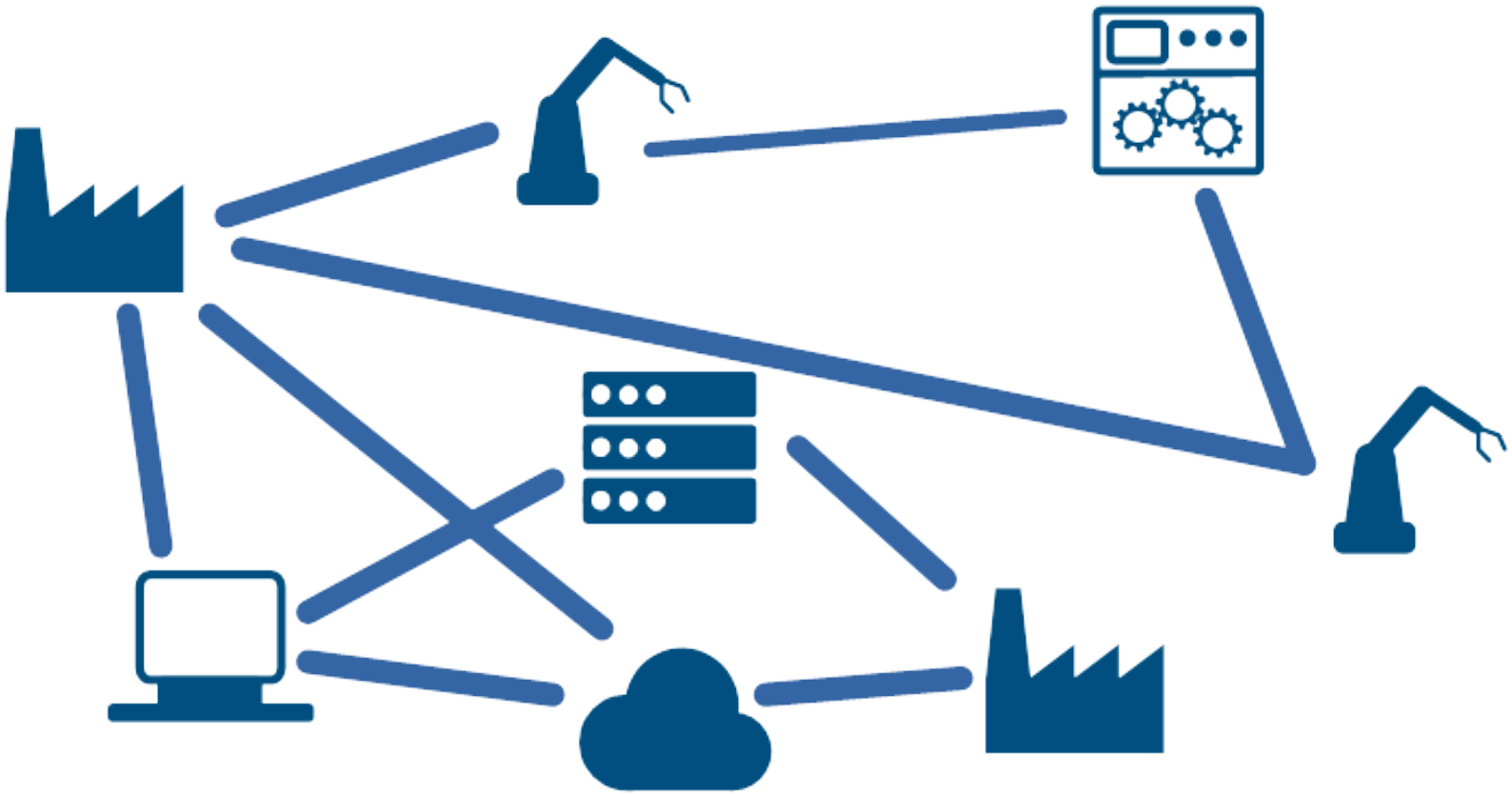
Bundesamt
für Sicherheit in der
Informationstechnik

# Workshop:
# Aktuelle Angriffsvektoren und Gegenmaßnahmen

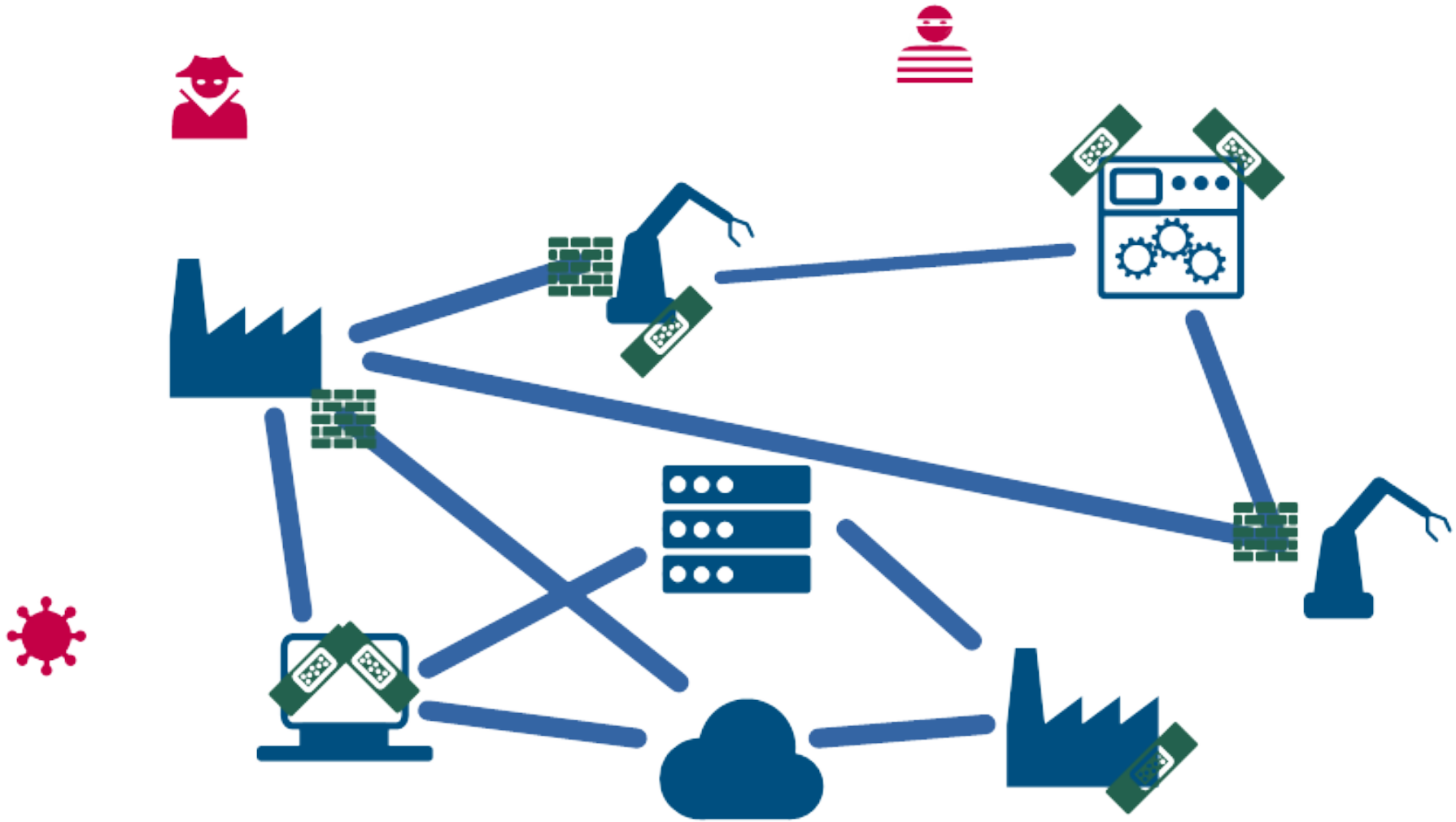
# Agenda

1. Einführung
2. Sammeln von Meinungen/Stichworten in Kleingruppen
3. Vorstellung & Diskussion

# 1. Einführung



Bundesamt
für Sicherheit in der
Informationstechnik

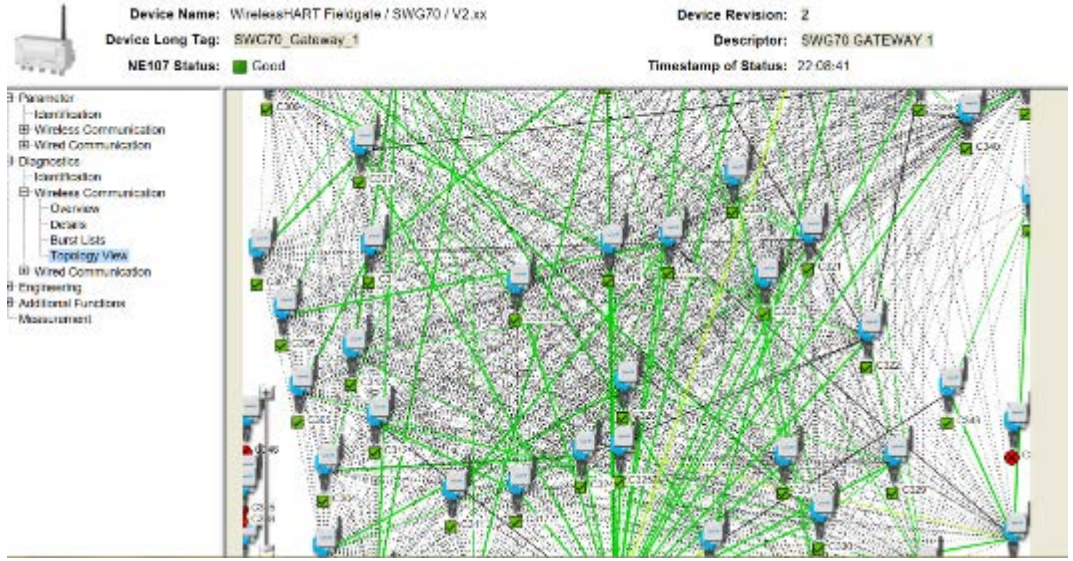


Bundesamt
für Sicherheit in der
Informationstechnik

# Industrieanlagen - Einfach Angreifbar?

Siemens Scalance Internet Router.


