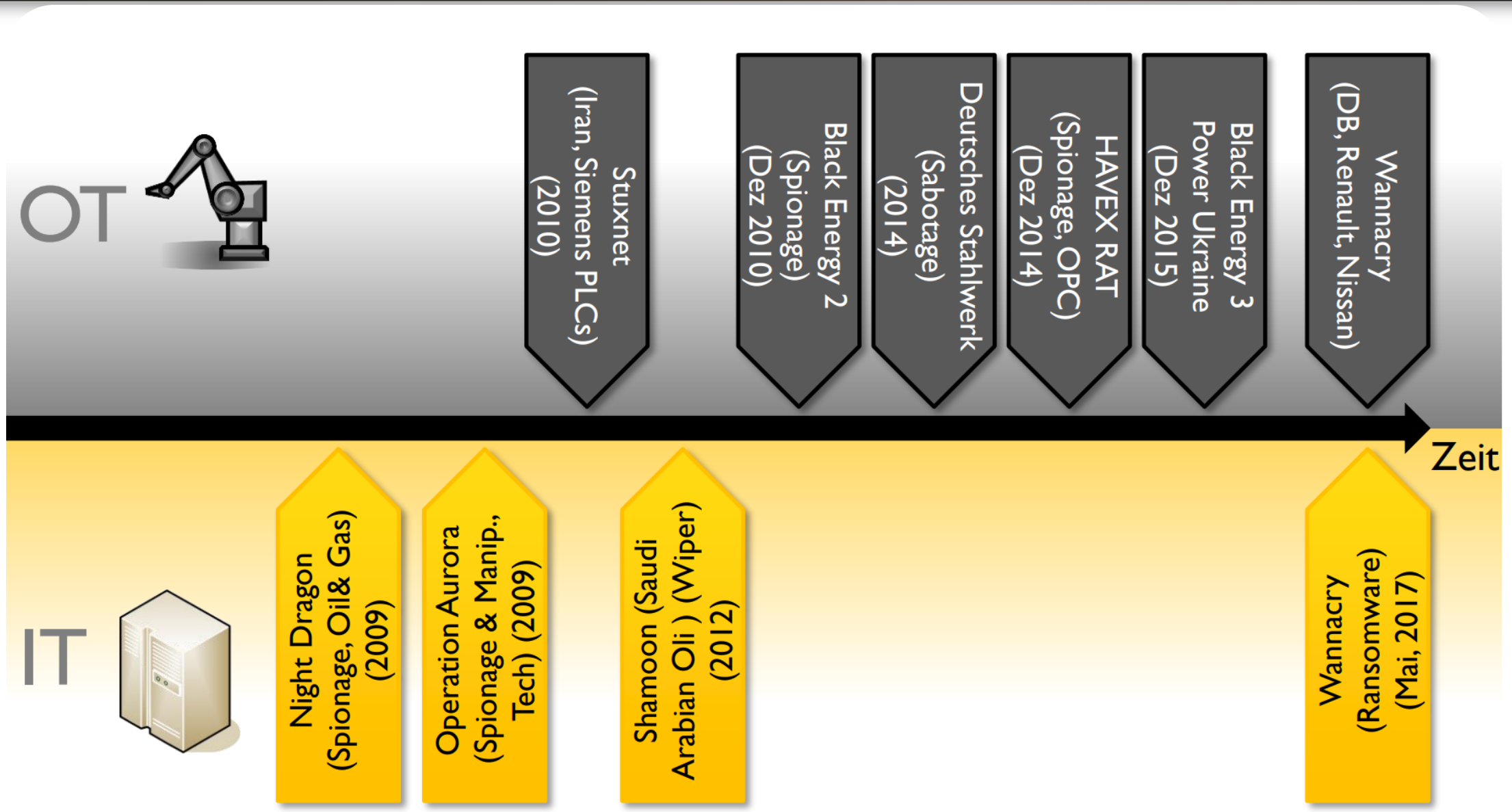


Warum Steuerungen einen Netzwerkanschluss haben

Wie groß ist
das Problem?

d:e

Industrieviren



Quelle: PROF. DR. TOBIAS HEER – HOCHSCHULE ALBSTADT SIGMARINGEN

Ransomware


Wanna Decryptor 1.0
Ooops, your files have been encrypted!
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)
You can try to decrypt some of your files for free. Try now by clicking <Decrypt>.
If you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
How Do I Pay?
Payment will be raised on
5/15/2017 16:25:02
Time Left
02:23:58:28
Your files will be lost on
5/19/2017 16:25:02
Time Left
06:23:58:28
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
QR Code
15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1
Copy
Check Payment
Decrypt

Wie groß ist das Problem?

$$P_1 \times P_2 \times I$$

Wahrscheinlichkeit
eines Angriffes

=

???

