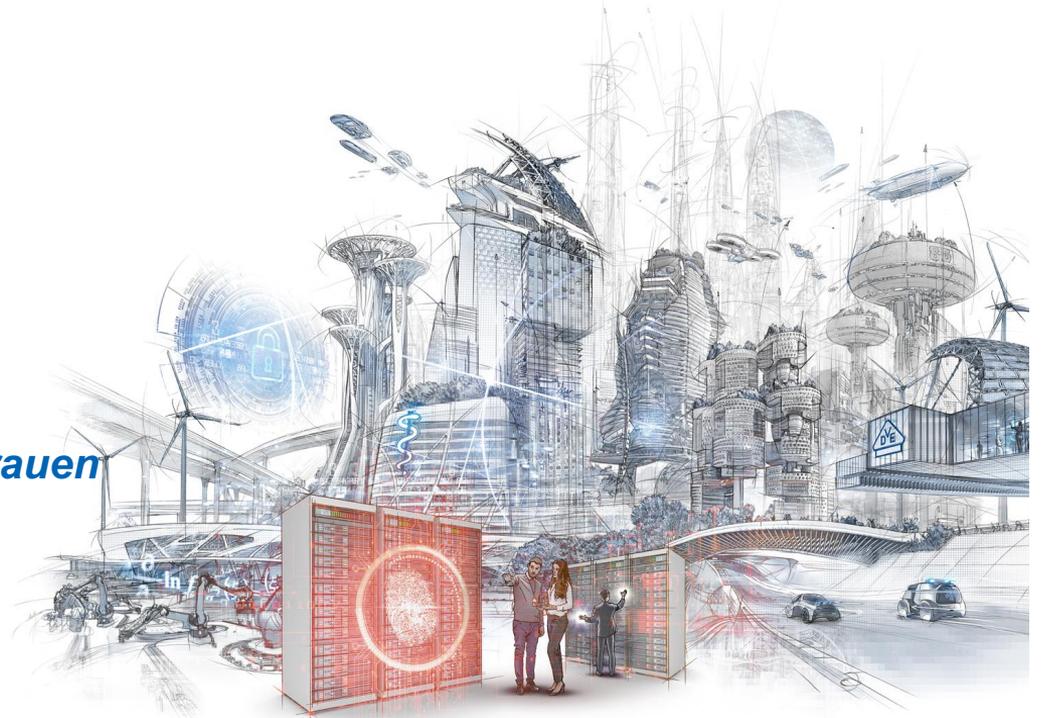


CERT@VDE- Professioneller Umgang mit OT-Sicherheitslücken schafft Vertrauen

Andreas Harner
Abteilungsleiter CERT@VDE



Web: <https://cert.vde.com>
Twitter: <https://twitter.com/certvde?lang=de>
Alert Feed: <https://cert.vde.com/de-de/media/feeds>
Advisory Feed: <https://cert.vde.com/de-de/advisories>

CERT-IFICATES?



