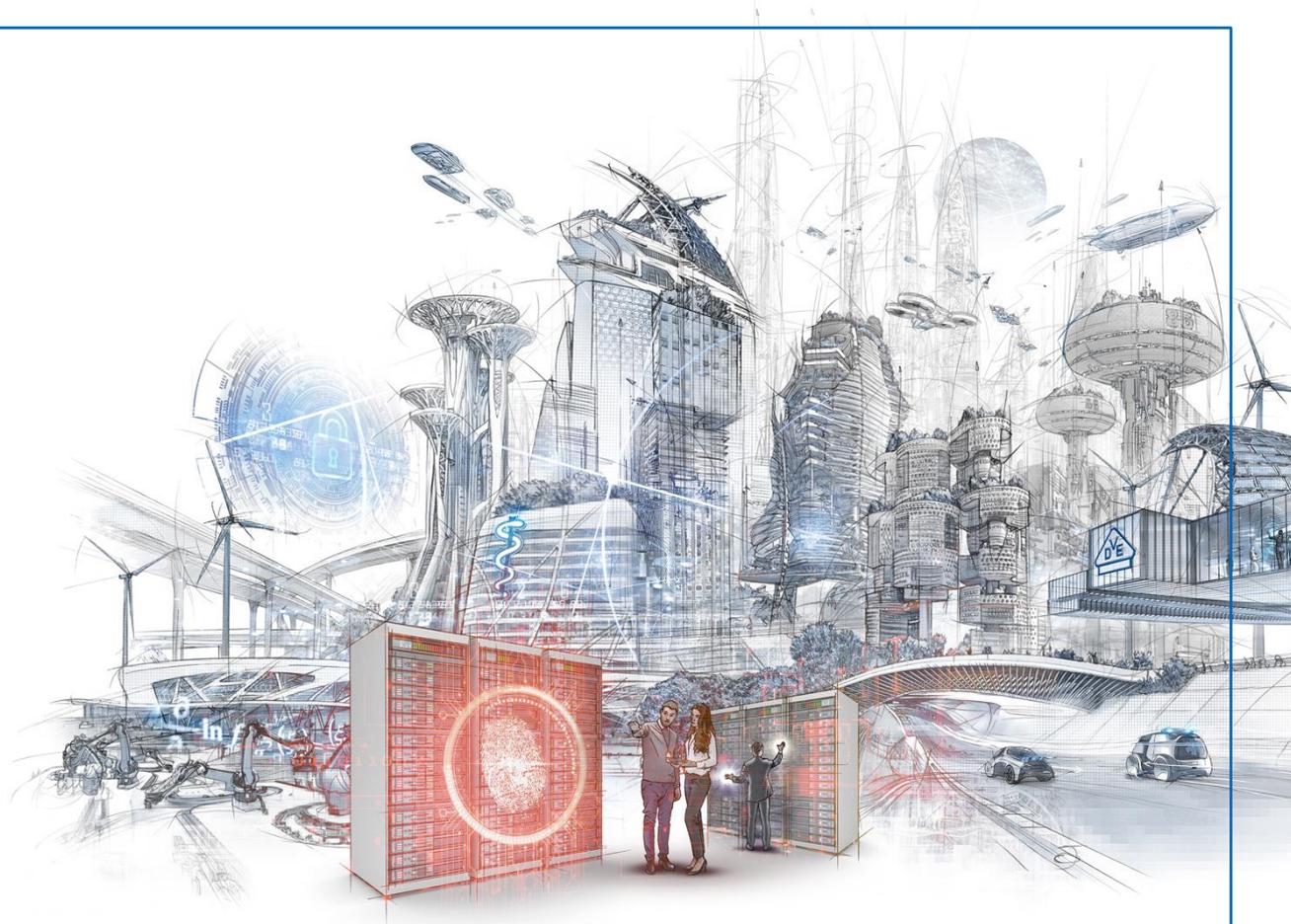


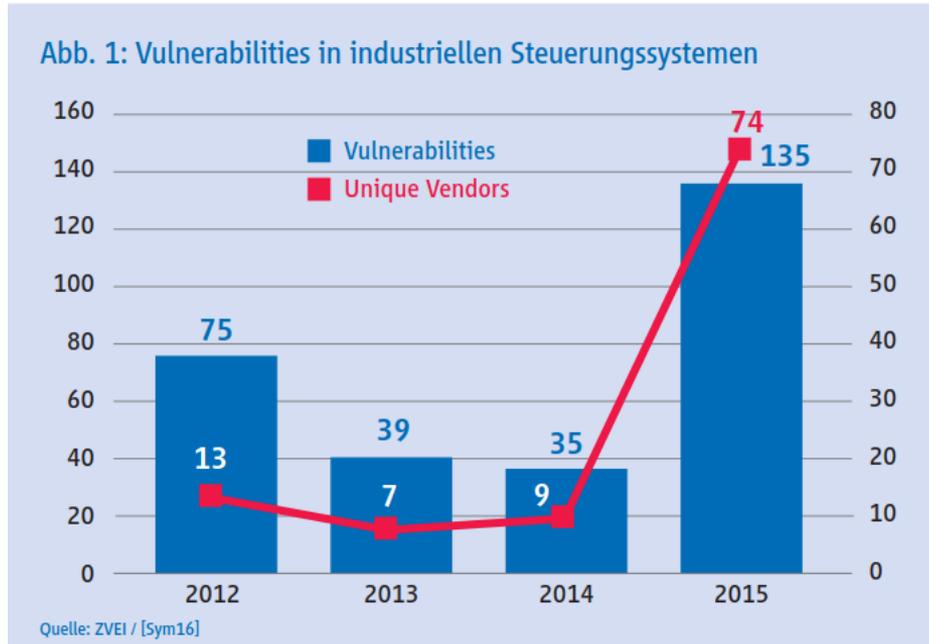
Cybersecurity CERT@VDE

Andreas Harner



Schwachstellenmanagement: Ein paar Zahlen...

Behauptung: „Die Anzahl von Schwachstellen steigt kontinuierlich an!“



- Stimmt diese Behauptung?
- Gibt es mehr oder weniger Schwachstellen?