Wireless Hart Fieldgateway.




ANDY GREENBERG SECURITY 07.24.15 12:30 PM

AFTER JEEP HACK, CHRYSLER RECALLS 1.4M VEHICLES FOR BUG FIX


## Top Schwachstellen

[1 - 4] Digitale Sorglosigkeit beim Betreiber.

[5] Fehlende IT Security Checkliste bei Übergabe vom Systemintegrator an den Betreiber.

# Ungezielte und gezielte Angriffe

Ungezielte Angriffe

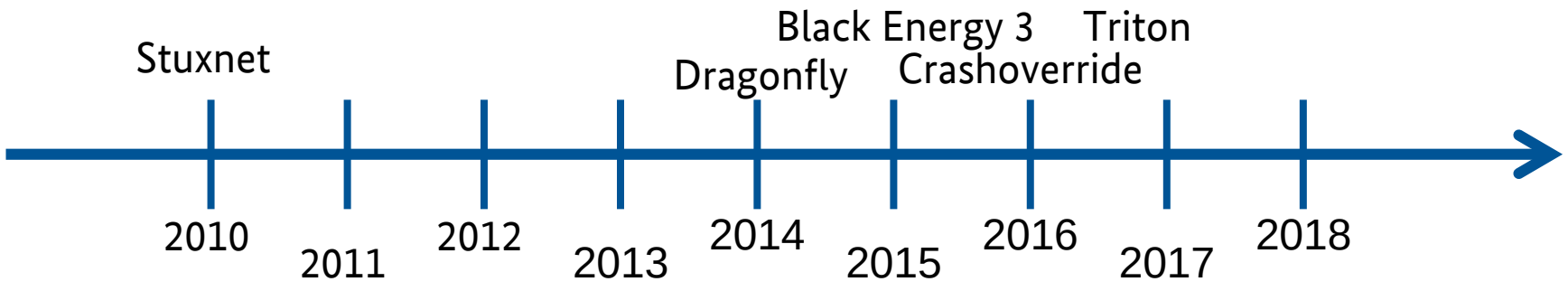
- Vergleichsweise einfach
- Viren & Würmer
- Ärgerlich, aber Tagesgeschäft
- Es müssen Prozeduren & Verfahren etabliert sein, damit umzugehen

**Gezielte Angriffe**

- Aufwendig
- Diebstahl von Geschäftsgeheimnissen
- Beeinträchtigung der Produktion
- Verringerung der Qualität
- Ransomware (gegen Maschinen und Anlagen)

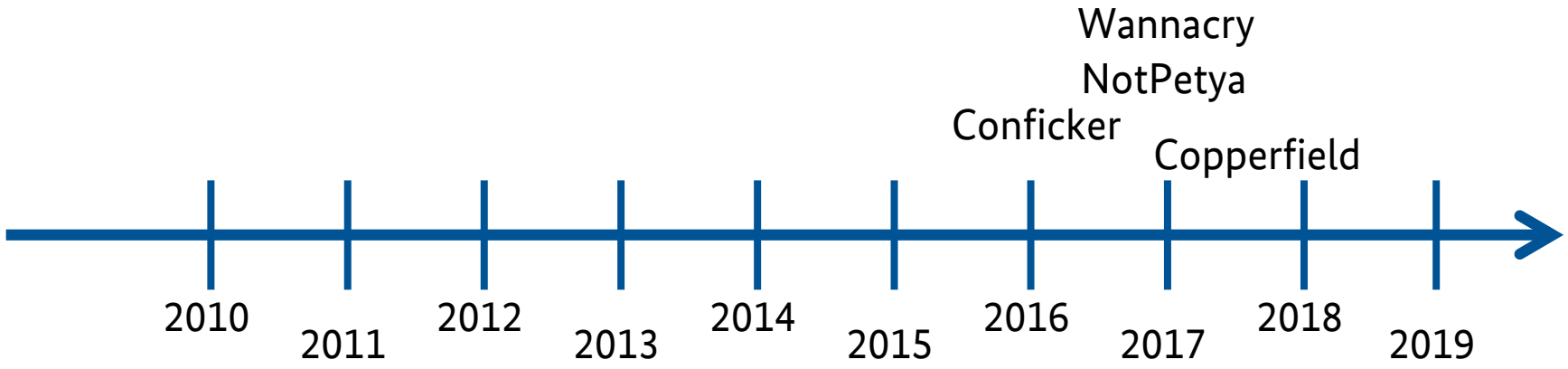
# Auszug gezielter Angriffe

| Angriff | Jahr | Ort | Ziel |
|---|---|---|---|
| Stuxnet | 2010 | Iran | Kernkraft |
| Dragonfly/Havex | 2014 | EU, USA | Industrie |
| Black Energy 3 | 2015 | Ukraine | Energie |
| Crashoverride / Industroyer | 2016 | Ukraine | Energie |
| Triton/Tritis | 2017 | Mittlerer Osten | Safety-System |



# Auszug ungezielter Angriffe

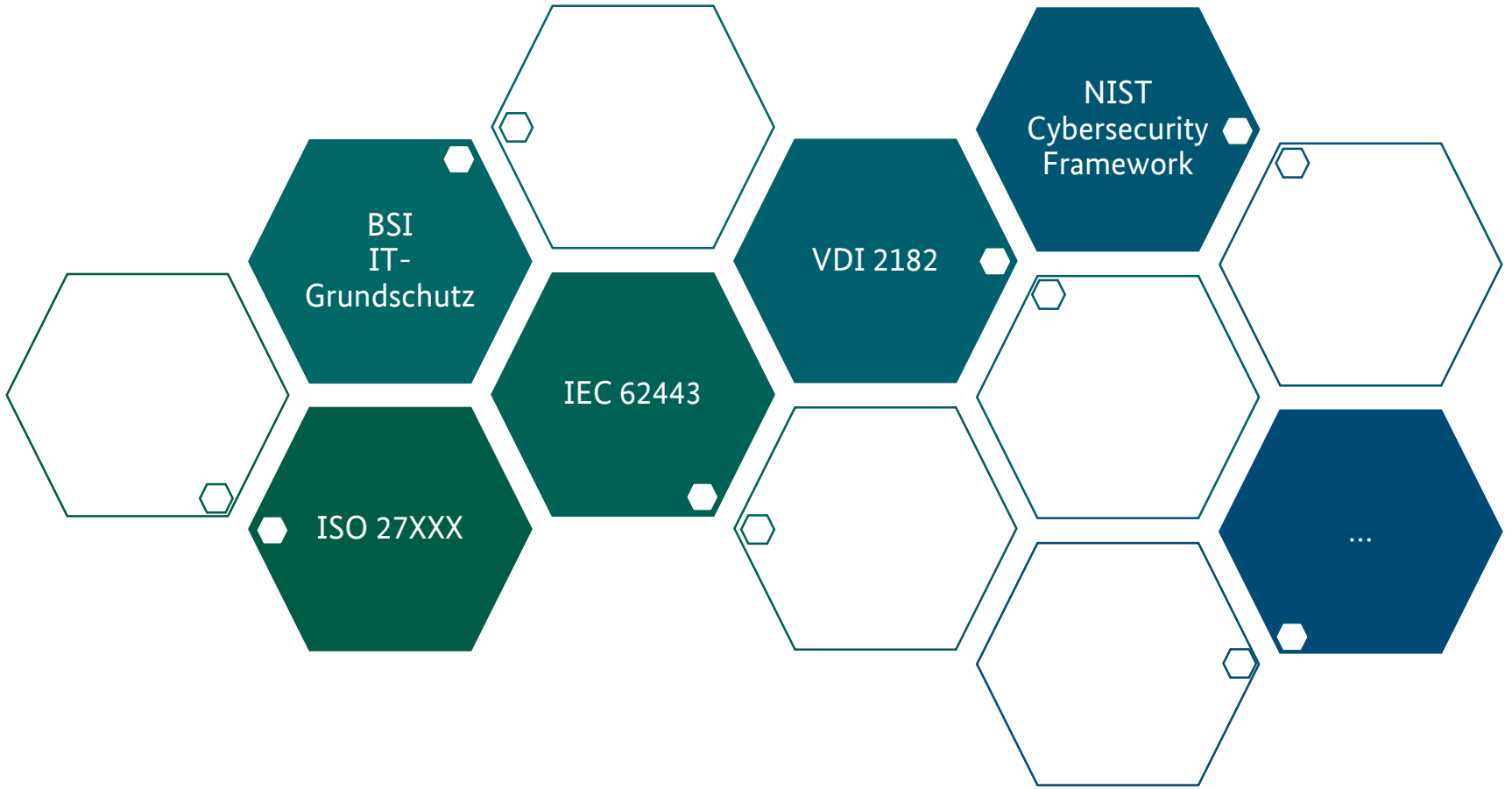
| Angriff | Jahr | Ort | Ziel |
|---|---|---|---|
| Conficker | 04/2016 | Deutschland | Kernkraftwerk |
| Wannacry | 05/2017 | Weltweit | Windowssysteme |
| NotPetya | 06/2017 | Weltweit | Windowssysteme |
| Copperfield | 12/2017 | Mittlerer Osten | Kritische Infrastruktur |
| Norsk Hydro | 03/2019 | Norwegen | Aluminium-Hersteller |



# Probleme sind schon da!

# Wie können wir damit umgehen?

# Standards & Normen




Bundesamt
für Sicherheit in der
Informationstechnik

# 2. Fragen

# Leitfragen

- Wo sehen Sie die größten Gefährdungen & Herausforderungen in Ihren Unternehmen?
- Welche Herausforderungen entstehen bei der Umsetzung von Cyber-Sicherheit?
- Welche Hilfestellungen/Standards nutzen Sie?
  - Wo sehen Sie Verbesserungsbedarf?
- Welche Erwartungen werden an das BSI gestellt?