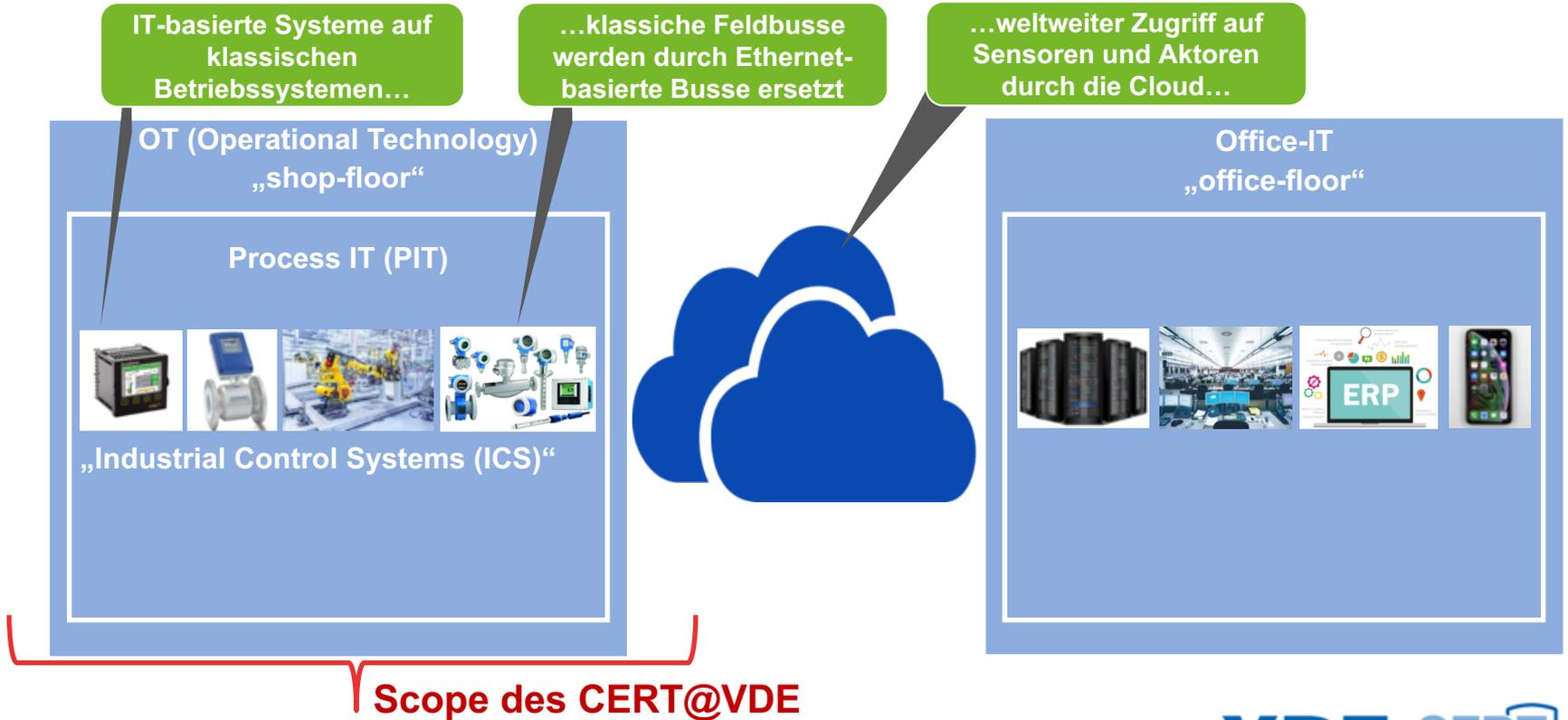
CERT-IFICATES?

NEIN!

Computer Emergency Response Team

- „**Computersicherheits-Ereignis- und Reaktionsteam**“
(aka *Computer Security Incident Response Team* (CSIRT))
- Gruppe von Cybersecurity Spezialisten...
- Kein CERT gleicht dem anderen! (Branche, firmenintern, Zielgruppe)
- **CERT@VDE** befasst sich mit **Produkten** seiner Zielgruppe: **PSIRT**
(*Product Security Incident Response Team*)
 - Herausgabe von Warnungen vor Sicherheitslücken in Produkten
 - Koordinator
 - Herausgabe von Lösungsansätzen (engl.: „advisories“)
 - Prävention durch Information

Industrie 4.0 / Smart Grid: Wirkungsbereich des CERT@VDE



Warum wurde CERT@VDE seitens der Industrie initiiert, 2017?



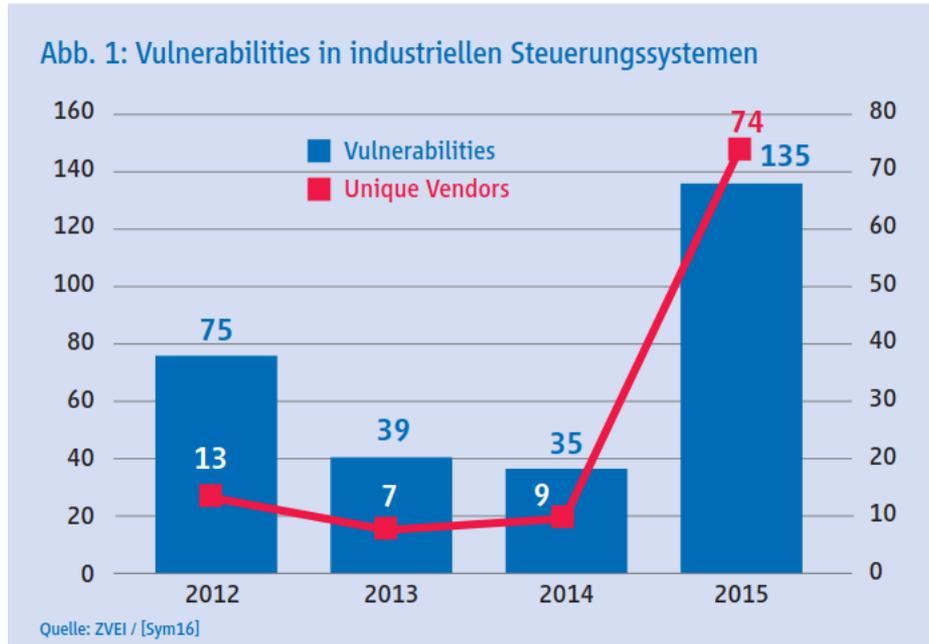
KEINER KÜMMERT SICH IN DEUTSCHLAND & EUROPA...

