# Industrial Cyber Security Servcies für den Mittelstand

## Wie erreicht man ausreichenden Schutz vor drohenden Cyberangriffen in IACS und in industriellen Netzen?

**Dirk Kretzschmar, CEO TÜViT**



**Messe Hannover, 07.04.2022**

TÜViT

# Cybersecurity Deutschland – Lagebericht BSI 2021



Die Frage ist nicht mehr, ob man ein mögliches Angriffsziel ist, sondern nur noch wann der Angriff erfolgt und wie gut man dann darauf vorbereitet ist

# Maßnahmenempfehlungen des Nationalen IT-Krisenreaktionszentrums

zur aktuellen Entwicklung der Ukraine-Krise
CSW-Nr. 2022-197345-1012, Version 1.0 vom 24.02.2022

**3 / Orange** Die IT-Bedrohungslage ist geschäftskritisch.
Massive Beeinträchtigung des Regelbetriebs.

TÜVIT
TÜV NORD GROUP

Bundesamt für Sicherheit in der Informationstechnik

Nationales IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | **VORFALL** | IT-ASSETS

## Sonderlagebericht des Nationalen IT-Krisenreaktionszentrums

*Aktuelle Entwicklungen zur Ukraine-Krise*

*CSW-Nr. 2022-197345-1012, Version 1.0, 24.02.2022*

IT-Bedrohungslage*: 3 / Orange

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

**TLP:WHITE: Unbegrenzte Weitergabe**

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP" zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP

### Sachverhalt

Am frühen Morgen des 24. Februar 2022 kam es zu einer Invasion russischer Kräfte in das Staatsgebiet der Ukraine. Diese militärische Operation wurden durch Verfügbarkeitsangriffe auf Webseiten sowie Sabotage-Angriffe (Wiper) auf ausgewählte ukrainische Institutionen begleitet:

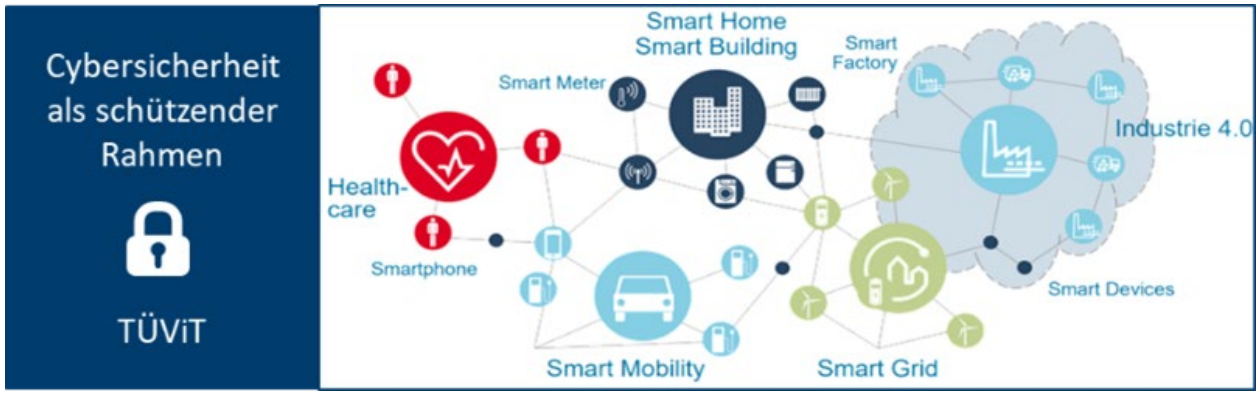
- Die DNS-Amplification DDoS-Angriffe waren auf Webseiten zweier ukrainischer Banken und auf Webseiten ukrainischer Ministerien sowie des Parlaments beschränkt.
- Nahezu zeitgleich wurden Daten-Lösch-Programme, sogenannte Wiper, auf ukrainischen Rechnern entdeckt.
  Betroffen waren (ungenannte) Banken, sowie Dienstleister der ukrainischen Regierung mit Sitz in Litauen und Lettland. Der genaue Zweck der Wiper-Angriffe ist bisher nicht bekannt.
  Der Wiper besitzt keine neuen Methoden für den Angriffsvektor und keine automatisierte Verbreitungsfunktion. In Teilen scheint er auf im Vorfeld infizierte Systemen zum Einsatz gekommen zu sein.
  Da die Schadprogramme in einigen Fällen über Windows Group Policies verteilt wurden, müssen die Täter bereits entsprechende Administrator-Rechte und Zugang zu zentralen Servern gehabt haben.

Mehrere NATO-Partner sehen seit dem heutigen Tag vermehrte aggressive Scan-Aktivitäten in ihren Netzen.