Wahrscheinlichkeit
eines Schadens

=

bei schlechtem Schutz
> 95 %

Schwere des Schadens
(Spionage, Sabotage, Erpressung)

=

Schäden:
Kosten für Produktionsausfall
Kosten für Instandsetzung
Kosten für Marktverluste

Was kann / muss man tun?

d:e

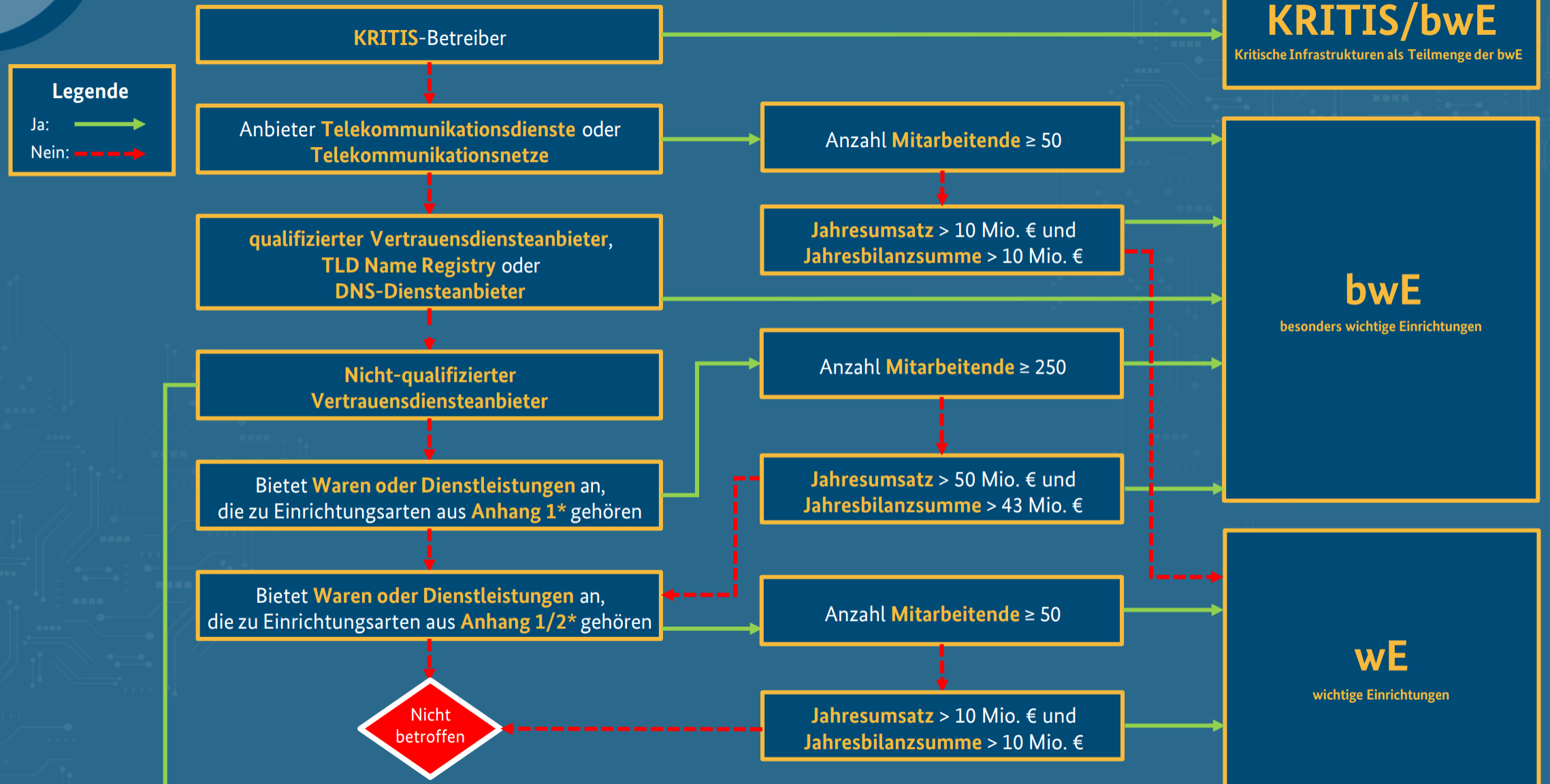
NIS-2 Umsetzungsgesetz

- Am 13.11.2025 im Bundestag beschlossen.
- Inkrafttreten ist Anfang 2026 avisiert.

- Registrierungspflicht
- Meldepflicht
- **Risikomanagementmaßnahmen**
  - Geeignet, verhältnismäßig, wirksam
  - Technisch und organisatorisch
  - Dokumentationspflicht
  - Ziel: Störungen der Verfügbarkeit, Integrität und Vertraulichkeit vermeiden
  - Muss alle informationstechnischen Systeme, Komponenten und Prozesse, die Unternehmen für die Erbringung ihrer Dienste nutzen, adressieren!

- Risikomanagementmaßnahmen mindestens:
  - Risikoanalyse
  - Bewältigung von Sicherheitsvorfällen
  - Aufrechterhaltung des Betriebs (z. B. Backup-Management, Wiederherstellung nach einem Notfall, Krisenmanagement)
  - Sicherheit der Lieferkette
  - Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen
  - Wirksamkeitsprüfung von Risikomanagementmaßnahmen
  - Schulungen und Sensibilisierung zu Cybersicherheit
  - Kryptographische Verfahren
  - Konzepte für Personalsicherheit (z. B. Zugriffskontrolle, Verwaltung von IKT-Systemen)
  - Multi-Faktor-Authentifizierung, gesicherte Kommunikation sowie ggf. Notfallkommunikation

#nis2know



*Anlage 1: www.bsi.bund.de/dok/nis-2-anlage-1 | Anlage 2: www.bsi.bund.de/dok/nis-2-anlage-2

NIS2 Maschinenbau (C28)

28			Maschinenbau	
	28.1		Herstellung von nicht wirtschaftszweigspezifischen Maschinen	
		28.11	Herstellung von Verbrennungsmotoren und Turbinen (ohne Motoren für Luft-und Straßenfahrzeuge)	2811
		28.12	Herstellung von hydraulischen und pneumatischen Komponenten und Systemen	2812