es fehlen:

Information (Know-How), Austausch, Unterstützung, Vernetzung, Routine,

Schwachstellenmanagement: Ein paar Zahlen...

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



Quelle: ZVEI: Orientierungsleitfaden für Hersteller zur IEC 62443

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

→ Es werden mehr Schwachstellen gefunden..
von Kunden, Konkurrenten, ...

Schwachstellenmanagement: Ein paar Zahlen...



Anforderung: Umgang mit Schwachstellen

- **IT-Grundschutz:**

IND.1.A12 Etablieren eines Schwachstellen-Managements

[...] Grundlage dafür SOLLTEN Schwachstellenmeldungen (Advisories) von Herstellern [...] sein. [...]

- **ISO 27002:**

Informationen über technische Schwachstellen von verwendeten Informationssystemen sollten rechtzeitig eingeholt, [...] bewertet und angemessene Maßnahmen [...] ergriffen werden.

- **IEC 62443-2-1:**

4.2.3.14 Maintain vulnerability

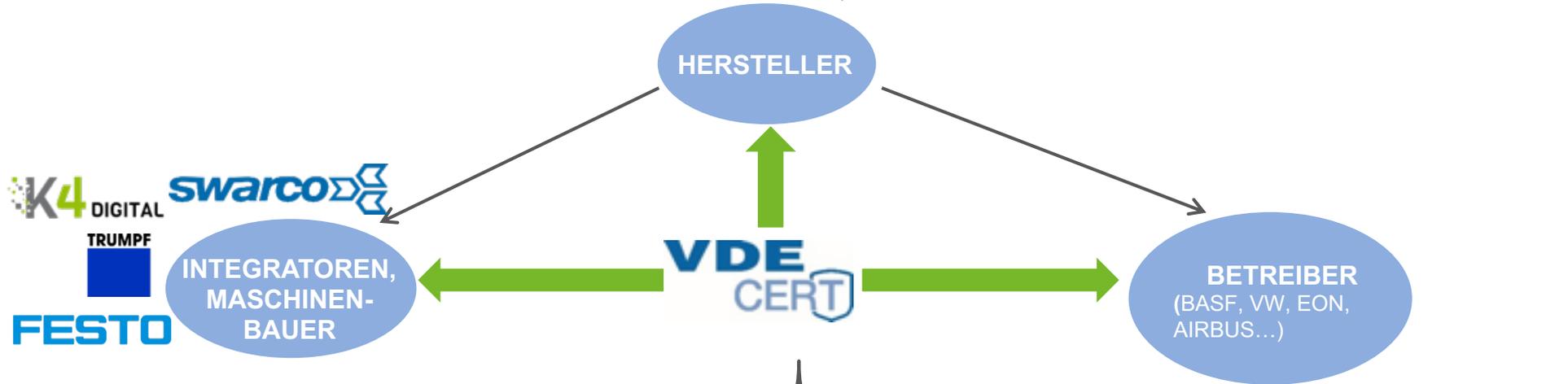
assessment records

Up-to-date vulnerability assessment records should be maintained for all assets comprising the IACS.

- **IEC 62443-4-1:**

DM-1: Empfang von Meldungen über sicherheitsbezogene Probleme

CERT@VDE: koordinierendes Produkt-CERT (PSIRT)





Frühwarnsystem durch Wissensvorsprung

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



- CERT ist „gnadenloses Informationsmanagement“!
- CERT ist „Krisenstab“ und nicht die „Eingreiftruppe“!
- Unterstützt „organisationales Lernen“

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)