# Herausforderungen

- Fehlende Transparenz & Kontrolle & Know-How
  - wegen zugekaufter Lösungen
  - Fachkräftemangel / Qualifiziertes Personal
  - Fehlende Dokumentation
    - Aktuelles Asset-Management
    - Unüberschaubare Zahl von IP-Komponenten
- „unsichere“ externe Welt mit der „unsicheren“ Welt intern verbinden
  - Keine Segmentierung
  - Schlechte Vernetzung OT <-> IT
- Begrenzte Ressourcen
  - Zeitdruck in der OT
  - Patchmanagement (fehlende Zeitfenster)
- Gesetzliche Vorgaben der Länder sicher erfüllen
- Fehlende Prozesse
  - Patches werden ungeprüft eingespielt
- Abhängigkeit von Dienstleistern
  - Keine Updates verfügbar
  - Insolvenz des Hard-/Softwareherstellers
- Komplexität/Vielfältigkeit
  - Heterogene Maschinenumgebung / Viele Hersteller, viele Standards
  - Lebenszyklus OT vs. IT
  - Alte Hard-/Software (z.B. WinXP)
  - Unsichere Maschinen im Bestand / Keine Updates verfügbar
  - Cloud
  - Keine Standardisierung bei Fernwartung OT / Risiken durch Fernwartung
  - Alles muss immer online sein
  - Historischer Wildwuchs / OT mehr Vernetzung -> größere Anfälligkeit

- Kommunkation / Sensibilität
  - IT versteht die Bedürfnisse der OT nicht
  - Mitarbeiter Awareness in der Produktion !?!
  - Virus kommt mit externer Hardware (z.B. Servicetechniker)
  - Gefahr durch Office (E-Mails)
  - Angriffe durch Social Engineering
  - Verständnis für Cybersicherheit ist wie Verständnis für Arbeitssicherheit vor X Jahren
  - CEO Awareness
  - Sicherheitsrisiko Endanwender intern + extern
- Lieferkette
  - (fehlende) Verantwortung der Hersteller
  - Lieferanten ziehen sich nach der Inbetriebnahme aus der Verantwortung
  - Security in Supplier Relationship

- Effizient (Arbeitsfähigkeit) vs. Sicherheit
- Umgang mit den Daten „Gold der Zukunft“
- Dynamische Bedrohungen vs. Statische Infrastruktur
- Geringes Risiko für Cyber-Kriminelle
- Priorisierung der „richtigen“ IT-Sicherheitsmaßnahmen
  - Sicherheit von Gateways mit Schnittstellen
    - LoRA
    - Bluetooth
  - Ist DMZ für Legacy-Systeme genug?

# Umsetzung

- Festes System zur Prüfung von Software bei Neukauf oder Updates
- Checklisten (High-Level & im Detail) für
  - Produktion
  - Einkauf
  - Neues Gerät im Firmennetz (Fragen an Hersteller)
- Kommunikation
  - Unterstützung durch Top-Management
  - IT-Koordinator IT <-> OT
  - Verständnis zwischen IT und OT + Verantwortlichkeiten festlegen
  - IT als Enabler wahrnehmen
  - Mitarbeitersensisbilisierung auf allen Ebenen
  - Widerstände vs. Awareness (Akzeptanz für IT-Sicherheitsthemen schaffen)
- Richtlinien (Leitfäden) für Kunden + Lieferanten
  - Spezifikationen für Maschinenhersteller
  - Security-Level als Feature für Anlagenhersteller
  - IT-Sicherheit muss ins Pflichtenheft bei jeder Neubeschaffung
- Umsetzung
  - Gefahren- & Risikoanalyse
  - Security-Checkpoint in Projekten
  - Security vs. Usability (Secure-Login müsste vereinfacht/automatisiert sein)
  - Bestandsaufnahme + Netzwerkscans + Detektion
  - Gefährdete Bereiche segmentieren
  - Pen-Tests
- Notfallplan
- Cyberversicherungen
- Standardisierung/Vereinheitlichen der Strukturen

# Erwartungen an das BSI

- Normen
  - Globale Handlungsempfehlungen
  - Internationale Vernetzung
- Awareness-Kampagnen
  - Unterstützung für sicheres Verhalten
  - E-Learning für Sensibilisierung
  - Awareness Toolkit
- Best-Practices / Standards / Handlungsleitfäden
  - für Fernwartung
  - Laptop-Zugriffe
  - Priorisierung der Anforderungen (must/opt/nice)
- Bessere / Anwendbarere Vorgaben und Unterstützung für Betreiber
- Enterprise-Kompatibilität des BSI erhöhen vs. Grundschutz zu umfangreich
- Standards / Stand der Technik definieren
- Zeitnahe Information über aktuelle Bedrohungen (z. B. Newsletter)
- Zertifizierung (bspw. ähnlich zu CE-Zeichen)
- (Gesetze)
- Sicherheit für Architekturen der Zukunft
  - Industrie 4.0
  - IIoT
  - 5G
- Fact für Industriefirmware
- Produktklassifizierungsleitfaden
- Gefährdungeskatalog für Risikoanalyse

# Informationen zu den Themen aus dem Workshop

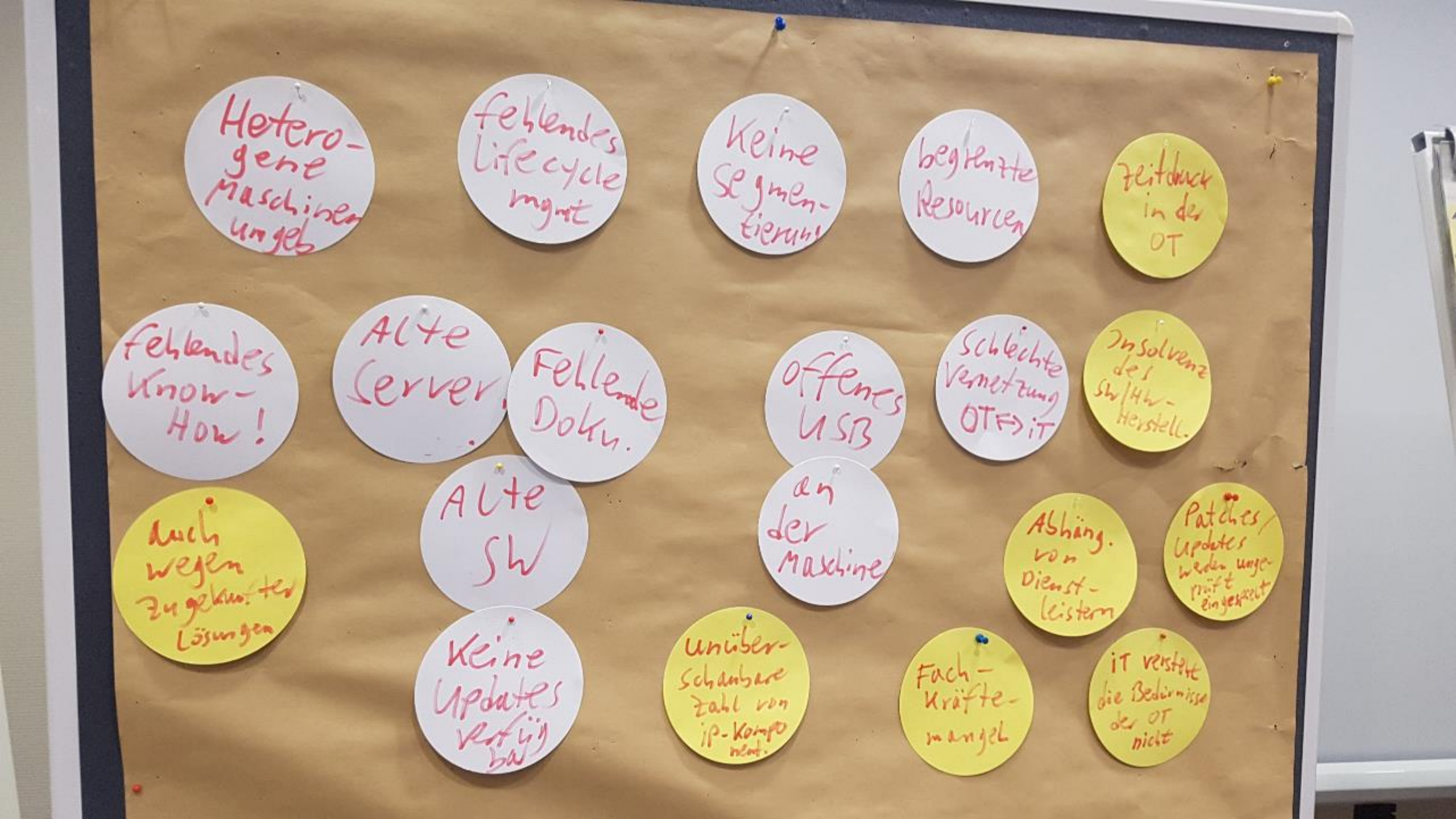
- Allianz für Cybersicherheit: https://www.allianz-fuer-cybersicherheit.de
- Empfehlungen für industrielle Systeme: https://www.bsi.bund.de/ICS
- Übersichtsseite des IT-Grundschutz: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html
  - Für Nutzung von Cloud ist der Baustein **OPS.2.2 Cloud-Nutzung** relevant oder https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Zielgruppen/Anwender/anwender_node.html
  - Für Nutzung von Mobile Devices SYS.3.2.2 Mobile Device Management oder https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Mobile-Device-Management.html
  - Für den Bereich Fernwartung:
    - **OPS.2.4 Fernwartung**
    - **https://www.bsi.bund.de/ACS/DE/_/downloads/BSI-CS_108.html**
    - **https://www.bsi.bund.de/ACS/DE/_/downloads/BSI-CS_054.html**