		28.13	Herstellung von Pumpen und Kompressoren a. n. g.	2813*
		28.14	Herstellung von Armaturen a. n. g	2813*
		28.15	Herstellung von Lagern, Getrieben, Zahnrädern und Antriebselementen	2814
	28.2		Herstellung von sonstigen nicht wirtschaftszweigspezifischen Maschinen	
		28.21	Herstellung von Öfen und Brennern	2815
		28.22	Herstellung von Hebezeugen und Fördermitteln	2816
		28.23	Herstellung von Büromaschinen (ohne Datenverarbeitungsgeräte und periphere Geräte)	2817
		28.24	Herstellung von handgeführten Werkzeugen mit Motorantrieb	2818
		28.25	Herstellung von kälte-und lufttechnischen Erzeugnissen, nicht für den Haushalt	2819*
		28.29	Herstellung von sonstigen nicht wirtschaftszweigspezifischen Maschinen a. n. g.	2819*
	28.3		Herstellung von land-und forstwirtschaftlichen Maschinen	
		28.30	Herstellung von land-und forstwirtschaftlichen Maschinen	2821
	28.4		Herstellung von Werkzeugmaschinen	
		28.41	Herstellung von Werkzeugmaschinen für die Metallbearbeitung	2822*
		28.49	Herstellung von sonstigen Werkzeugmaschinen	2822*
	28.9		Herstellung von Maschinen für sonstige bestimmte Wirtschaftszweige	
		28.91	Herstellung von Maschinen für die Metallerzeugung, von Walzwerkseinrichtungen und Gießmaschinen	2823
		28.92	Herstellung von Bergwerks-, Bau-und Baustoffmaschinen	2824
		28.93	Herstellung von Maschinen für die Nahrungs-und Genussmittelerzeugung und die Tabakverarbeitung	2825
		28.94	Herstellung von Maschinen für die Textil-und Bekleidungsherstellung und die Lederverarbeitung	2826
		28.95	Herstellung von Maschinen für die Papiererzeugung und –verarbeitung	2829*
		28.96	Herstellung von Maschinen für die Verarbeitung von Kunststoffen und Kautschuk	2829*
		28.99	Herstellung von Maschinen für sonstige bestimmte Wirtschaftszweige a. n. g.	2829*