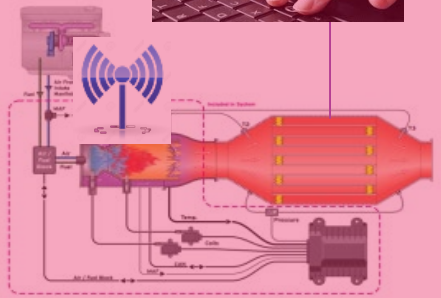
# Industrial Security


Mit allen Vorteilen der Digitalisierung (Industrie 4.0) werden Anlagen der Steuerungs- und Leittechnik zunehmend aus standardisierten Hardware- und Softwarekomponenten zusammengesetzt und vernetzt.

Die zunehmende Digitalisierung und erforderliche Vernetzung der Industrieanlagen führt zu einer **signifikanten Erhöhung der IT Sicherheitsrisiken**, der Rechnung getragen werden muss.



# Industrial Security



# INDUSTRIAL CYBER SECURITY

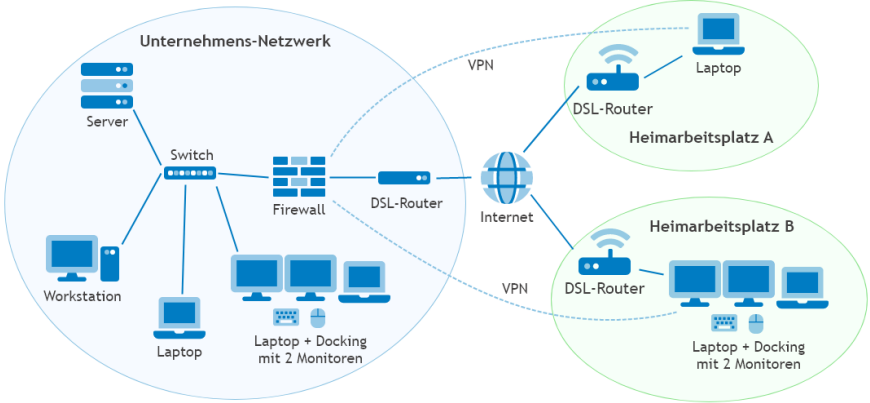
Die Digitalisierung von Industrial Automation & Control System (IACS) und die schnell wachsende Technologie für Industrie 4.0. erhöhen die Komplexität im Bereich der IT-Sicherheit

## zunehmende Vernetzung

- Innerhalb der OT-Umgebung (Operational Technology)
- Zwischen IT- und OT-Umgebungen
- Zwischen Geschäftspartnern (Lieferanten und Kunden usw.)

Zuvor isolierte Bereiche werden vernetzt. Das erhöht die Angriffsmöglichkeiten

# DIGITAL TRANSFORMATION





Office Network
VSAT Dish
Windows
Firewall
Office PC
Laptop
IPPBX
24 port Switch
FXO
GSM gateway - Unitel
DECT base
Laptop
IP Phone 4m
Angola telecom line
Windows
WiFi Access point

# Security Services
at all levels

## ICT-Security at all levels of digital infrastructures.

**Organizations**

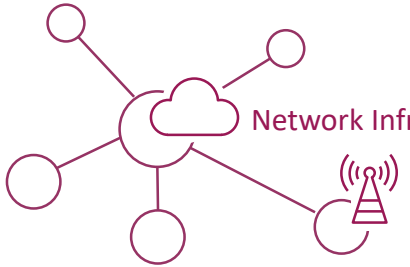
- Information Security Management (ISO/ITGS)
- Data Privacy (GDPR)
- ICT-Project and Quality Management
- Process Optimization

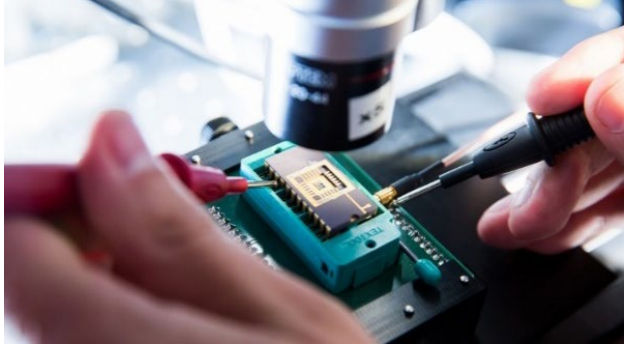
**Systems**

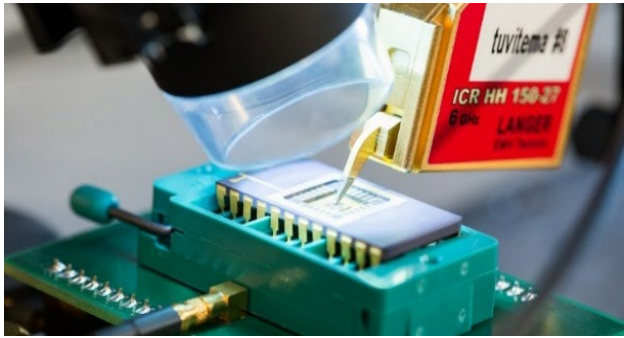
- Industrial Security (IEC)
- System & Network Security (NIST)
- Web App. & Mobile Security (OWASP)
- Data Center (TSI)