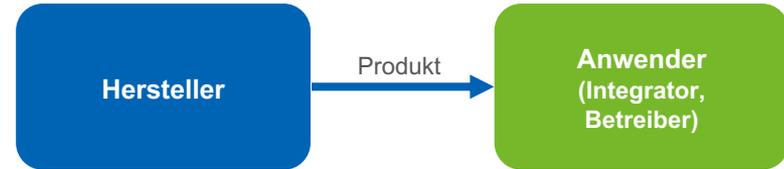
Austausch - Vernetzung - Hilfe

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



Motivation für CERT@VDE: Beziehung Hersteller - Kunde

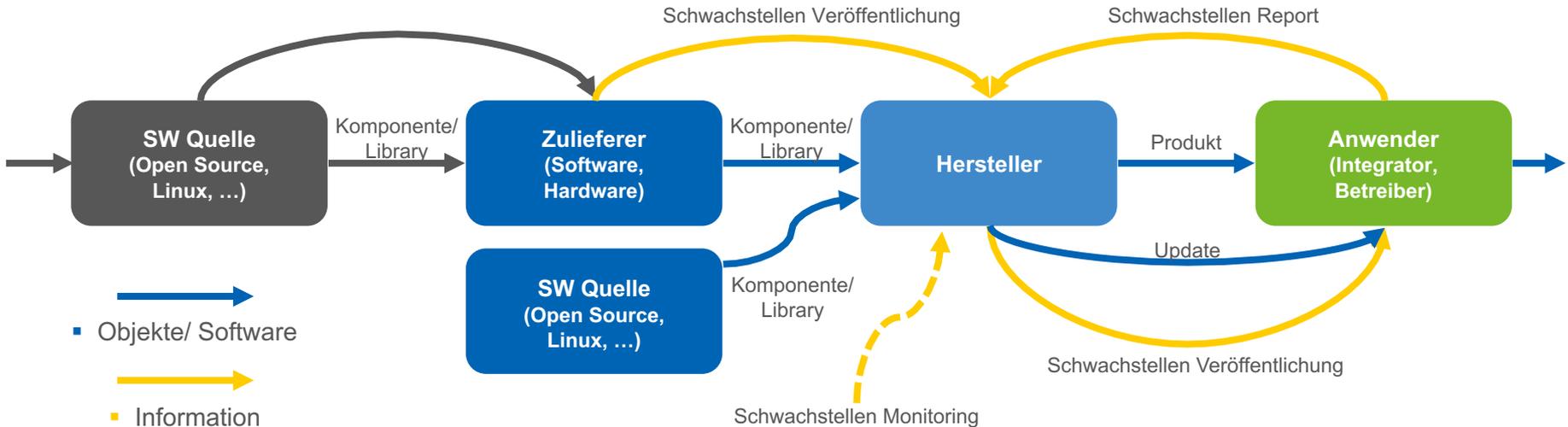
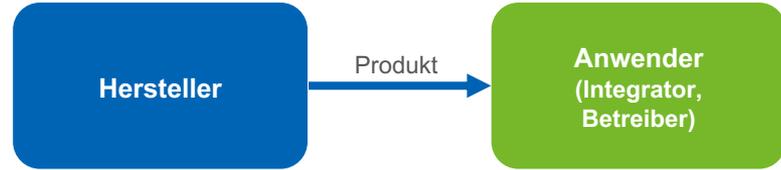
Traditionell → Einbahnstraße“



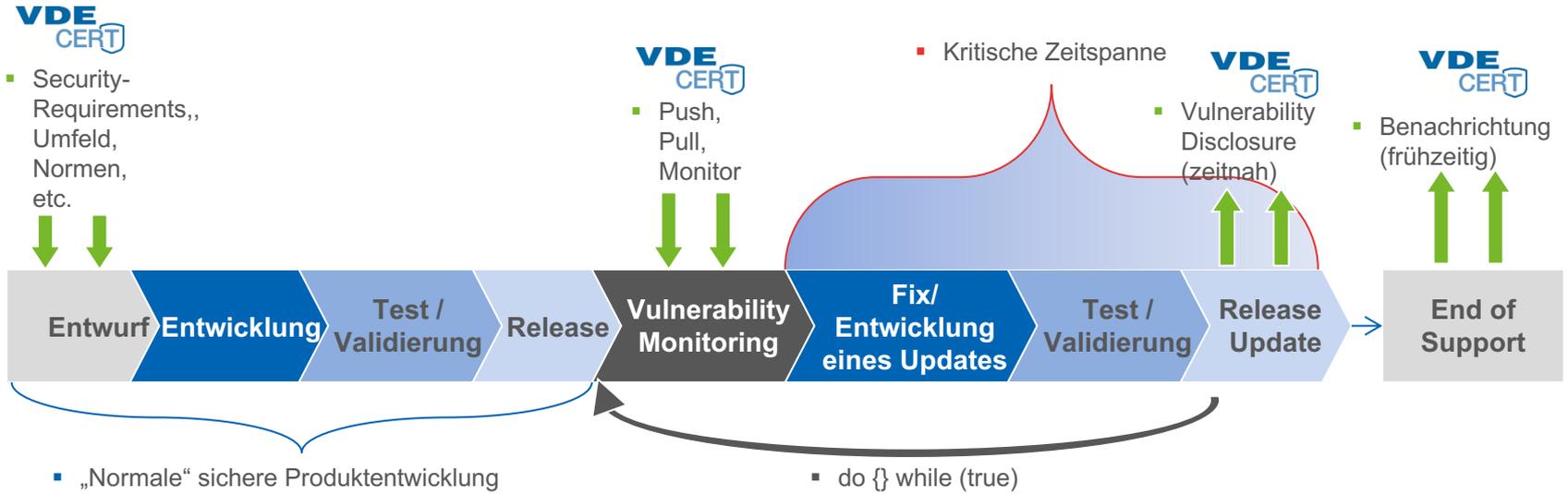
Motivation für CERT@VDE: Beziehung Hersteller - Kunde