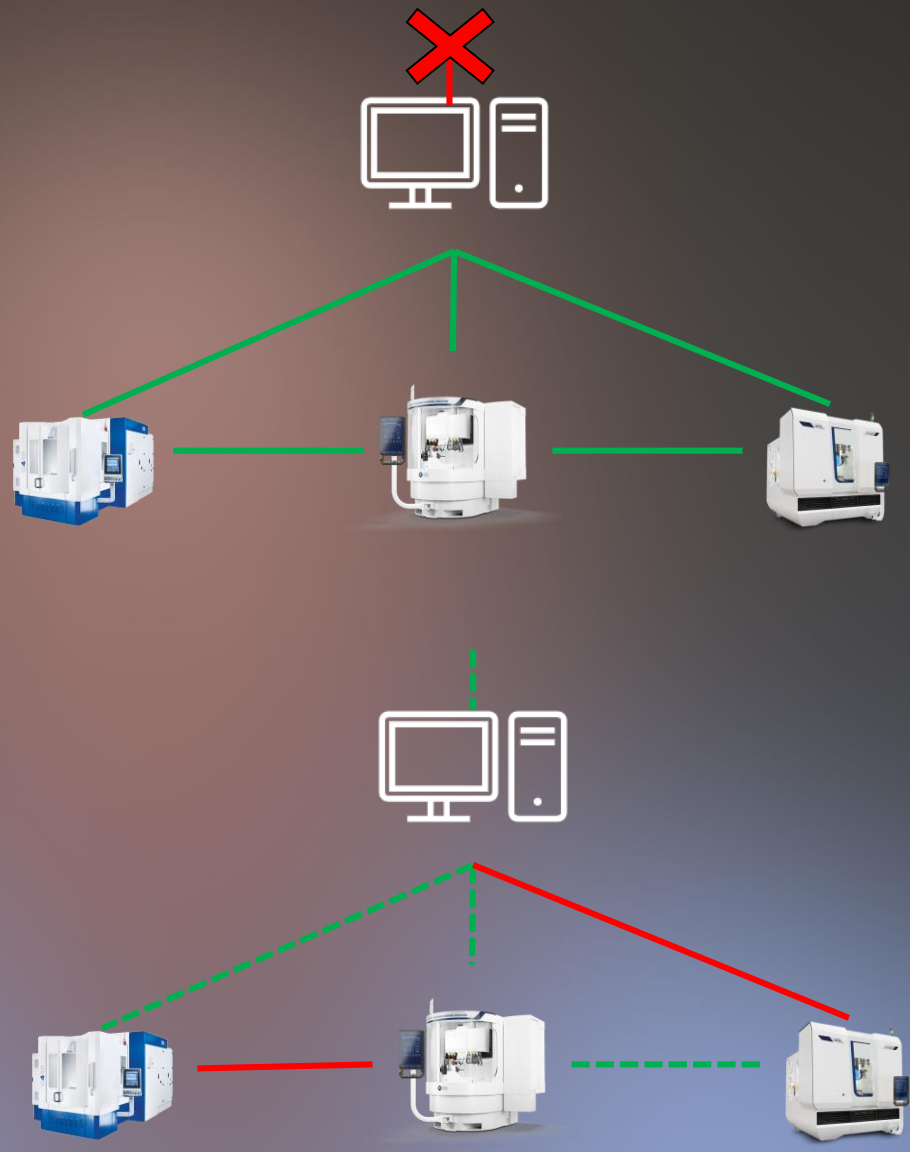
NIS2 Fahrzeugbau

29			Herstellung von Kraftwagen und Kraftwagenteilen	
	29.1		Herstellung von Kraftwagen und Kraftwagenmotoren	
		29.10	Herstellung von Kraftwagen und Kraftwagenmotoren	2910
	29.2		Herstellung von Karosserien, Aufbauten und Anhängern	
		29.20	Herstellung von Karosserien, Aufbauten und Anhängern	2920
	29.3		Herstellung von Teilen und Zubehör für Kraftwagen	
		29.31	Herstellung elektrischer und elektronischer Ausrüstungsgegenstände für Kraftwagen	2930*
		29.32	Herstellung von sonstigen Teilen und sonstigem Zubehör für Kraftwagen	2930*

a. n. g.: anderweitig nicht genannt				*Teil von
Abteilung	**Gruppe**	**Klasse**		**ISIC Rev. 4**
30			Sonstiger Fahrzeugbau	
	30.1		Schiff-und Bootsbau	
		30.11	Schiffbau (ohne Boots-und Yachtbau)	3011
		30.12	Boots-und Yachtbau	3012
	30.2		Schienenfahrzeugbau	
		30.20	Schienenfahrzeugbau	3020
	30.3		Luft-und Raumfahrzeugbau	
		30.30	Luft-und Raumfahrzeugbau	3030
	30.4		Herstellung von militärischen Kampffahrzeugen	
		30.40	Herstellung von militärischen Kampffahrzeugen	3040
	30.9		Herstellung von Fahrzeugen a. n. g.	
		30.91	Herstellung von Krafträdern	3091
		30.92	Herstellung von Fahrrädern sowie von Behindertenfahrzeugen	3092
		30.99	Herstellung von sonstigen Fahrzeugen a. n. g.	3099

Wie schützen?

- **IT/OT-Profis konsultieren!**
- Prozesse Analysieren: Wie kommen Daten auf die Maschine, warum und immer?
- Zugriff lieber über Netzwerk
  - Lokale Ports schließen / verriegeln!
  - Nur benötigte Verbindungen zulassen!
  - Firewall am besten „Deep Inspection“
- Datensicherungen auch von Maschinen!
- Verantwortlichen benennen / Mitarbeiter sensibilisieren!
- Notfallstrategie entwickeln!