**Components**

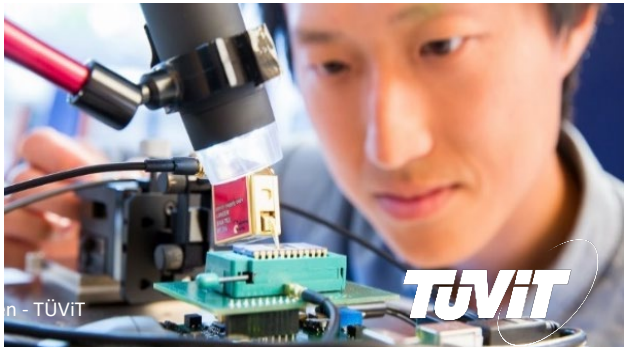
- Product Evaluation (CC)
- Validation Tests (FIPS140-2)
- Security Tests/Assessments
- Source Code Analysis (SW/Embedded)



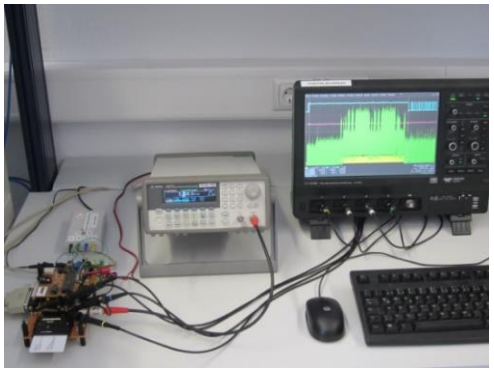






# Our hardware laboratory service is a core competence of TÜViT.



# Fehlerattacken - alternative Fehlerquellen (invasiv/minimal invasiv)

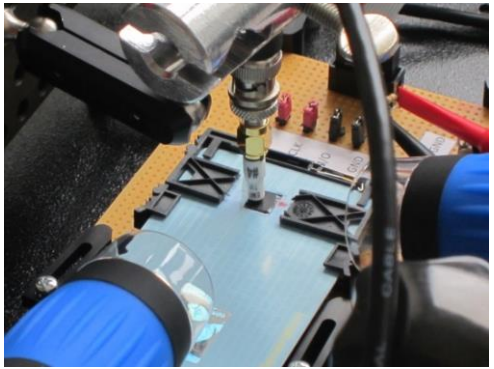


Voltage Glitches


Temperature

Manipulation von:

- Programmablauf (z.B. Übersprungbefehle)
- Berechnete Daten (z.B. Ergebnis einer Berechnung)
- Speicherinhalt (z.B. gespeicherter Wert)



