



# **STILLSTAND VERMEIDEN – CYBERSECURITY SMART UMSETZEN!**

**WKOÖ Webinarreihe Experts Group IT-Security 2025**

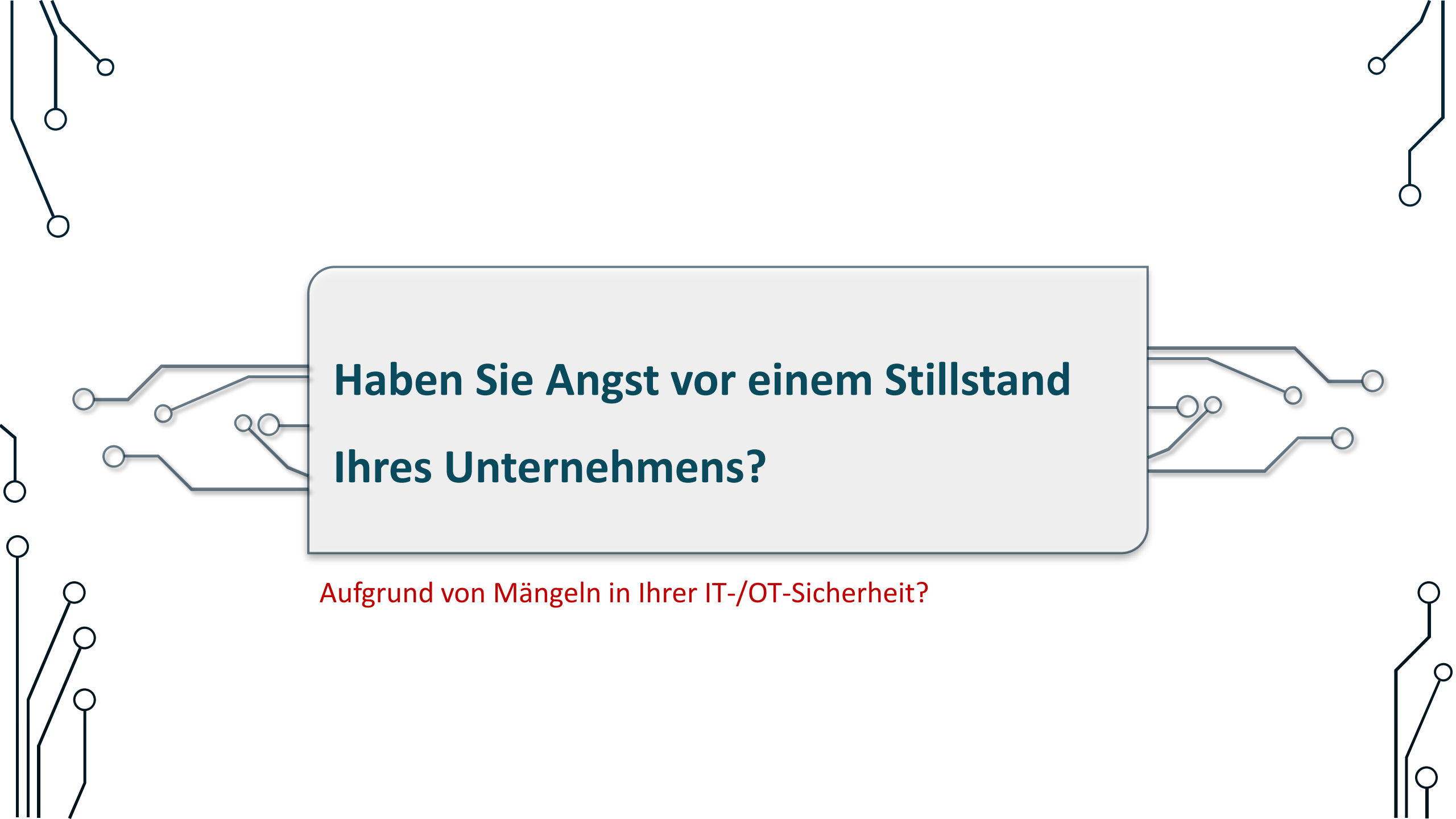
**04. November 2025**

Experts Group IT-Security

# **STILLSTAND VERMEIDEN – CYBERSECURITY SMART UMSETZEN**

**mit Barbara Hauer und Thomas Pfeiffer**



The background of the slide is decorated with stylized circuit board traces. These lines are dark blue and feature small white circles at various points, resembling solder points or vias. The traces are distributed across the corners and sides of the slide, framing the central content area.