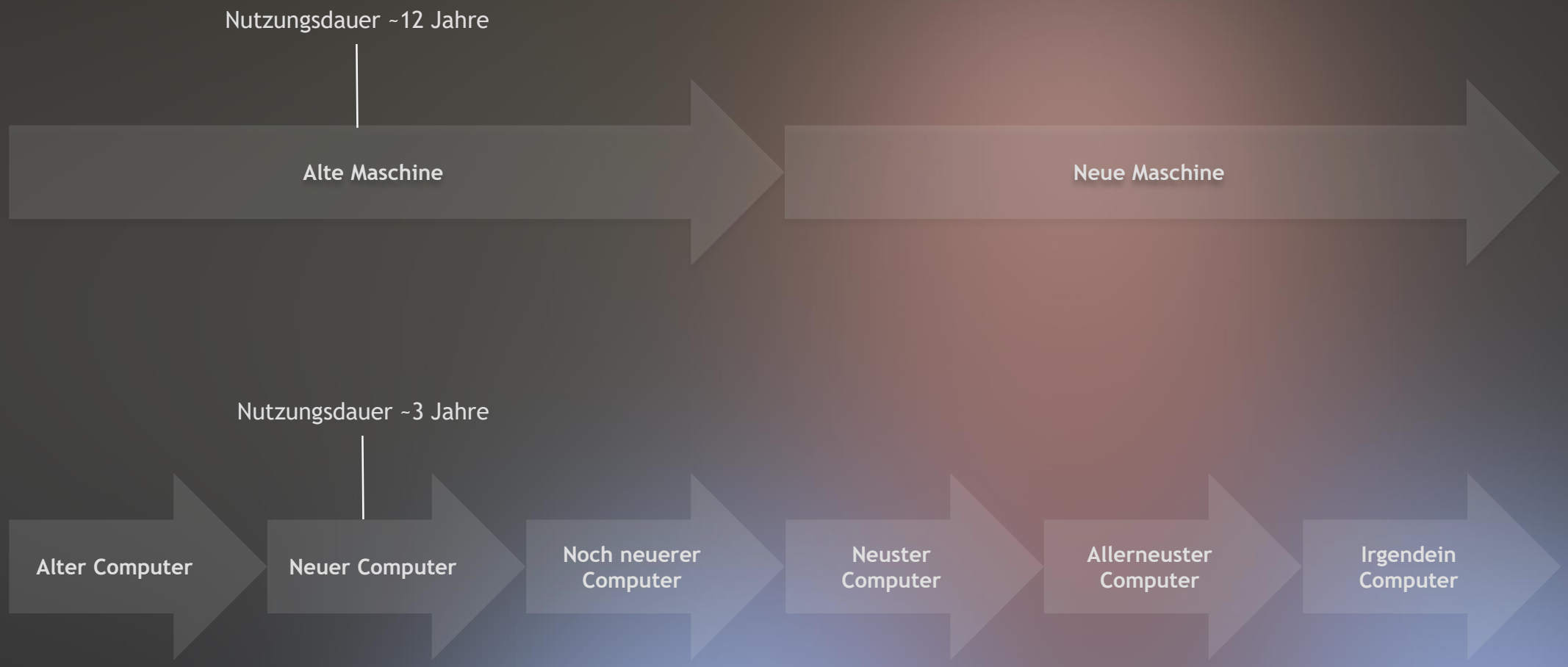


Eine Fritzbox ist zu wenig!

Wir werden das Problem noch lange haben.

- Der CRA kommt, aber wirkt langsam!
  (die typische Nutzungsdauer von **Maschinen in Deutschland beträgt 15-30 Jahre!)**
- Eine IT-Security-Strategie muss immer ganzheitlich betrachtet werden.
- Solange unsicherer Maschinen in der Produktion stehen ist diese auch unsicher!

Erneuerungsrate von Maschinen und Computern



Software- und Hardwareentkopplung

Vielen Dank für die Aufmerksmakeit!

d:e

INDUSTRIE DIGITAL 2025

VORTRAG

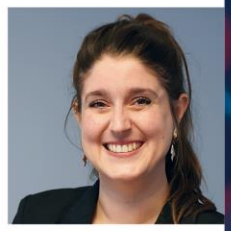
FORUM 5
IT-Security in Produktionssystemen – von der Achillesferse zum Schutzschild

d:e

Dr.-Ing. Karl Doreth
Berater & Entwickler digitaler Lösungen,
doreth:engineering

Dr.-Ing. Jan Brinkhaus
Berater für Industrie-Software & Dienste,
Brinkhaus GmbH

X4B



Dr.-Ing.
Sarah Majid Ansari,
Geschäftsführerin,
X4B Serviceagentur für die Wirtschaft GmbH

Was passiert auf EU-Ebene, was ist der CRA?

Dr.-Ing. Jan Brinkhaus

Dr.-Ing. Jan Brinkhaus

Geschäftsführer Brinkhaus GmbH

Kunden:

- Maschinenbauer & deren Zulieferer
- Dienstleister im Maschinenbau
- Externer Berater

Zuvor:

- Geschäftsführer der KOMET Brinkhaus GmbH als digitaler Zweig der KOMET-Gruppe

Beispiel „Ukraine“ – wenn digitale Produkte zum Ausfallrisiko werden

Ukraine, 24.02.2022

- Beginn der Invasion: Ein Cyberangriff trifft das Satelliten-Internet KA-SAT von Viasat.
- Tausende Modems werden durch Wiper-Malware unbrauchbar („AcidRain“).
- Folge: Breitband-Kommunikation in Teilen der Ukraine und Europas fällt aus – auch bei kritischen Nutzern.

Root Causes

- Single Point of Failure + schwach gesicherte Management-Zugänge → massenhafter Ausfall auf Knopfdruck.
- Physische Wirkung durch digitale Schwachstelle: Kommunikation weg → Koordination, Logistik, Betrieb von Systemen massiv gestört.