EM pulses

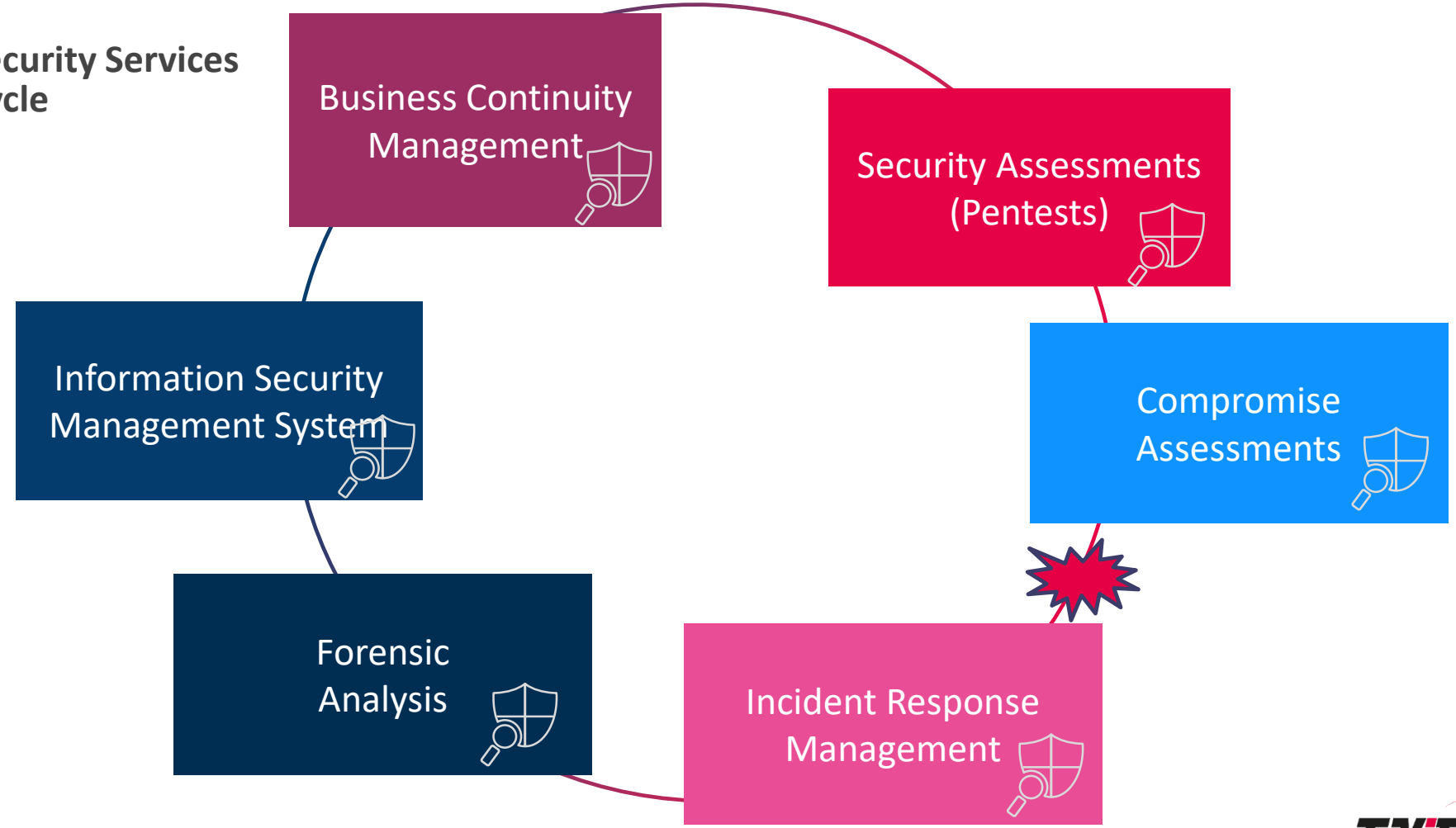
# SOFTWARE EVALUATION

Überprüfung des Quellcodes

- Vollständig automatisierte Testumgebung für die Bewertung von Protokollen und Kryptoalgorithmen
- Nutzung virtueller Testumgebungen für die Bewertung von Softwareprodukten
- Einsatz modernster Analyse- und Testwerkzeuge (z. B. Smart Meter Gateway Test Suite)
- Kontinuierliche Investition und Entwicklung von Testumgebungen, um die neuesten Technologien testen zu können


Building trust in IT security products – complete test concepts for software and hardware

# Security Services Cycle



# Industrial Security Assessments

Schwachstellenanalyse im industriellen Umfeld

# Industrial Security Assessments

Im Rahmen von Industrial Security Assessments kann die Sicherheit der im industriellen eingesetzten Lösungen bzw. Industrial Control Systems (ICS).

Dabei werden organisatorische sowie technische Gefährdungen auf verschiedenen Ebenen überprüft. Die Vorgehensweise der Experten orientiert sich dabei u.a. an den  Top 10 Bedrohungen für Industrial Control Systems (ICS) vom BSI.


https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/Allgemeine-Empfehlungen/Empfehlungen-fuer-ICS-Betreiber/empfehlungen-fuer-ics-betreiber.html

# Industrial Security Assessments

Zu den Top 10 Bedrohungen für Industrial Control Systeme gehören

- Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
- 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
- Kompromittierung von Smartphones im Produktionsumfeld


(Quelle Bundesamt für Sicherheit in der Informationstechnologie)

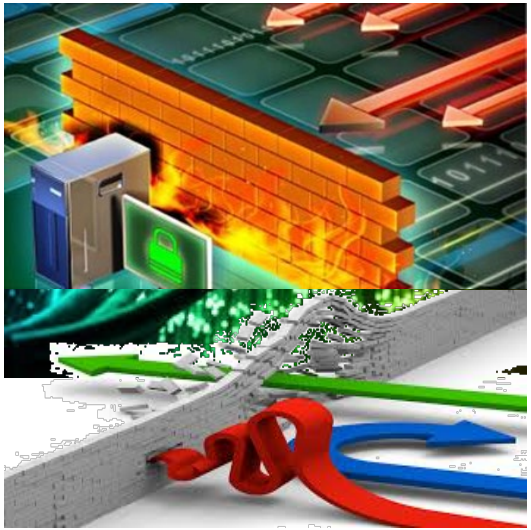
# Industrial Security Assessments

Im Rahmen des Assessments werden verschiedene Module angewendet.
Jeder Test umfasst dabei Angriffstechniken, die  Hacker anwenden