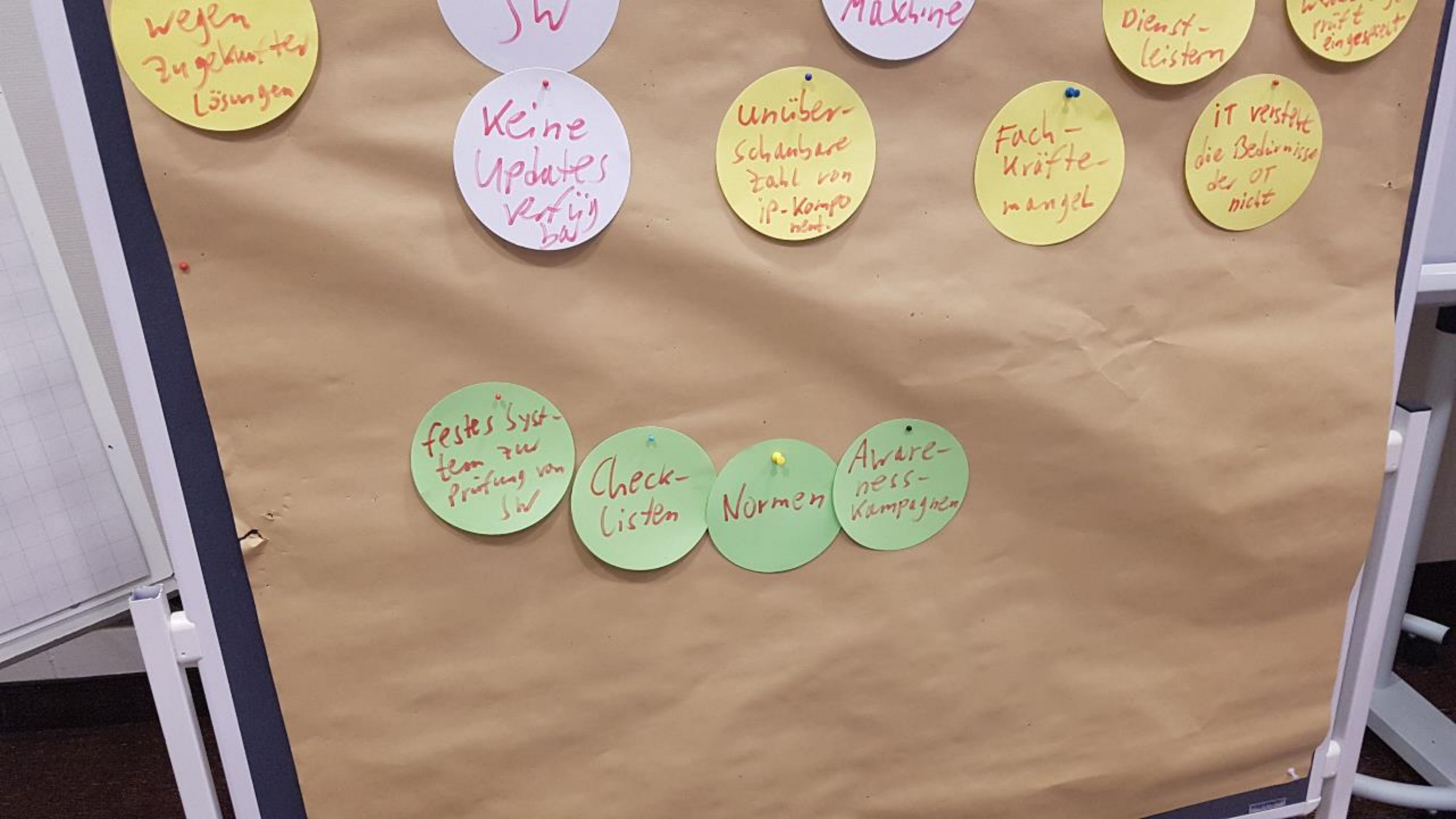
# Vielen Dank für die Aufmerksamkeit!

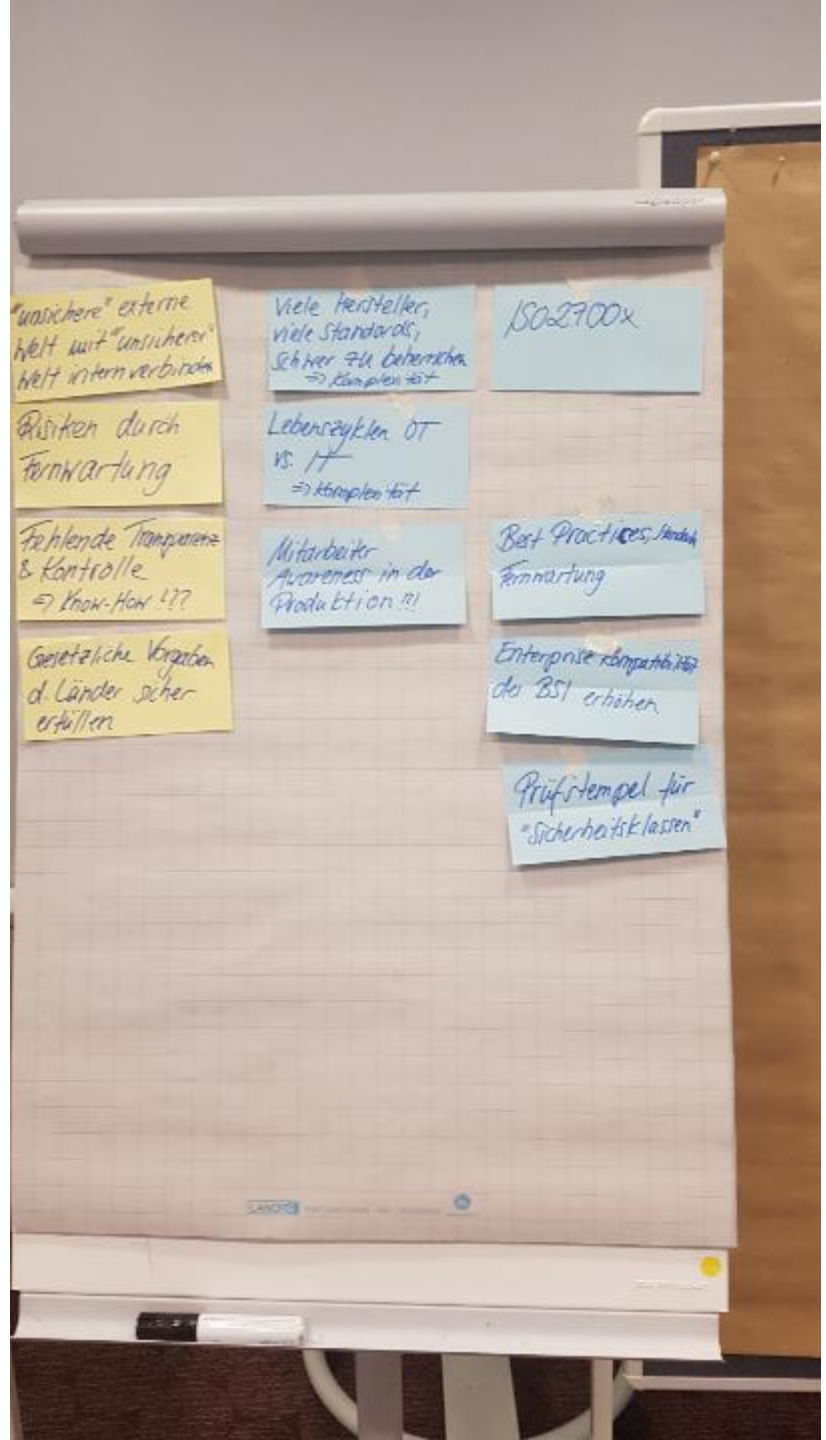
## Kontakt

Bundesamt für Sicherheit in der Informationstechnik
Referat TK 15 – Industrielle Automations- und Steuerungstechnik
Godesberger Allee 185-189
53175 Bonn

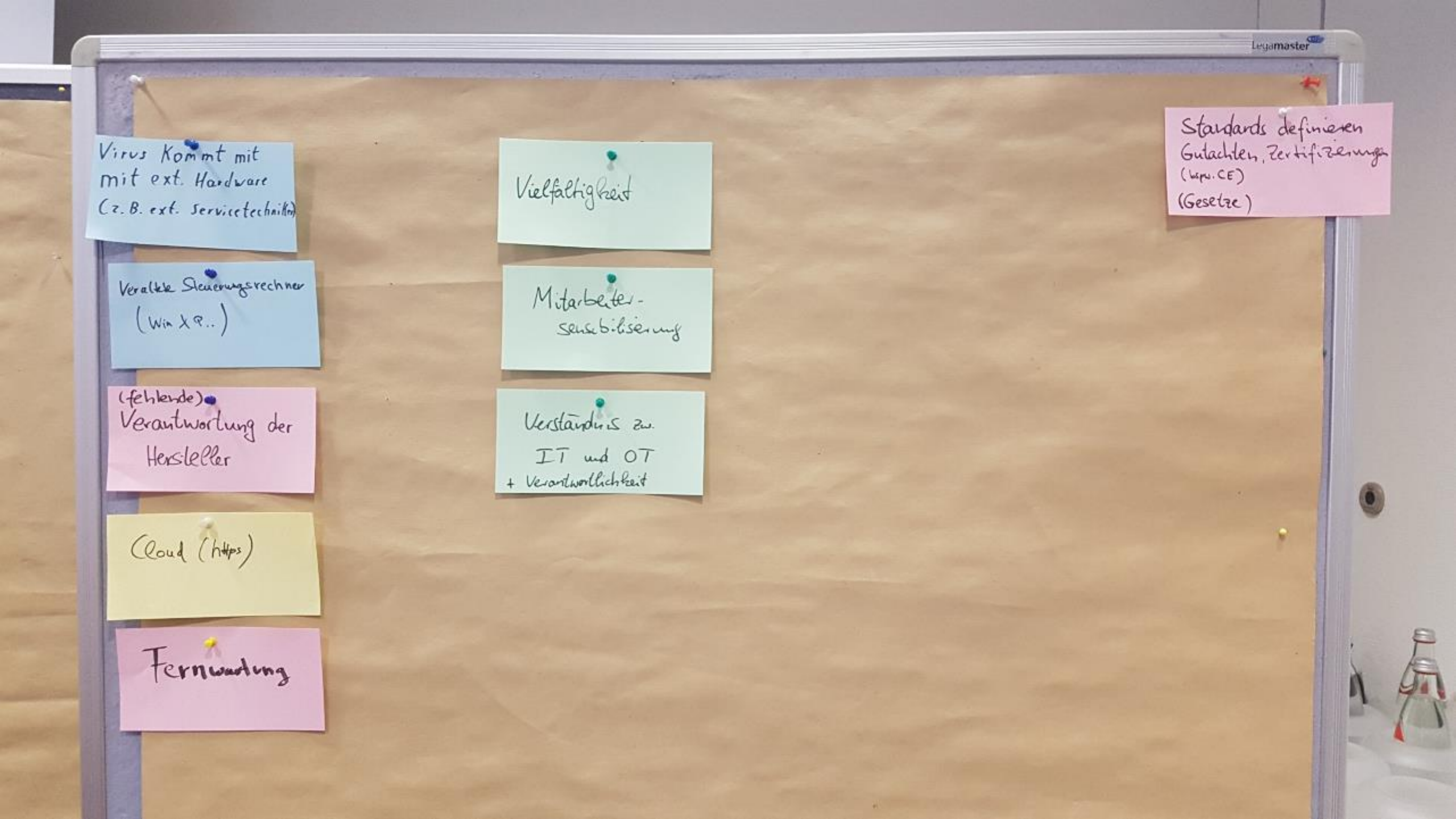
Ansprechpartner
Hr. Jens Mehrfeld
jens.mehrfeld@bsi.bund.de
www.bsi.bund.de
Tel. +49 228 99 9582 5936
Fax +49 228 9910 9582 5936


