TÜV Rheinland

Digital Bodyguard for Industry Transformation

Inter

- 10

Wolfgang Kiener Global Head of Advanced Threat Centre



What is a Digital Bodyguard?





Where to find the Digital Bodyguard?





Key Challenge of the Digital Bodyguard

Risks develop exponential in the digital transformation.



Technical Development
---- Know-How

INDUSTRY 4.0

- Automation
- Scalability and Interconnectivity
- AI and Machine Learning
- Agility

CYBER RISK 4.0

- Attack automation
- AI and Machine Learning
- Attackers are agile
- Complexity increases attack surface
- Vulnerabilities are hardly to avoid

Cyber Risk = Business Risk



A brief History on Attacks in OT

Attack frequency and impact is increasing





What do our Digital Bodyguards say?

TÜVRheinland[®]

Precisely Right.

TÜV Rheinland Industrial Security Survey 2019



Industrial Security in 2019: A TÜV Rheinland Perspective

www.tuv.com/informationsecurity

HAVE YOU IMPLEMENTED OPERATIONAL TECHNOLOGY-RELATED CYBERSECURITY POLICIES AND PROCEDURES IN YOUR BUSINESS?



What do our Digital Bodyguards say?

TÜVRheinland[®] Precisely Right.

TÜV Rheinland Industrial Security Survey 2019

Industrial Security in 2019: A TÜV Rheinland Perspective

www.tuv.com/informationsecurity

WHAT FRAMEWORKS OR STANDARDS DID YOU USE FOR THE [CYBERSECURITY RISK] ASSESSMENT? (MULTIPLE SELECTIONS POSSIBLE)

Global Industrial Control Systems Security Trends

Vulnerabilities and attacks continuously increase

DRAMATIC INCREASE IN ICS SECURITY VULNERABILITIES DISCLOSURES

GLOBAL TREND OF TARGETED INDUSTRIES

Source: Demonstrate relative attack frequency on industry based on sector reports

Source: Fireeye

Industrial Control Systems Vulnerability and Attack Trends Analysis

Comparing vulnerability and attack trends indicate corporate systems see most attacks; providing access for threat actors to exfiltrate data and infiltrate industrial networks

		VULNERABILITY DISCLOSED	CYBER ATTACKS
Level 5 Enterprise Business Zone (Internet, Servers, Corporate Applications)	Enterprise Systems		
Level 4 Business Unit Zone (Servers, Applications)	Business Planning & Logistics		
Level 3.5 Demilitarized Zone (Application Servers, Infrastructure)	Infrastructure and IT Systems		
Level 3 Operations Zone (Servers, Workstations)	Site Manufacturing Operations & Control		
Level 2 Supervisory Control Zone (SCADA, HMI, Engineering W/S Historian)	Area & Supervisory Control		
Level 1 Basic Control Zone (PLC, RTU)	Basic Control Devices		Ę
Level 0 Safety Zo Control Zone (Sensors, Actuators) Process I/O D	one Devices		
Safety Instrumented Systems			

Monitoring and Threat Detection is paramount

It is possible in OT environments as well.

Win a RISK ASSESSMENT

Hall 5 Booth 29

Wolfgang Kiener Global Head of Advanced Threat Center Phone +49 174 1880217

https://tuv.com/informationsecurity

LEGAL DISCLAIMER

This document remains the property of TÜV Rheinland. It is supplied in confidence solely for information purposes for the recipient. Neither this document nor any information or data contained therein may be used for any other purposes, or duplicated or disclosed in whole or in part, to any third party, without the prior written authorization by TÜV Rheinland. This document is not complete without a verbal explanation (presentation) of the content. TÜV Rheinland AG