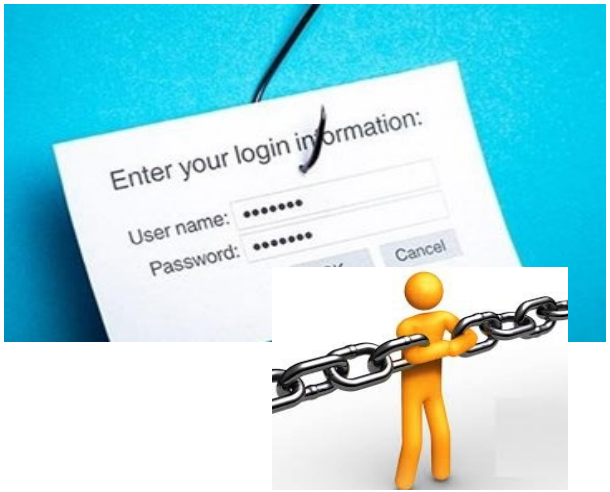
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Begehungen | Physische Sicherheit | IT-Räume | Social Engineering | … | | | |
| Interviews / Review-Dokumentation | Firewall Review | Netzwerk-architektur | Sicherheits-konzepte | Backup / Restore | … | | |
| Technische Tests / Pentests | System Review | Aktive / Passive Scans | MES / PCS Systeme | WLAN-Sicherheit | Daten banken | Fern wartung | |
| | (Web-) Anwendungen | Infrastruktur komponenten | Passwort sicherheit | Virus Scans | Security Systems | … | |

# INDUSTRIAL SECURITY ASSESSMENTS:

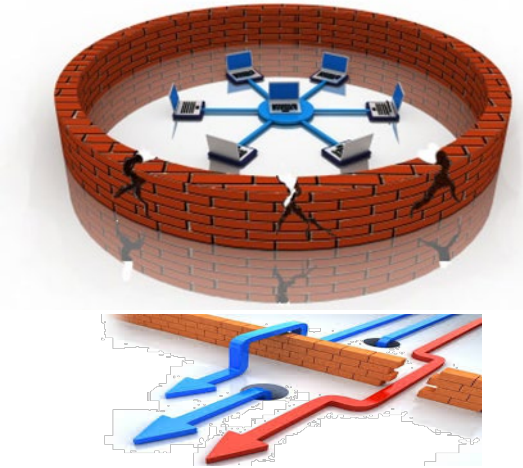
Netzwerkanalyse



Social Engineering




Umgehung der physischen Sicherheitsmaßnahmen und interne Bedrohungen



# Pentest von IT-Infrastrukturen

Port-& Schwachstellenscans

Manuelle Penetrationstests

Sniffing

Passives Mitlesen des Netzwerkverkehrs

Überprüfung der WLAN-Sicherheit

Host Discovery

Ermittlung von Systemen

Überprüfung der Härtung nach Best Practises / Konfigurationsanalysen

Review von Firewall-Regelwerken

Review von Sicherheits-richtlinien/-konzepten, Netzwerkarchitektur etc.

# ADVANCED PERSISTENT THREATS & SOCIAL ENGINEERING

Liebe [redacted]-Mitarbeitende,

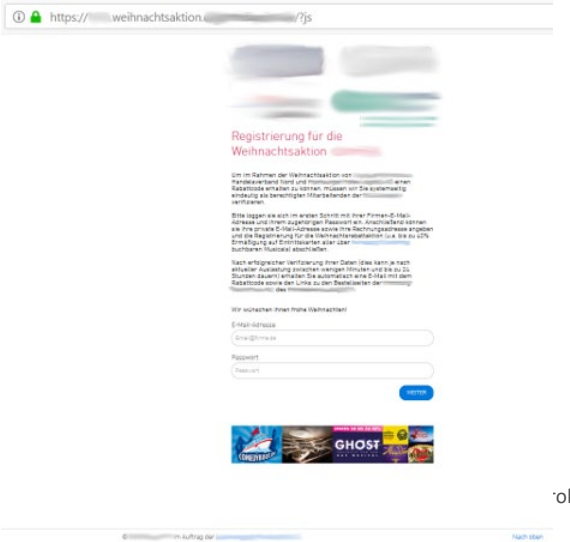
Weihnachten steht vor der Tür und Sie wissen immer noch nicht was sie Ihren Liebsten schenken sollen? Wie wäre es mit einem Last-Minute-Geschenkgutschein?

Im Rahmen einer gemeinsamen Weihnachtsaktion von [redacted] besteht ab sofort für alle Mitarbeitenden der [redacted] die Möglichkeit über die Internetseite https://[redacted]weihnachtsaktion.[redacted].de Gutscheine für diverse Kulturveranstaltungen, Musicals, Museen, Ausstellungen, Geschäfte des lokalen Einzelhandels sowie ausgewählte Online-Partner zu vergünstigten Konditionen zu erwerben. Dabei sind Rabatte von bis zu 40% möglich.

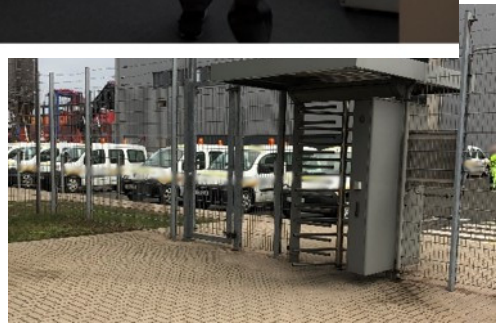
Die Registrierung zum Erhalt des Rabattcodes ist ausschließlich im Zeitraum vom 17.12.2018 bis zum 24.12.2018 möglich.