- Nicht nur „Kriegsszenario“: Das gleiche Muster gilt für Energie, Produktion, Logistik – überall, wo digitale Produkte Basisfunktionen tragen.

Cyber Resilience Act (CRA)

Genau solche systemischen Schwächen adressiert der CRA: sichere Defaults, abgesicherte Admin-Zugänge, Update-Pflicht.

Bislang war Produktsicherheit oft ein "Nice-to-have".

Wer es gut macht, hat Kosten. Wer es ignoriert hat, hat kurzfristig Vorteile. Der CRA dreht das um: unsichere digitale Produkte dürfen nicht mehr in den EU-Markt.

Der CRA macht "Security" zu einer Produkteigenschaft wie EMV oder Maschinensicherheit – verpflichtend, prüfbar und über den gesamten Support- und Nutzungszeitraum.

Cyber Resilience Act (CRA)

- Rechtsnatur: EU-Verordnung (gilt in allen Mitgliedstaaten, keine nationale Umsetzung erforderlich) (In Kraft seit 10.12.2024).
- Zielgruppe: Hersteller von Hardware und Software, die vernetzt oder digital betrieben werden.

- Melde-/Reportingpflichten greifen ab dem 11.09.2026

- Ab dem 11.12.2027 dürfen nicht-konforme Produkte nicht mehr auf den Markt

Cyber Resilience Act (CRA)

- Secure-by-design & Secure-by-default: Sicherheit wird von Anfang an mitentwickelt – nicht nachträglich „drangeflanscht“.
- Pflicht zu Updates & Support über die erwartbare Lebensdauer. Kein „Ende der Verantwortung nach Auslieferung“.
- Transparenz über Supportdauer & Updates
- Vulnerability-Management + Meldepflichten: Schwachstellen finden, bewerten, fixen, kommunizieren.
- CE-Konformität für Cybersecurity: Ab Ende 2027 ist CRA-Compliance Voraussetzung für CE-Kennzeichnung bei „Produkten mit digitalen Elementen“.

Cyber Resilience Act (CRA) - Schwerpunkt

- Verpflichtung, Sicherheitsupdates über eine Mindestzeit bereitzustellen.
- Produkte müssen "Secure by Design" sein (z. B. keine Standard-Passwörter, abgesicherte Kommunikation).
- Hersteller müssen ein Sicherheitsrisikomanagement durchführen und dokumentieren.
- Sicherheitszertifizierungen oder Konformitätserklärungen für bestimmte Produktkategorien.

Welche Firmen betrifft der CRA?

- Hersteller vernetzter Hardware- und Softwareprodukte mit digitalen Elementen

  → z. B. Industrie-PCs, Steuerungen, IoT-Geräte, Softwareplattformen

- Entwickler von Software, die in Produkte integriert oder separat vertrieben wird

  → auch reine Softwarelösungen sind erfasst, wenn sie vernetzt sind

- Unternehmen mit Eigenentwicklungen für den internen oder industriellen Einsatz

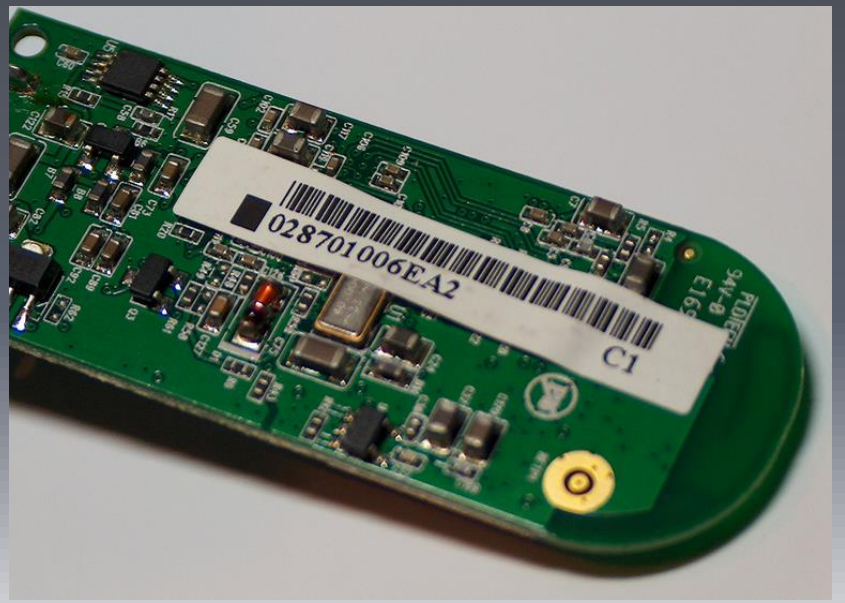
  → wenn Produkte extern genutzt oder vertrieben werden