## **Haben Sie Angst vor einem Stillstand Ihres Unternehmens?**

Aufgrund von Mängeln in Ihrer IT-/OT-Sicherheit?

# INFORMATION != OPERATIONAL TECHNOLOGY

## Geschäftsprozesse

IT-Systeme (Server, PCs,  
Drucker, Smartphones, ...)  
TCP/IP-Netzwerke  
Standardisierte Protokolle

## Fokus

Information und Daten  
Compliance

## Prioritäten

Vertraulichkeit  
Integrität  
Verfügbarkeit

## Systeme

Sichtbar für IT-Security  
Aktualisierbare Systeme  
Lebensdauer ~ 3 Jahre



## Information Technology (IT)

## Physische Prozesse

Industrielle Systeme (ICS, SCADA,  
PLC, Sensoren, ...)  
Industrielle Netzwerke  
Proprietäre Protokolle

## Fokus

Automation  
24/7 effiziente Produktion  
Real-time

## Prioritäten

Safety  
Verfügbarkeit  
Integrität  
Vertraulichkeit

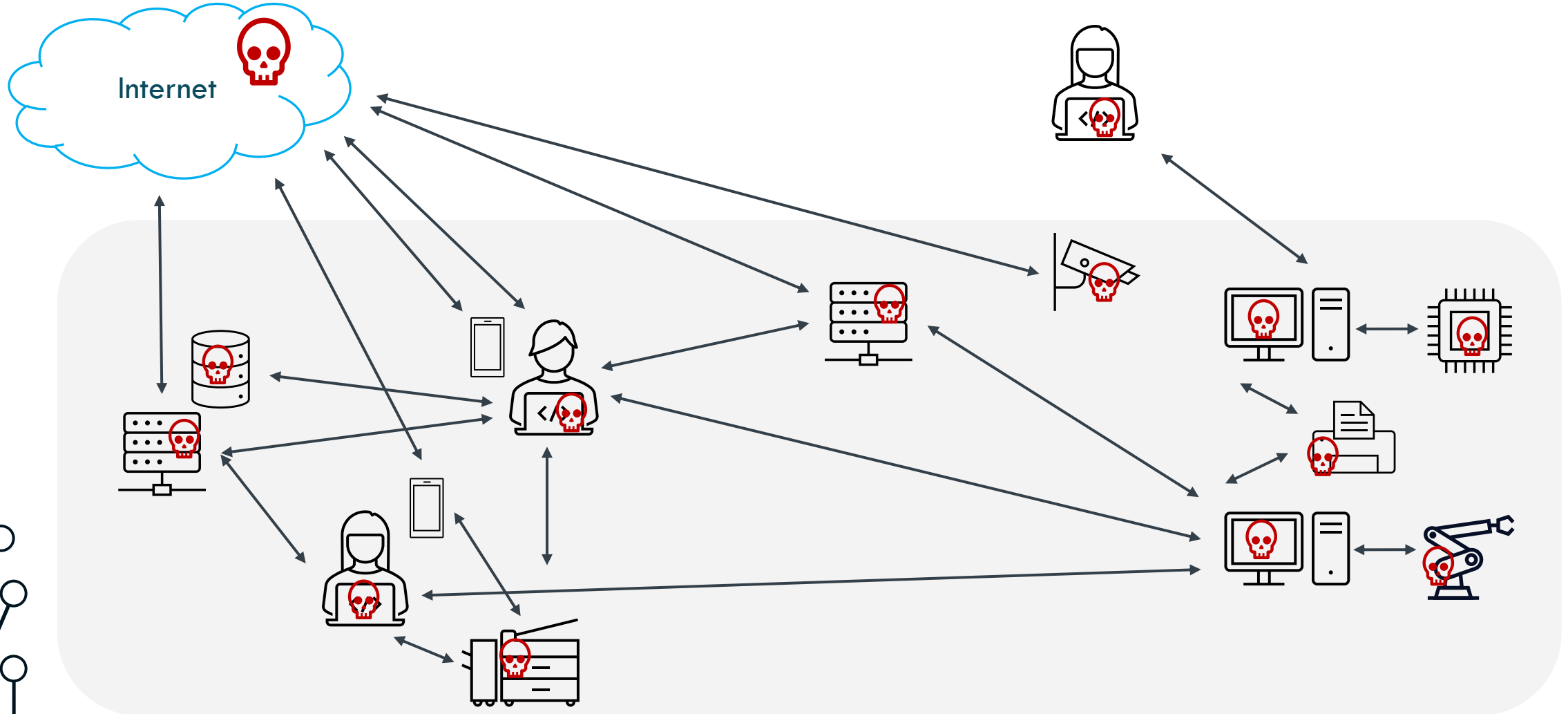
## Systeme (Assets)