Mit freundlichen Grüßen
[redacted]
--
Leiterin Online und Event-Marketing
[redacted]
Ihre Agentur für Online- und Printmedien
[redacted]

Telefon: [redacted]
Fax: [redacted]
E-Mail: [redacted]



# Zutrittsschutz



# Zutrittsschutz

# IEC 62443:

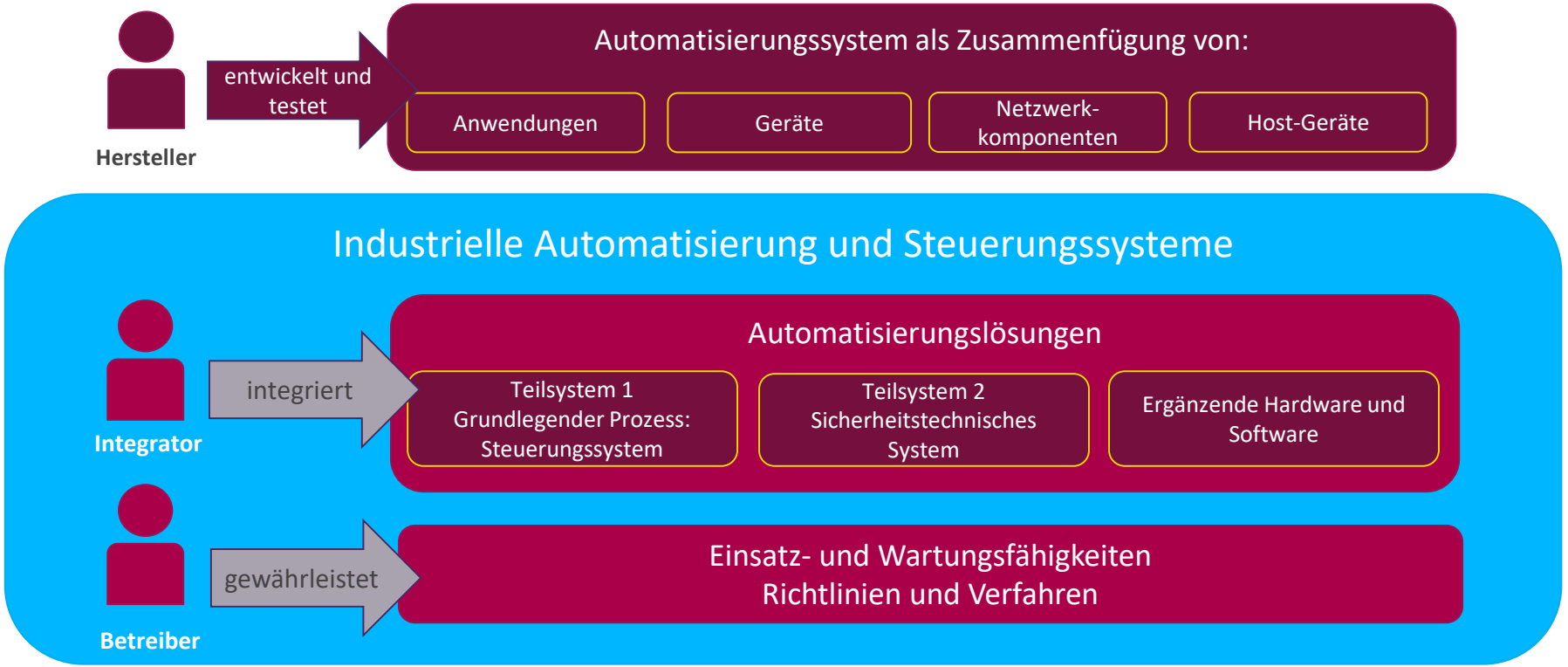
# Security for industrial control and automation systems

# MOTIVATION
## STANDARD FINDINGS


- NO patch management
- NO malware protection
- NO awareness on site
- NO backup

Die internationale Norm IEC 62443 befasst sich mit all diesen Fragen zur Sicherheit von IACS

# IEC 62443
## Definierte Rollen



# Übersicht IEC 62443

## IEC 62443 Normreihe

| Allgemein | Management System | Industrielle IT Sicherheit (IACS) | Eingebettete Sicherheitskomponenten |
|---|---|---|---|
| 1-1 Terminologie, Konzepte & Modelle | 2-1 Einrichtung eines IACS-Sicherheitsprogramms | 3-1 Sicherheits-technologien für IACS | 4-1 Anforderungen an die Produktentwicklung |
| 1-2 Glossar der Begriffe und Abkürzungen | 2-2 Betrieb eines IACS-Sicherheitsprogramms | 3-2 Sicherheitsrisiko-bewertung und Systementwurf | 4-2 Technische Sicherheits-anforderungen für IACS-Komponenten |
| 1-3 Metriken zur Einhaltung der Systemsicherheit | 2-3 Patch Management in der IACS-Umgebung | 3-3 Systemsicherheits-anforderungen und Sicherheitsstufen | |
| | 2-4 Anforderungen für Anbieter von IACS-Lösungen | | |