- Gibt es mehr oder weniger Offenlegung?
 - Durch Externe?
 - Durch Interne?

→ Es werden mehr Schwachstellen gefunden!

Quelle: ZVEI: Orientierungsleitfaden für Hersteller zur IEC 62443

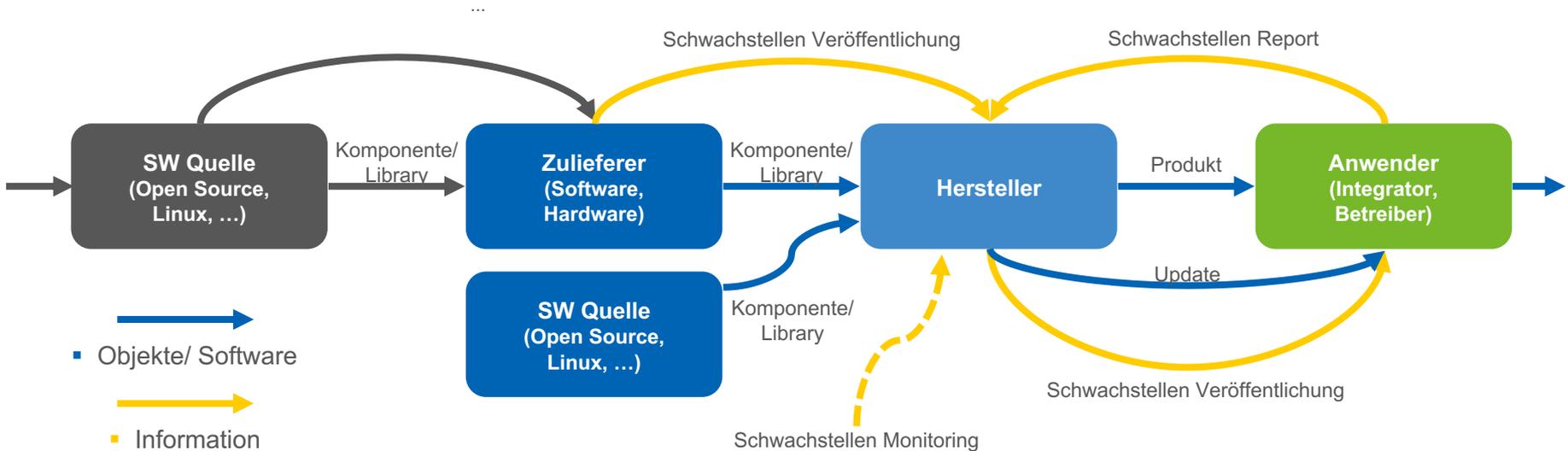
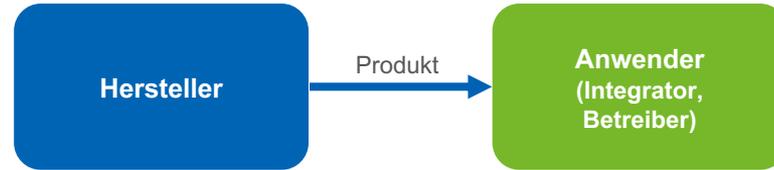
IEC 62443: Normative Anforderungen