Unsichtbar für IT-Security  
„Sensible“ Legacy Systeme  
Lebensdauer > 30 Jahre

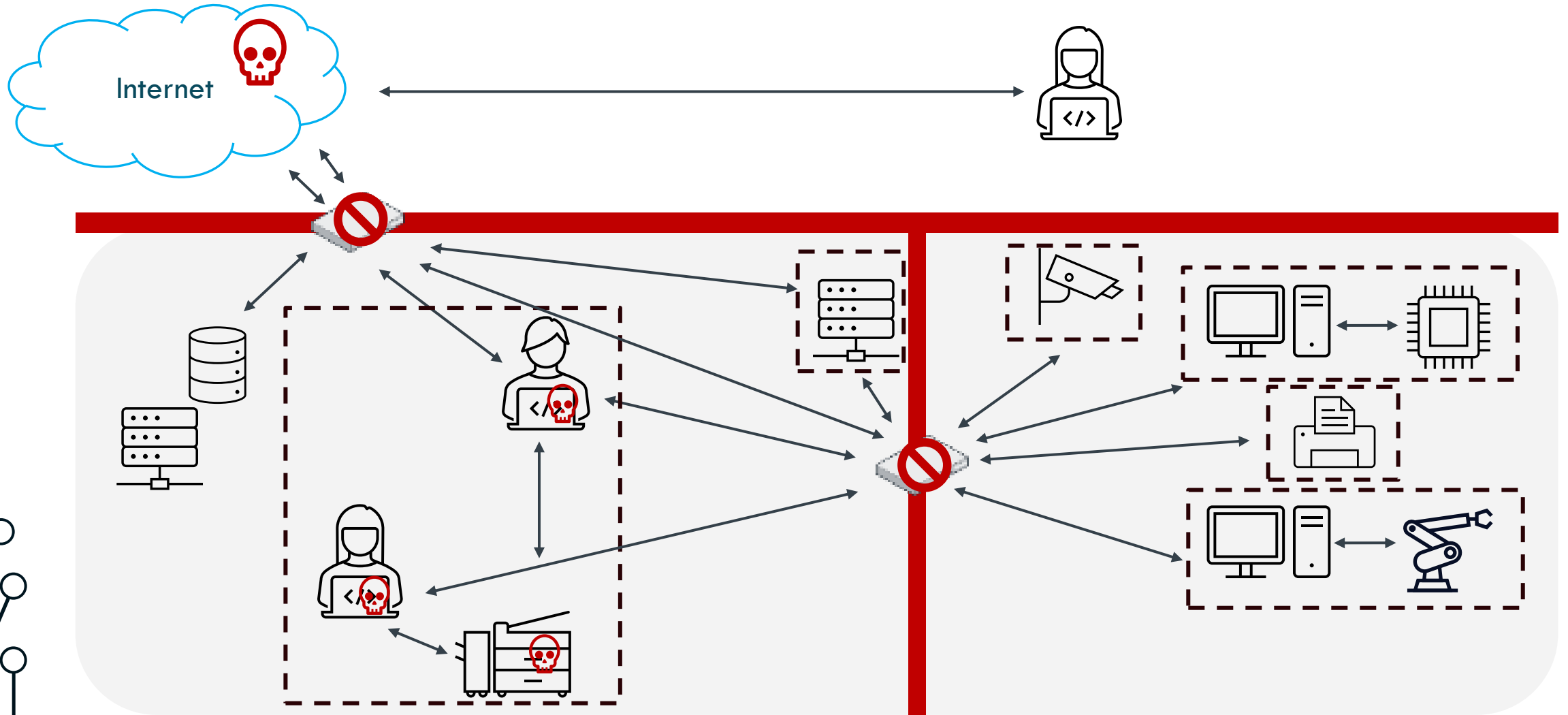


## Operational Technology (OT)

# BEDROHUNGSSZENARIO



# GEGENMAßNAHMEN ERGREIFEN



# CYBER RESILIENCE ACT (CRA)

## Aktuell

Unzureichendes Cybersicherheitsniveau in vielen Produkten

Mangel an rechtzeitigen Sicherheitsupdates für Produkte und Software

Auf den guten Willen von Herstellern der Produkte mit digitalen Elementen angewiesen

**10.12.2024**

CRA ist in Kraft getreten

**2026**

Juni: Vorgaben für Bewertungsstellen

September: Meldepflichten für Schwachstellen und Sicherheitsvorfälle

**11.12.2027**

Verpflichtungen gelten

## Fakten zum Cyber Resilience Act?

- EU-weit verbindliche Cybersicherheitsanforderungen für Hersteller und Händler
- Produkte mit digitalen Elementen, die in der EU hergestellt, importiert oder vertrieben werden
- CE-Kennzeichnung

# HOHES GEMEINSAMES CYBERSICHERHEITSNIVEAU VON NETZ -UND INFORMATIONSSYSTEMEN (NIS-RICHTLINIE)

## Aktuell

AT: *Netz- und Informationssystemsicherheitsgesetz (NIS-Gesetz)*

- Für hohes Sicherheitsniveau
- Betreiber wesentlicher Dienste
- Qualifizierte Stellen prüfen
- Österreichische Aufsicht: Bundeskanzleramt & BMI