**Legende**

- Noch nicht veröffentlicht und zertifizierbar
- Veröffentlicht, noch nicht zertifizierbar
- Veröffentlicht und zertifizierbar

# Das Ziel muss eine ganzheitliche Security Beratung sein

**Information Security Management Systeme (ISMS)**

- Aufbau und Implementierung von Information Security Management Systemen (ISMS)
  - ISO 27001
  - IT Grundschutz
- Datenschutz

**Business Continuity Management & Notfallplanung (BCM)**

- Beratung für den Aufbau und die Implementierung von Business Continuity Management und Notfallplanung

**Digital Forensics & Incident Response (DFIR)**

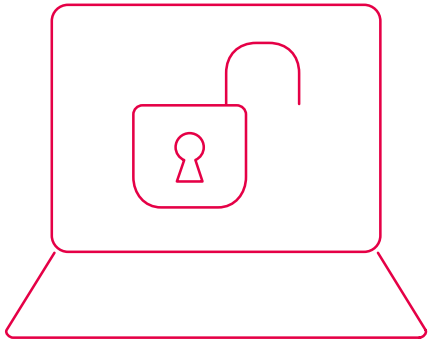
- Dienstleistungen zur Analyse und Aufklärung von Sicherheits-vorfällen
- Dienstleistungen zur Erkennung von Cyberangriffen
- Forensik-Rahmenverträge

Cybersecurity Services

# Compromise Assessment

## Compromise Assessment geht weiter als Pentesting

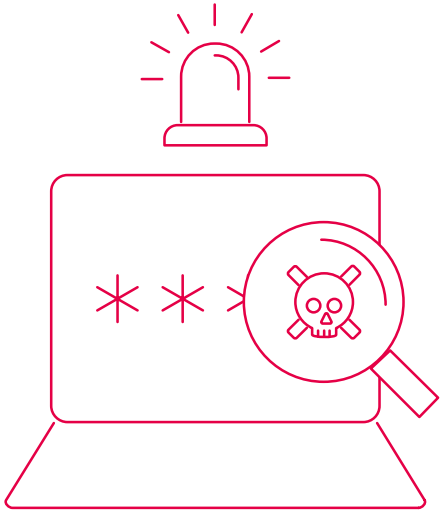
**Hackerangriffe zuverlässig erkennen.**



**Penetration Testing**

Hilft Ihnen Schwachstellen zu finden

**vs.**



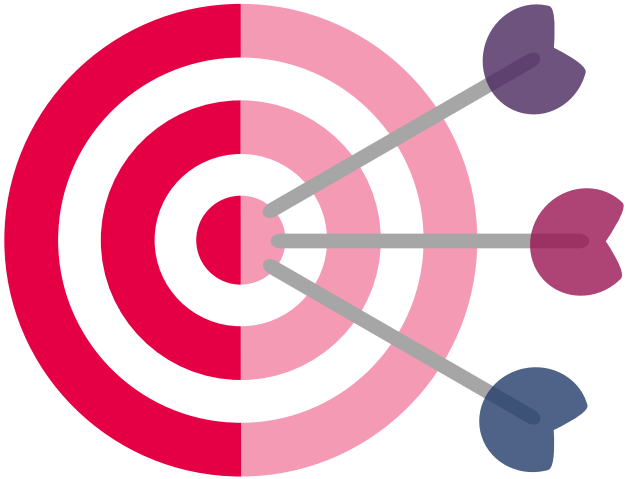
**Compromise Assessment**

Hilft Ihnen bereits erfolgte Hackerangriffe zu erkennen

# Compromise Assessment

## Angriffserkennung mit Compromise Assessment

**Cyberangriffe erkennen und abwehren!**



Wurden Schwachstellen ausgenutzt und sind IT-Systeme kompromittiert worden?

Tiefgreifende Untersuchung auf Betriebs-systemebene

Zuverlässiges Aufspüren von Angriffsspuren (IOC – Indicator of Compromise)