Hetero-
gene
Maschinen
ungeb.
fehlendes
Lifecycle
mgmt
Keine
Segmen-
tierung
begrenzte
Ressourcen
Zeitdruck
in der
OT
fehlendes
Know-
How!
Alte
Server
Fehlende
Dokum.
offenes
USB
an
der
Maschine
schlechte
Vernetzung
OT⇔IT
Insolvenz
der
SW/HW-
Herstell.
auch
wegen
zugekauften
Lösungen
Alte
SW
Keine
Updates
verfügbar
Unüber-
schaubare
Zahl von
IP-Kompo
nent.
Fach-
Kräfte-
mangel
Abhäng.
von
Dienst-
leistern
Patches/
Updates
werden unge-
prüft
eingespielt
IT versteht
die Bedürfnisse
der OT
nicht


wegen zugekauften Lösungen
SW
Maschine
Dienst-leistern
Keine Updates verfügbar
Unüber-schaubare Zahl von IP-Kompo nent.
Fach-Kräfte-mangel
IT versteht die Bedürfnisse der OT nicht
festes System zur Prüfung von SW
Check-listen
Normen
Aware-ness-Kampagnen




Bundesamt
für Sicherheit in der
Informationstechnik


Legamaster
Virus kommt mit mit ext. Hardware (z.B. ext. Servicetechniker)
Veraltete Steuerungsrechner (Win XP..)
(fehlende) Verantwortung der Hersteller
Cloud (https)
Fernwartung
Vielfältigkeit
Mitarbeiter-sensibilisierung
Verständnis zw. IT und OT + Verantwortlichkeit
Standards definieren Gutachten, Zertifizierungen (wg. CE) (Gesetze)

SENSIBILISIERUNG
INFORMATION
SCHULUNG
DER MITARBEITER

Secure Login müsste vereinfacht / automatisiert sein

Spezifikationen für Maschinenhersteller

Konkrete Hinweise für sichere Maschinenzugänge
- Fernzugriff
- Laptop-Zugriff

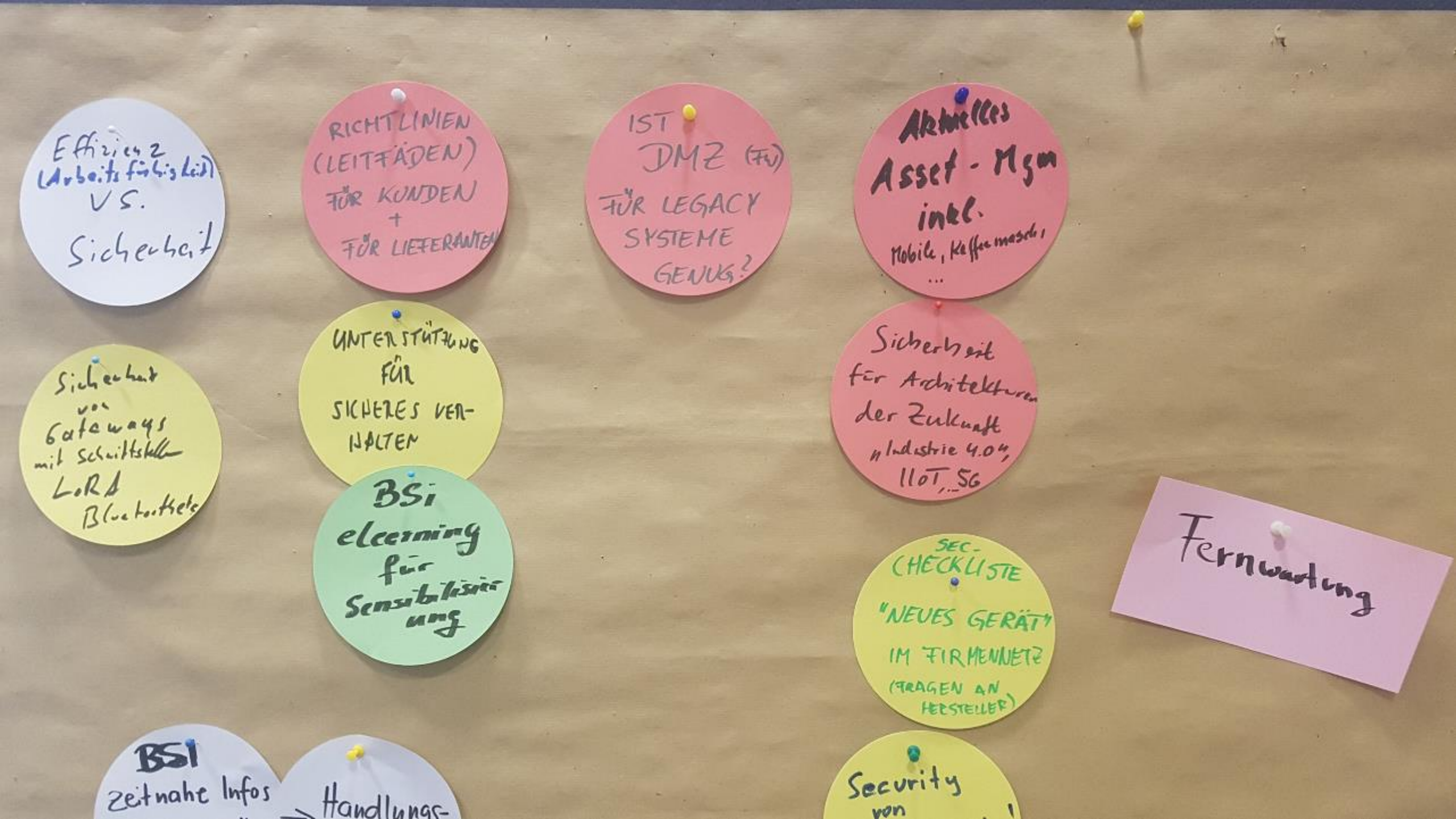
Überprüfung beim Kauf von (Teil-) Produkten oder Dienstleistungen?

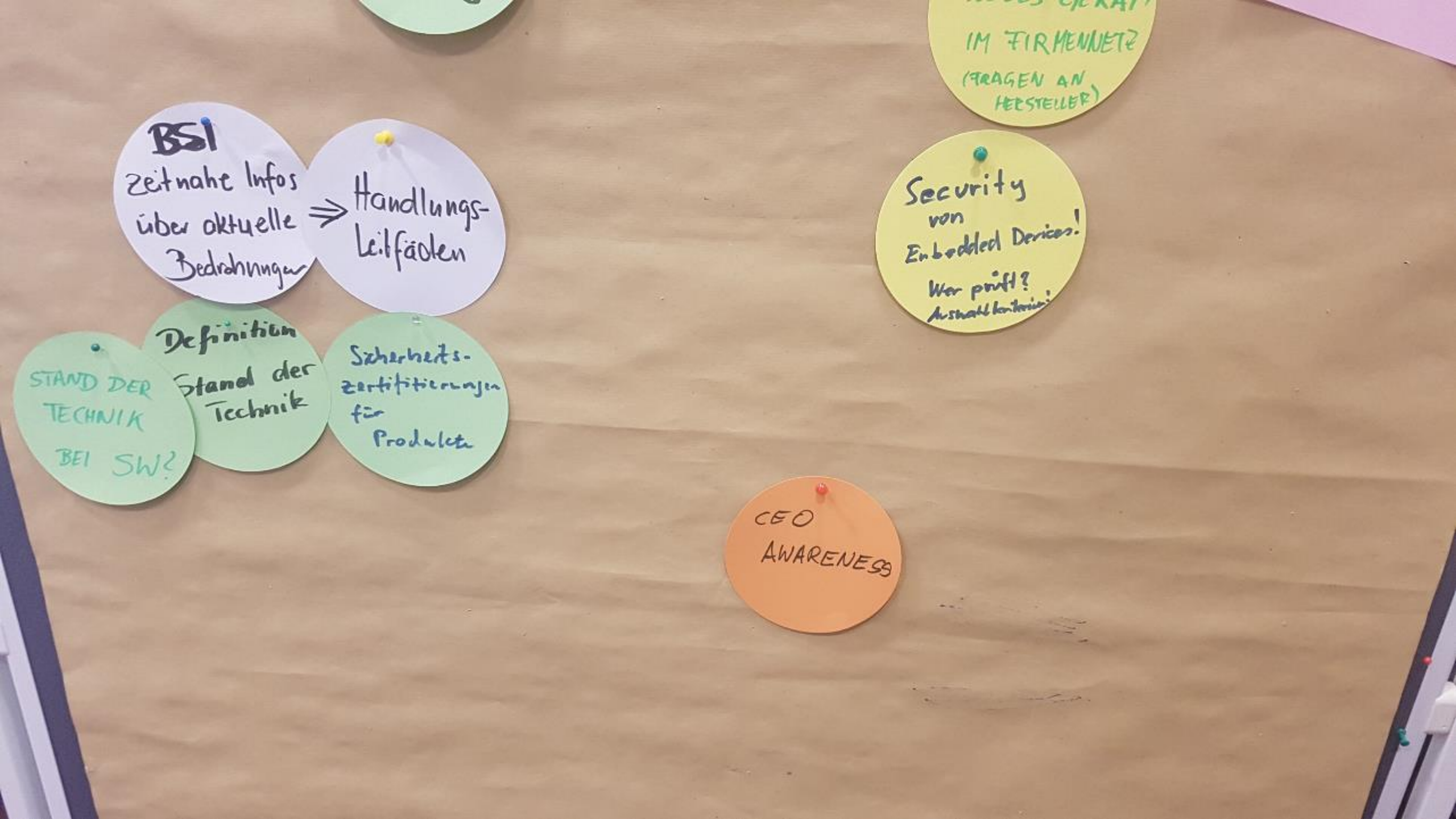
Security level als Feature für Anlagenhersteller