**27.12.2022**

Veröffentlichung der EU NIS-2-Richtlinie

**16.01.2023**

In Kraft treten der EU NIS-2-Richtlinie

**04.11.2025**

Umsetzung durch die Mitgliedsstaaten:

- NIS-2 ersetzt NIS
- Wesentliche und wichtige Einrichtungen
- Nationale Aufsicht & EU
- ABER in Österreich noch nicht erfolgt: Entwurf des NISG 2024 im Nationalrat an der 2/3-Mehrheit gescheitert und nicht beschlossen.
- Regelungen sollten 2025 in Kraft treten

## Warum eine EU NIS-2-Richtlinie / Richtlinie (EU) 2022/2555?

- NIS 1 startete Umdenken: Katalysator für institutionelle und regulatorische Cybersicherheitskonzepte
- Mängel der initialen NIS-Richtlinie / Richtlinie (EU) 2016/1148 beheben
- Widerstandsfähigkeit gegen rasch verändernde und komplexe Bedrohungslage



# INTERVIEW



**Dr. techn. Barbara Hauer, MSc**

**QualiSecA GmbH**

Geschäftsführerin & Gründerin

Barbara@QualiSecA.at



**Thomas Pfeiffer, BSc MSc**

**Council.at GmbH**

Geschäftsführer & Gründer

T.Pfeiffer@council.at

# WAS SIND IHRE ANFORDERUNGEN?

Ihr Fokus  
Ihre Stärken  
Ihre IST-Situation



Wo brauchen Sie  
Unterstützung für  
Ihre Soll-Situation?



Dr. techn. Barbara Hauer, MSc

[barbara@qualiseca.at](mailto:barbara@qualiseca.at)