General	Policies and procedures	System	Component
1-1 Technology, concepts and models	2-1 Requirements for an IACS security management system Ed 2.0 Profile of ISO 27001/27002	3-1 Security technologies for IACS (TR)	4-1 Secure product development lifecycle
1-2 Master Glossary of terms and abbreviations	2-2 <i>Implementation guidance for an IACS security management system</i>	3-2 Security risk assessment and system design	4-2 Technical security requirements for IACS products
1-3 System security compliance metrics	2-3 Patch management in the IACS environment (TR)	3-3 System security requirements and security levels	
1-4 System security lifecycle and use case	2-4 Requirements for IACS solution suppliers		
Definitions Metrics	Security Requirements for plant owner and suppliers	Security Requirements for a secure system	Security Requirements for secure components
		Process requirements	Functional requirements

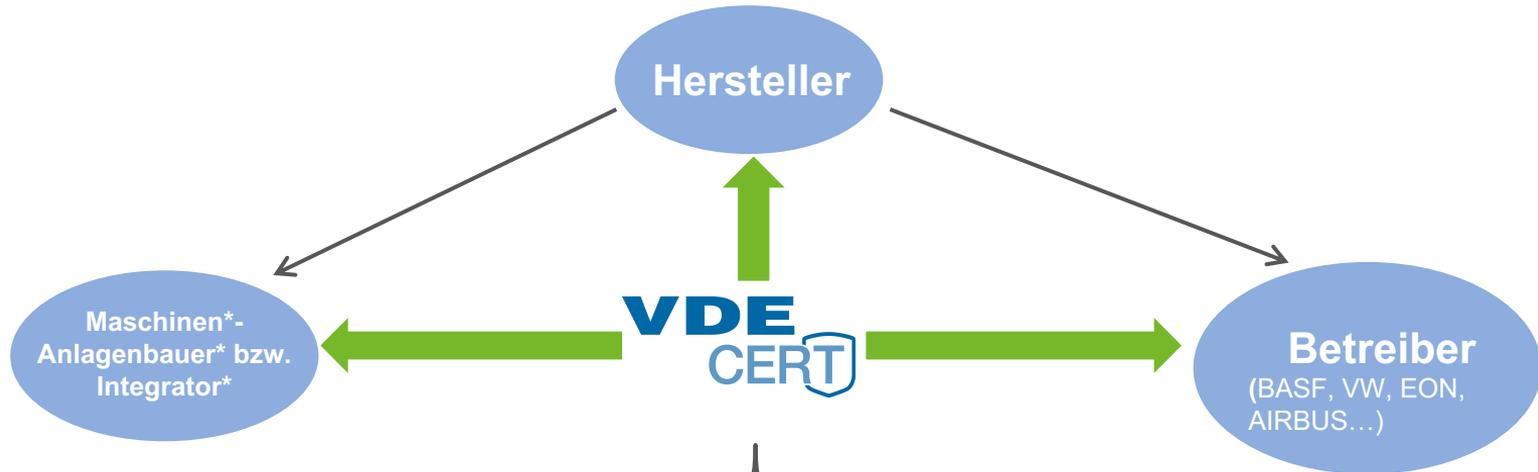
Motivation für CERT@VDE: Beziehung Hersteller - Kunde

Traditionell → Einbahnstraße

Heute → Netzwerk



CERT@VDE als koordinierendes Produkt-CERT (PSIRT)



CERT@VDE und IoT Inspector Schwachstellen in Firmware auf der Spur



IoT Inspector
The Firmware Security Analysis Platform

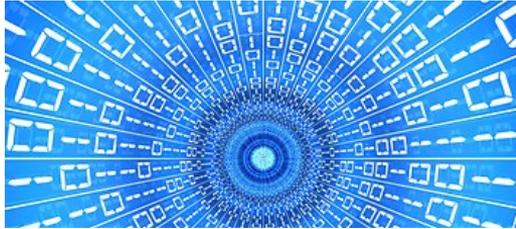


Die Automatisierte Sicherheitsanalyse für IoT-Firmware.
Einfach die Firmware hochladen, die Analyse starten und wenige
Minuten später stehen die Ergebnisse zur Verfügung.