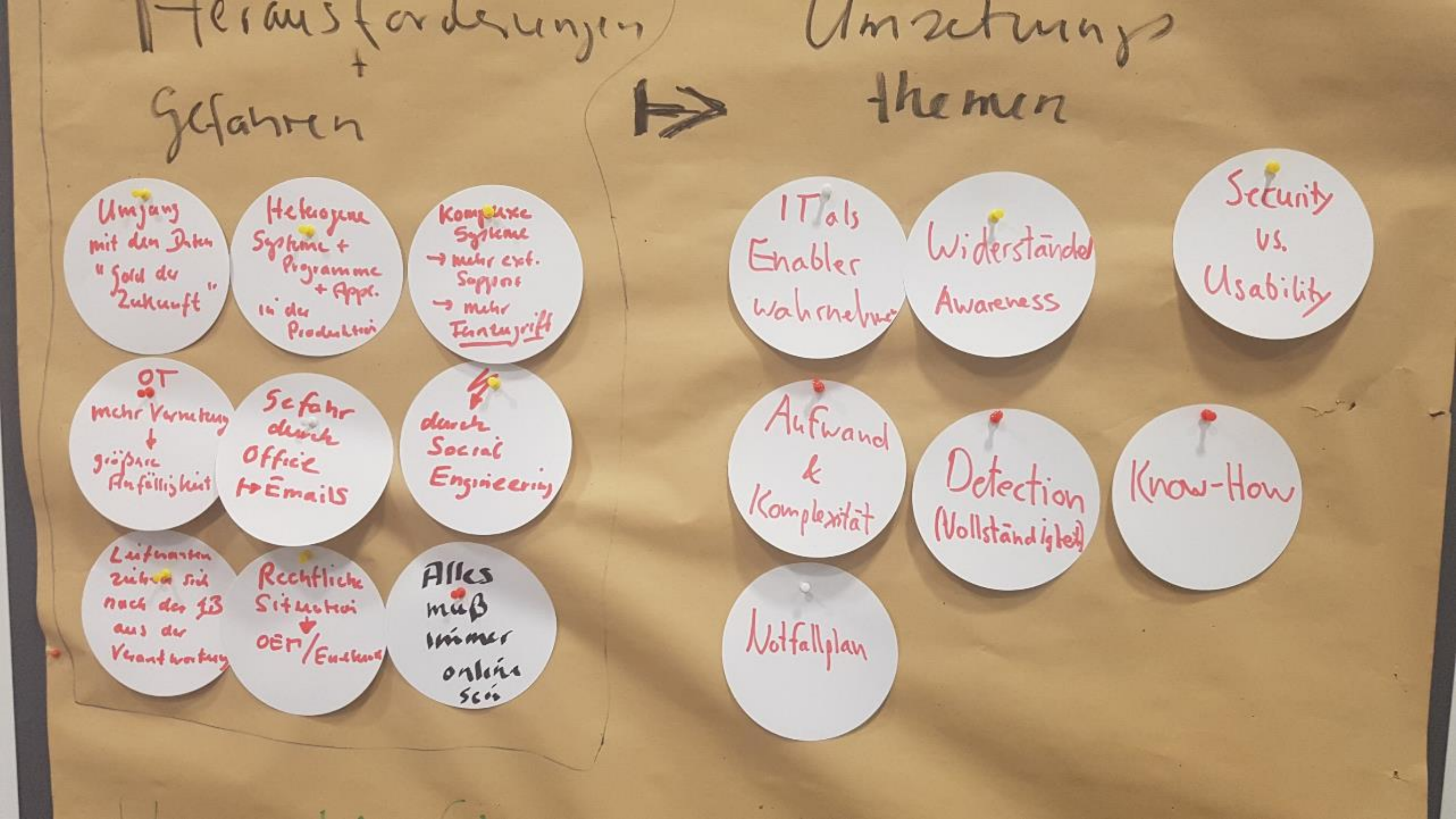
Verständnis für InfoSec heute ist wie Verständnis für Arbeitssicherheit vor X-Jahren.

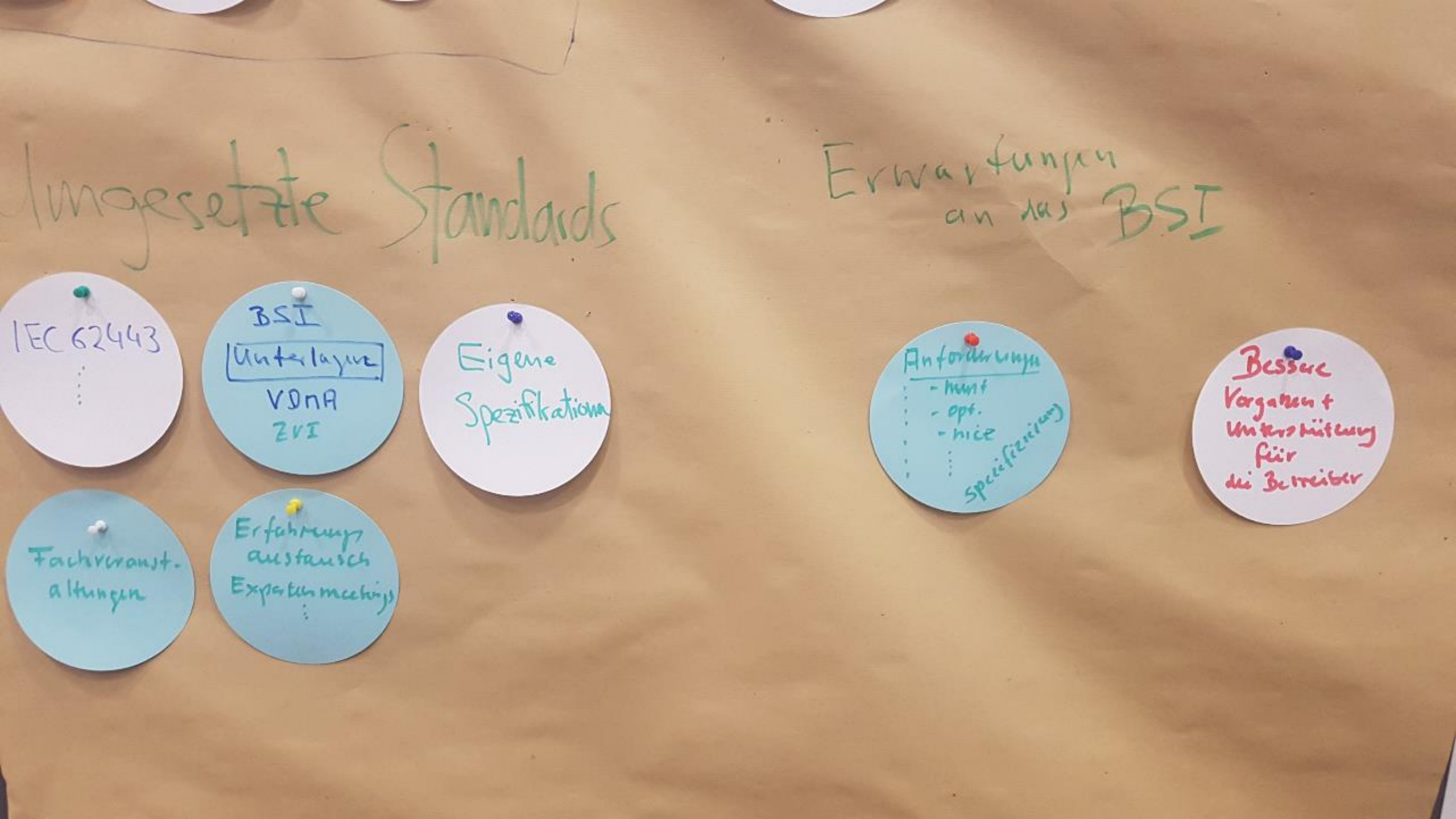
"Weg raus" aus dem Unternehmen.
Schwachstellen?