# Compromise Assessment

Mit uns erkennen Sie Hacker-Aktivitäten

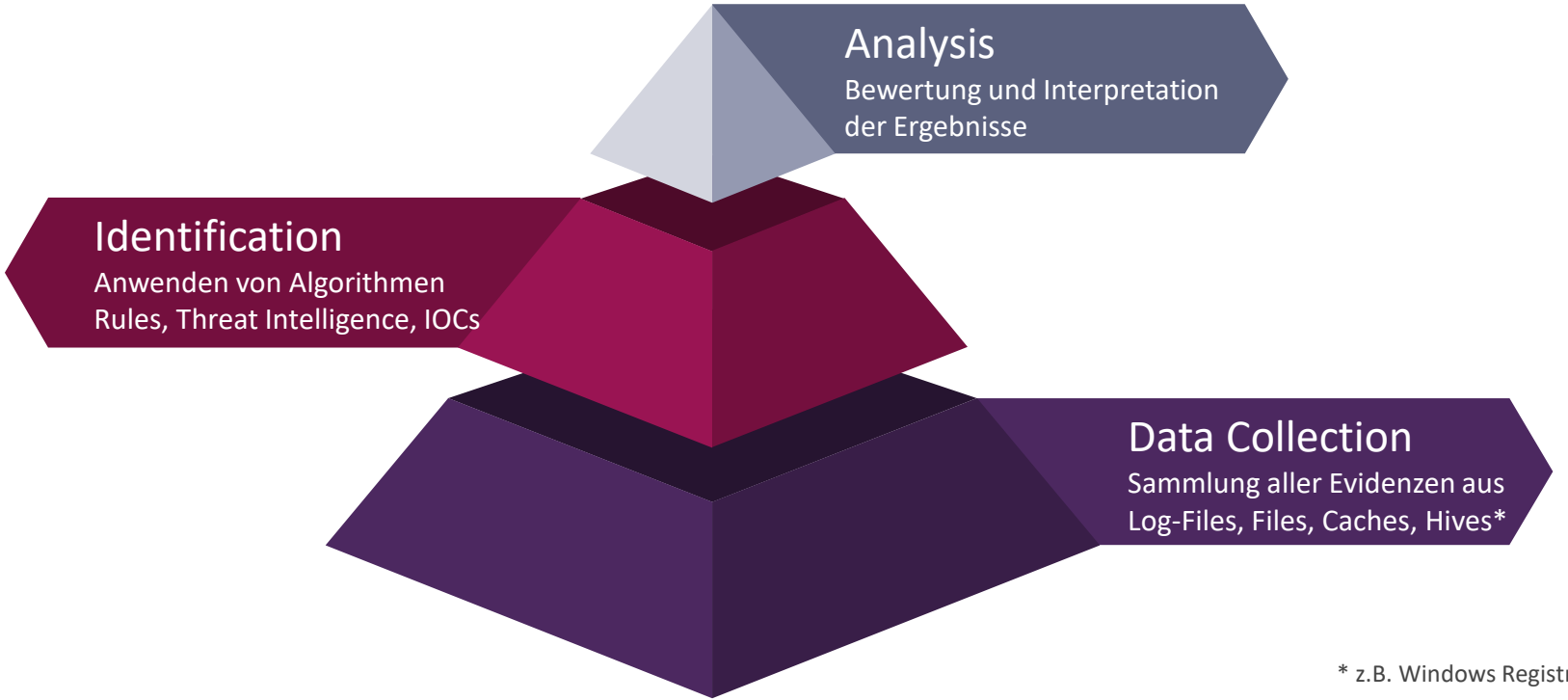
**Hacker-Aktivitäten auf Ihren Systemen erkennen.**

Mit Hilfe eines signaturbasierten Scanners werden
Systeme auf Hackeraktivitäten überprüft (>>12.000 Signaturen)

Diese Lösung wird vor Ort eingesetzt.
Daten verlassen ihr Unternehmen niemals.

# Compromise Assessment

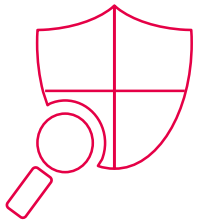
## Funktionsmodell eines Compromise Assessments




* z.B. Windows Registry

# Digital Forensics & Incident Response

## Der Forensik-Prozess Rahmenvertrag



### Ersthilfe

Erste qualifizierte Rückmeldung durch unsere Forensik Experten zur Abstimmung von Sofortmaßnahmen.

### Forensische Analyse

Remote oder Vor-Ort-Analyse der gesicherten Artefakte zur Aufklärung des Tathergangs.


### Fallaufnahme

Meldung des Sicherheitsvorfalls bei unserer Cyber Defense Hotline.

### Beweissicherung

Sicherung und Sammlung aller relevanten Evidenzen aus Hauptspeicher und Festplatten für die forensische Analyse.

### Wiederherstellung

Erstellen des Berichtes und Unterstützung bei der Umsetzung Behebungsstrategie.

# Compromise Assessment

## Die Daten sind sicher

Keine Daten verlassen das Unternehmen.

Es werden keine personenbezogenen Statistiken erstellt.

Es werden keine personenbezogenen Daten ausgewertet.

Die Auswertung erfolgt On-Site bei der TÜViT in Essen.

# Warum einen Forensik-Rahmenvertrag?

- ✓ Bei einem IT-Sicherheitsvorfall ist schnelle Hilfe gefragt
- ✓ Forensik Know-how ist rar
- ✓ Methoden, Equipment & Tools sind häufig nicht vorhanden
- ✓ Unsere Forensik-Experten sind erfahren und top-ausgebildet
- ✓ Betriebsunterbrechungen müssen so kurz wie möglich sein
- ✓ Eine Wiederholung des Cyber-Angriffs soll möglichst nicht stattfinden

**Schnelle Hilfe, wenn Sie sie brauchen.**

www.tuvit.de