V082018_DE

The image is a promotional graphic for IoT Inspector. It features a background of a city skyline at sunset with a network of glowing blue nodes and lines overlaid. The nodes are connected by thin white lines, creating a mesh-like structure. Several nodes are highlighted with larger, semi-transparent blue circles containing icons: a cloud, a Wi-Fi symbol, a plus sign, a house, and a bus. The overall color palette is dominated by blues and greys, with a warm orange glow from the setting sun on the right side.

CERT@VDE im VDE



Wissenschaft Technologien Innovationen

- Wissenstransfer im Expertennetzwerk
- Technologie- und Bildungspolitik
- Nachwuchsförderung



Normen Standards Grundlagen

- Internationale Normen und Standards



gemeinnützig



Prüfung Sicherheit Verbraucherschutz

- Produktprüfung und Zertifizierung

CERT@VDE – Mitmachen und Vorteile nutzen!

! Frühwarnsystem durch Wissensvorsprung

Frühzeitigeres Erkennen von Schwachstellen ermöglicht Partnern eine bessere Einschätzung!
...und dadurch eine schnelle, strukturierte Reaktion auf aktuelle Bedrohungen!

⚖ Minimierung Haftungsrisiken

- Best Practices des CERT@VDE unterstützen die Einhaltung von rechtlichen Vorgaben hinsichtlich „im Verkehr erforderliche Sorgfalt“ und „Stand der Technik“
- Bessere Nachweisbarkeit des richtigen Verhaltens „im Ernstfall“ durch Dokumentation
- Vertragliche und gesetzliche Produktbeobachtungspflichten der Partner werden unterstützt
- Das CERT@VDE hilft auch bei Kritis-Fällen, um die richtigen Wege zu gehen

🧠 Prozesse

- CERT@VDE stellt Partnern abgestimmte und solide Prozesse zur Verfügung
- Partner können diese Prozesse in eigene, übergeordnete Security-Prozesse integrieren
- Dadurch u.a. Hilfe bei der Umsetzung der IEC 62443



Single Point of Contact

- für Hersteller, Maschinenbauer (Integratoren), Betreiber
- für Behörden (z. B. BSI, Verfassungsschutz)
- für andere CERTs, CERT-Verbund
- für Security Consultants, Hacker und Forscher



Positives Firmenimage

Teilnehmende Partner dokumentieren verantwortungsbewussten Umgang mit IT-Sicherheit



Security Development Lifecycle

Partner können Schwachstelleninformationen in Planung, Entwicklung und Modellierung neuer Produkte berücksichtigen (“Security-by-Design”)



Advisory-Service

Unterstützung der Partner durch routinierte Security-Experten:

- koordinierte, abgestimmte Veröffentlichung
- Interaktion in deutscher und englischer Sprache
- Koordination mit anderen CERTs (z. B. ICS-CERT)



Austausch - Vernetzung - Hilfe

- Herstellerübergreifend, vertrauenswürdig und sicher (Security Experten)
- anonymisiert (auf Wunsch) und in gleicher Zeitzone
- gemeinsame Workshops und Best Practices

BECKHOFF

PHENIX CONTACT
INSPIRING INNOVATIONS

Miele

WAGO

PILZ
THE SPIRIT OF SAFETY

VDE
CERT



PEPPERL+FUCHS

HIMA
SMART SAFETY.

Weidmüller

EH
Endress+Hauser

BENDER

Vielen Dank für Ihre Aufmerksamkeit!

Web: <https://cert.vde.com>

Mail: info@cert.vde.com

Twitter: [@certvde](https://twitter.com/certvde)

Ihre Ansprechpartner:

Andreas Harner

Abteilungsleiter CERT@VDE

Tel. +49 69 6308-392

andreas.harner@cert.vde.com