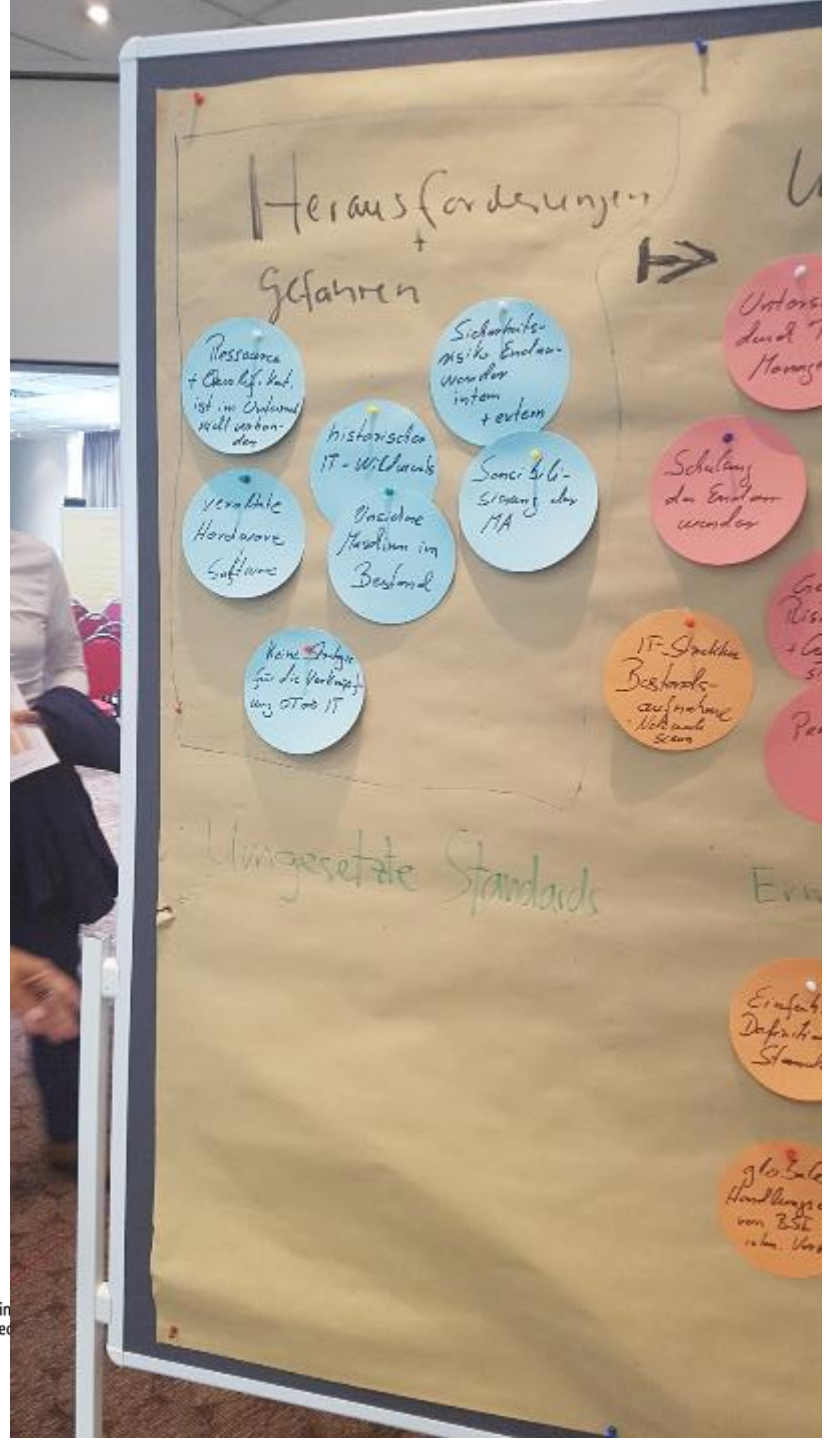
CHECKLISTEN
(high-level & im Detail) für
- Produktionen
- Einkauf (Maschinen etc)

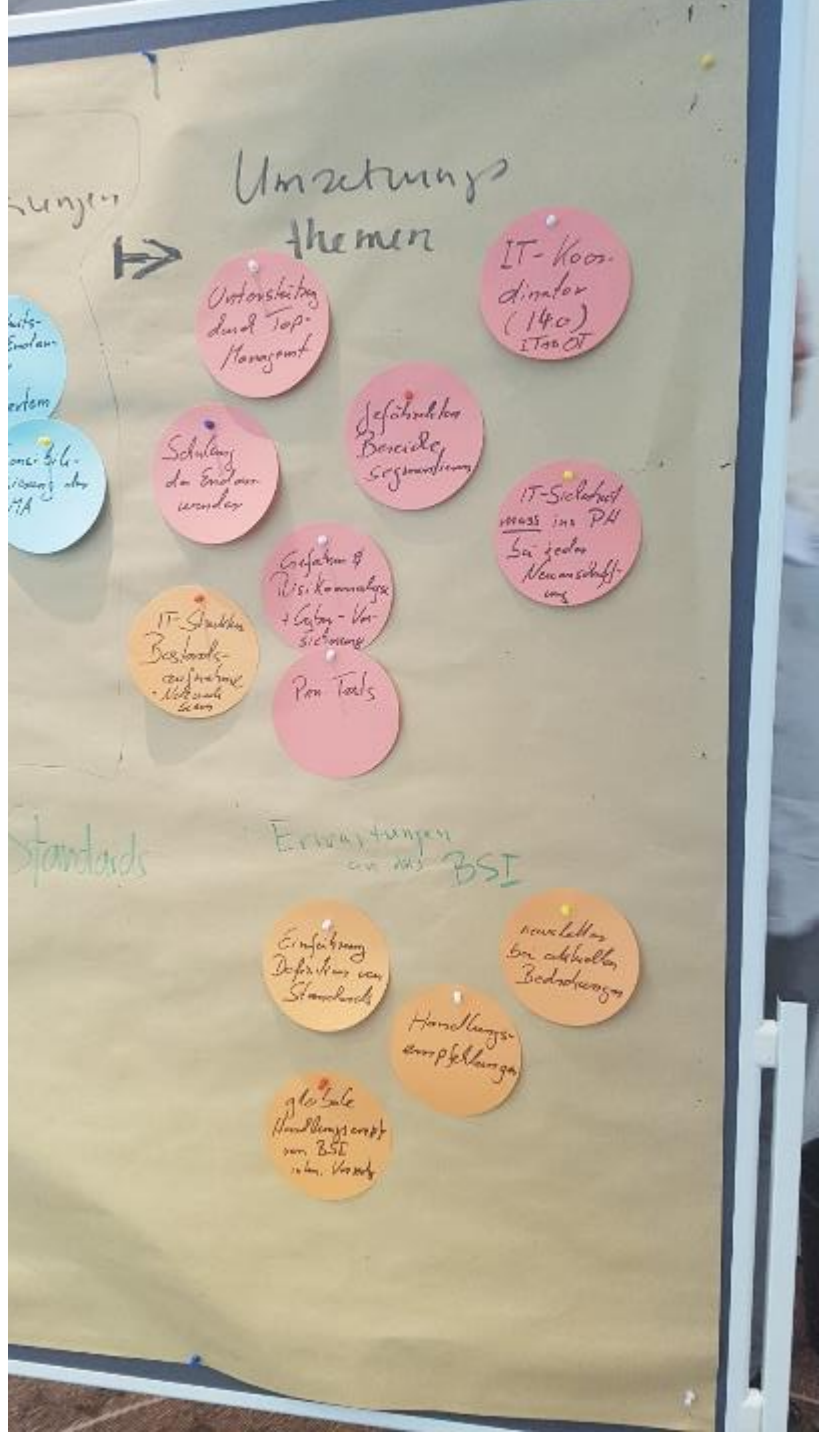

Effizienz
(Arbeitsfähigkeit)
vs.
Sicherheit
RICHTLINIEN (LEITFÄDEN) FÜR KUNDEN + FÜR LIEFERANTEN
IST DMZ (FW) FÜR LEGACY SYSTEME GENUG?
Aktuelles
Asset - Mgm
inkl.
Mobile, Kaffeemaschi,
...
Sicherheit von Gateways mit Schnittstelle
LoRA
Bluetooth etc
UNTERSTÜTZUNG FÜR SICHERES VERHALTEN
Sicherheit für Architekturen der Zukunft
„Industrie 4.0",
IIoT, 5G
BSI elearning für Sensibilisierung
Fernwartung
SEC-CHECKLISTE
"NEUES GERÄT"
IM FIRMENNETZ
(FRAGEN AN HERSTELLER)
BSI
zeitnahe Infos
Handlungs-
Security
von


IM FIRMENNETZ
(FRAGEN AN HERSTELLER)
BSI
Zeitnahe Infos über aktuelle Bedrohungen
⇒ Handlungs-Leitfäden
Security von Embedded Devices!
Wer prüft?
STAND DER TECHNIK BEI SW?
Definition Stand der Technik
Sicherheits-zertifizierungen für Produkte
CEO AWARENESS

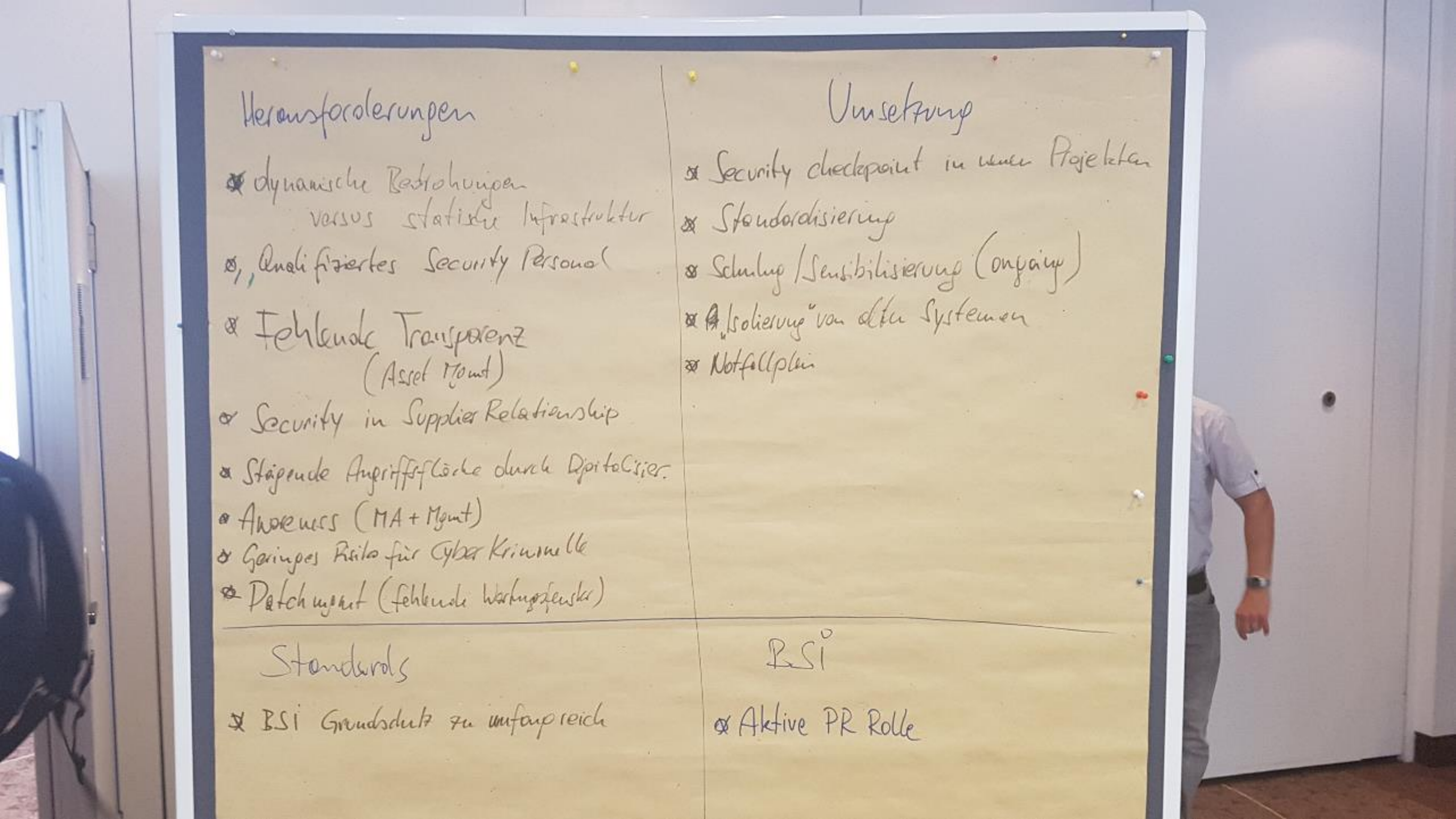

Herausforderungen
+
Gefahren
Umsetzungs
themen
Umgang mit den Daten "Gold der Zukunft"
Heterogene Systeme + Programme + Appl. in der Produktion
Komplexe Systeme → mehr ext. Support → mehr Fernzugriff
OT mehr Vernetzung → größere Anfälligkeit
Gefahr durch Office → Emails
durch Social Engineering
Leitwarten ziehen sich nach der §3 aus der Verantwortung
Rechtliche Situation → OEM/Endkunde
Alles muß immer online sein
IT als Enabler wahrnehmen
Widerständer Awareness
Security vs. Usability
Aufwand & Komplexität
Detection (Vollständigkeit)
Know-How
Notfallplan