- Zulieferer in der Industrie

  → auch bei Teilkomponenten
  (Embedded-Systeme, Firmware, Libraries)

- Start-ups und KMU

  → Gilt auch für KMU/Start-ups – Pflichten unabhängig von Unternehmensgröße, teils mit vereinfachten Konformitätswegen



Bedeutung für Zulieferer und Unternehmen

- Nicht nur das Produkt muss „CRA-konform“ sein – sondern auch das Unternehmen muss dafür organisatorisch aufgestellt sein.
- Selbst eine 2-Mann-Firma muss z.B.:
  - Security-Verantwortlichen festlegen (auch wenn‘s dieselbe Person wie der Entwickler ist)
  - Supportdauer schriftlich festlegen und kommunizieren
  - Release-Prozess mit CVE-Check / Dependency-Scanning verankern
  - „Audits von Zulieferern?“ → klare Pflicht/Notwendigkeit
  - Lieferkette bewerten (SBOM/Komponenten-Risiko), sonst keine CRA-Konformität nachweisbar.

Bedeutung für Produktentwicklung

- Bedrohungsanalyse und Risikobewertung
  - ✓ Netzwerkschnittstellen, offene Ports
  - ✓ Manipulation der Kommunikation
  - ✓ Bei komplexen Produkten: Bewertung eingesetzter Komponenten muss vorliegen (Audits von Zulieferern? → CRA-Konformität der Zulieferer sicherstellen)
  - ✓ …
- Umsetzung eines Cybersicherheits-Lifecycle-Prozesses
  - ✓ Patch-Management & Update-Pflicht
  - ✓ …
- CRA-Konformitätserklärung
  - ✓ Erklärung der Einhaltung des CRA
  - ✓ Kurzdarstellung der Maßnahmen und Risikobewertung
  - ✓ …
- Ggf. externe Zertifizierung
  - ✓ Prüfung auf Pflicht zur externen Zertifizierung

Praxisbeispiel mit Kunden

Kontext: Kernsoftware für sein Überwachungssystem wurde bei uns entwickelt. Kunde ist KMU.

Wir haben auch CRA-Know-How.

- Einführung / Schulung der Mitarbeiter inkl. des GF
- Installation eines Sicherheitsrisikomanagementsystems
- Planung und Durchführung eines Audits
- Ableitung von Auditmaßnahmen
- Erstellung einer Risikobewertung und CRA-Konformitätserklärung

Im Audit durch Kunden des Kunden: Auftreten ggü. Auditor als externer Berater, Führen des externen Auditors durch Auditprotokoll, Excel-Liste mit Auditergebnissen und Excel-Liste mit Auditmaßnahmen.

Das externe Audit war schnell vorbei und der Mitarbeiter des Kunden wandte sich anderen Problemen (bzw. anderen Zulieferern) zu 😉 .

Vielen Dank für Ihre Aufmerksamkeit!!

INDUSTRIE DIGITAL 2025

VORTRAG

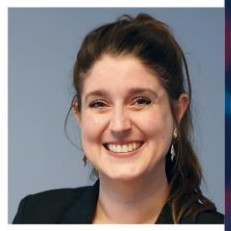
FORUM 5
IT-Security in Produktionssystemen – von der Achillesferse zum Schutzschild

d:e

Dr.-Ing. Karl Doreth
Berater & Entwickler digitaler Lösungen,
doreth:engineering

Dr.-Ing. Jan Brinkhaus
Berater für Industrie-Software & Dienste,
Brinkhaus GmbH

X4B



Dr.-Ing.
Sarah Majid Ansari,
Geschäftsführerin,
X4B Serviceagentur für die Wirtschaft GmbH