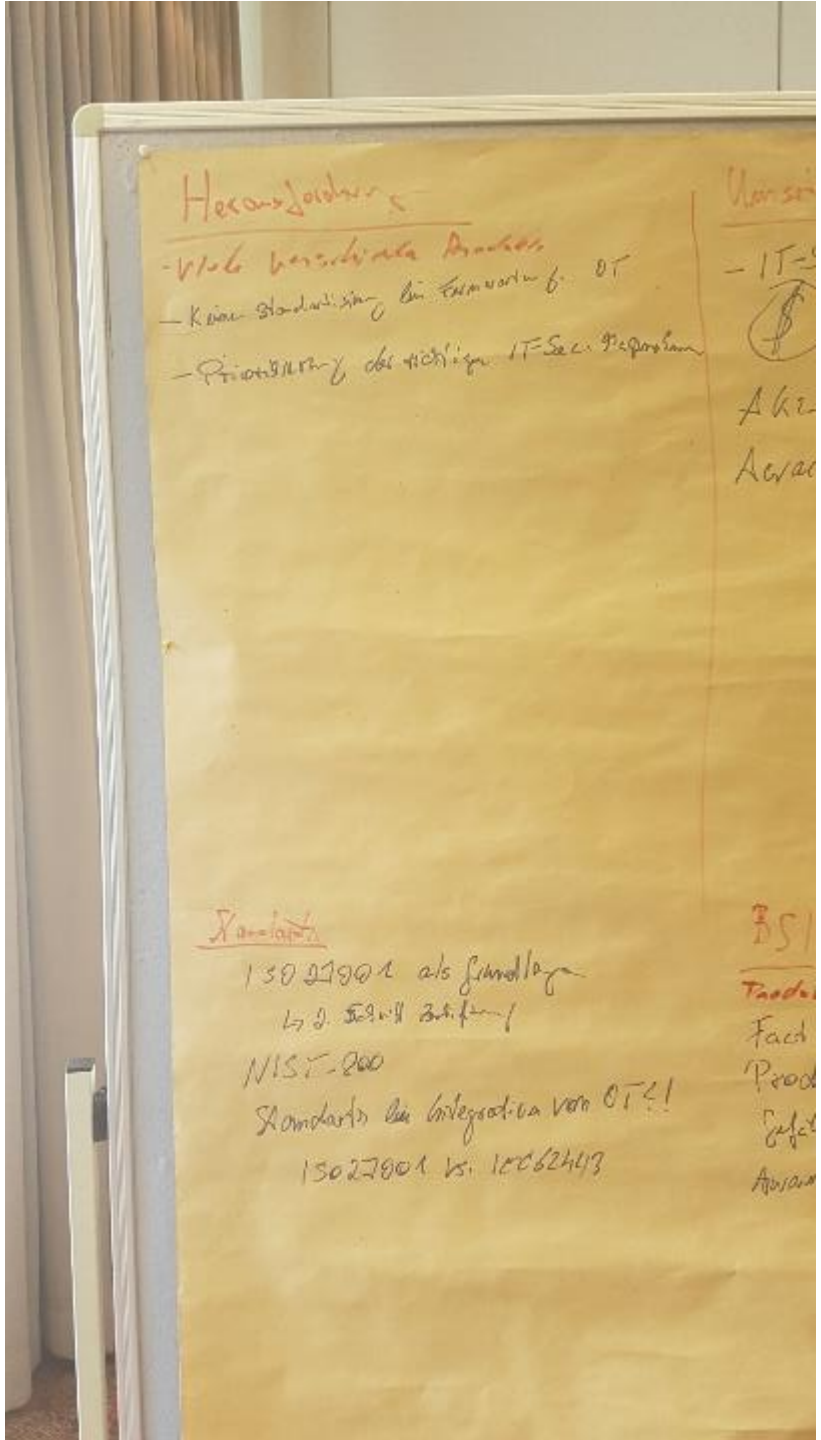

Umgesetzte Standards
IEC 62443
BSI
Umsetzung
VDMA
ZVEI
Eigene Spezifikationen
Fachveranstaltungen
Erfahrungsaustausch
Expertenmeetings
Erwartungen an das BSI
Anforderungen
- must
- opt.
- nice
spezifizieren
Bessere Vorgaben + Unterstützung für die Betreiber

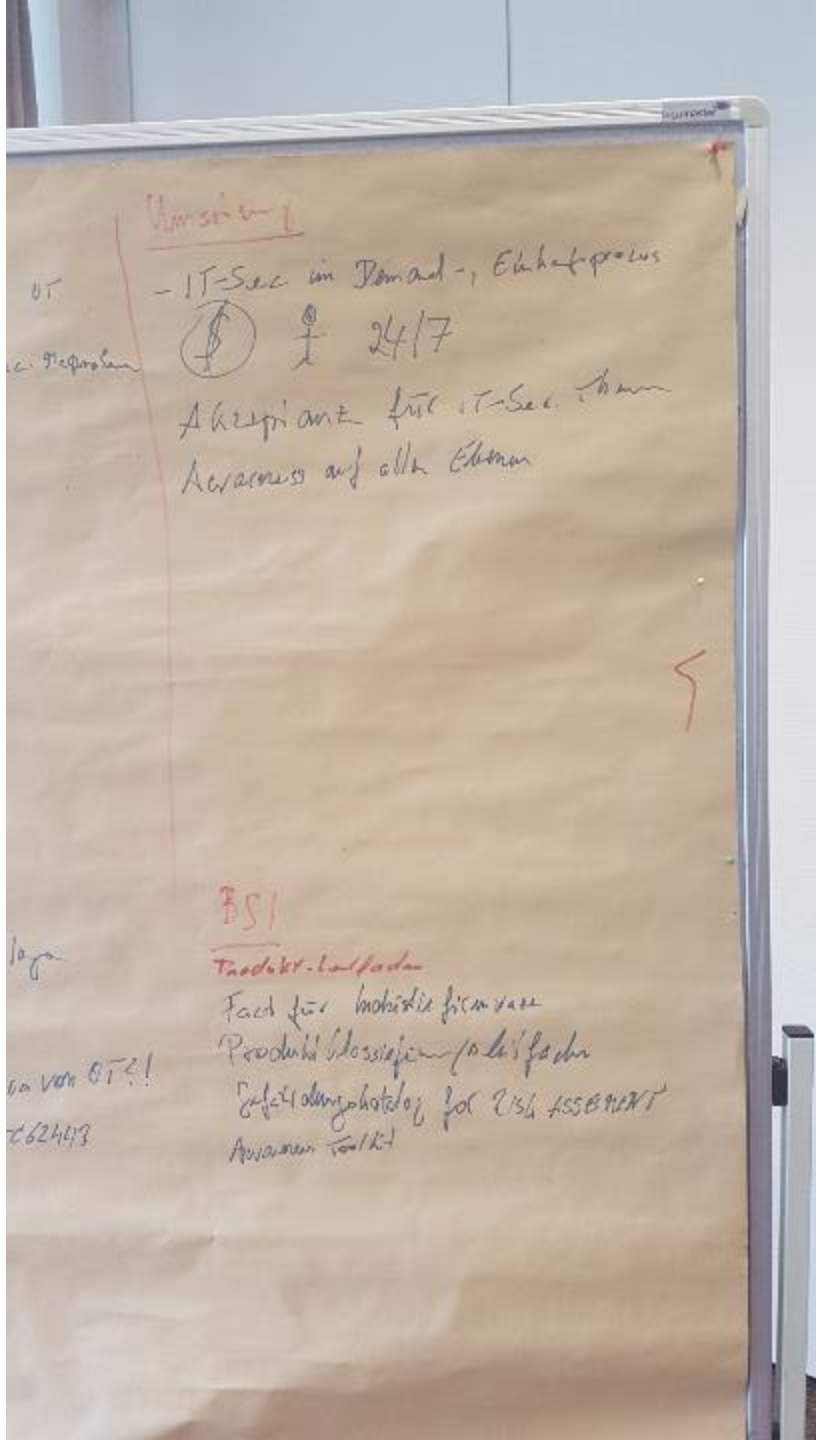



Bundesamt für Sicherheit in der Informationstechnik


Herausforderungen
dynamische Bedrohungen versus statische Infrastruktur
Qualifiziertes Security Personal
Fehlende Transparenz (Asset Mgmt)
Security in Supplier Relationship
Stätige Angriffsflächen durch Digitalisier.
Awareness (MA + Mgmt)
Geringes Risiko für Cyber Kriminelle
Patchmgmt (fehlende Wartungsfenster)
Umsetzung
Security checkpoint in neuen Projekten
Standardisierung
Schulung / Sensibilisierung (ongoing)
„Isolierung" von alten Systemen
Notfallplan
Standards
BSI Grundschutz zu umfangreich
BSI
Aktive PR Rolle




Bundesamt
für Sicherheit in der
Informationstechnik