Traditionell → Einbahnstraße

Heute → Netzwerk

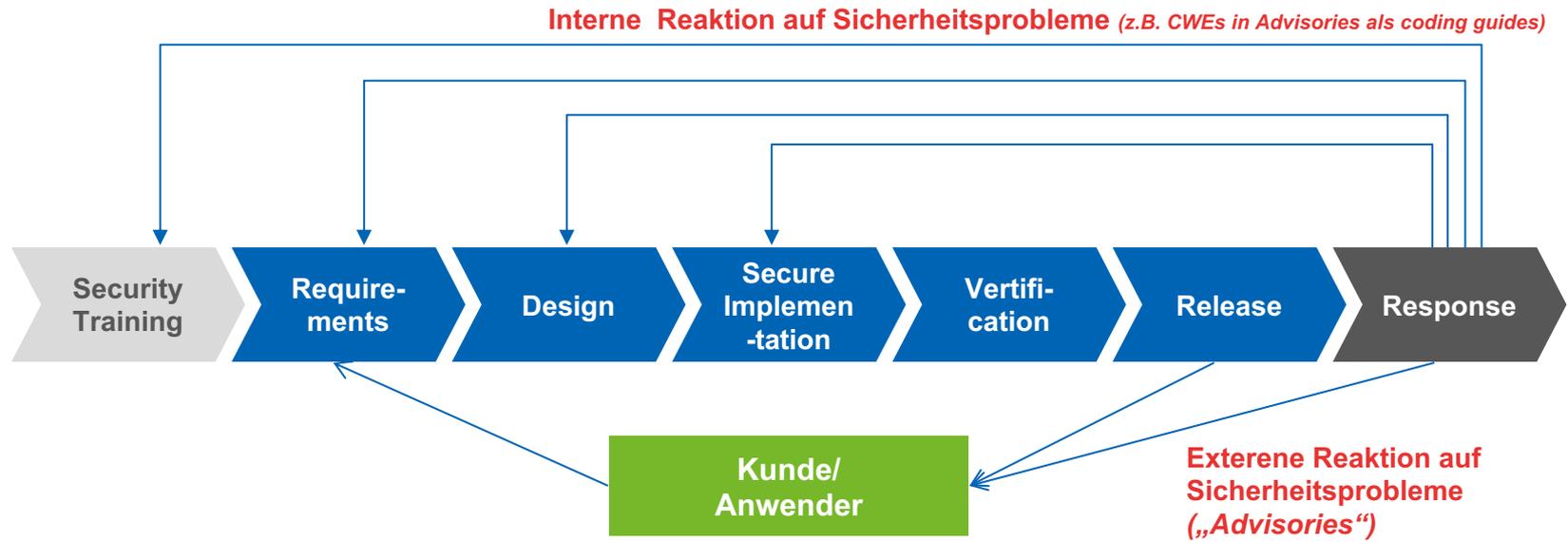


Produktlebenszyklus...und wo das CERT@VDE hilft



Fragestellungen & Herausforderungen

- Was muss der Gerätehersteller intern tun, um sichere Software zu erzeugen?
- Wie muss der Gerätehersteller mit seinen Kunden und Zulieferern interagieren?



Vernetzung: (inter)national



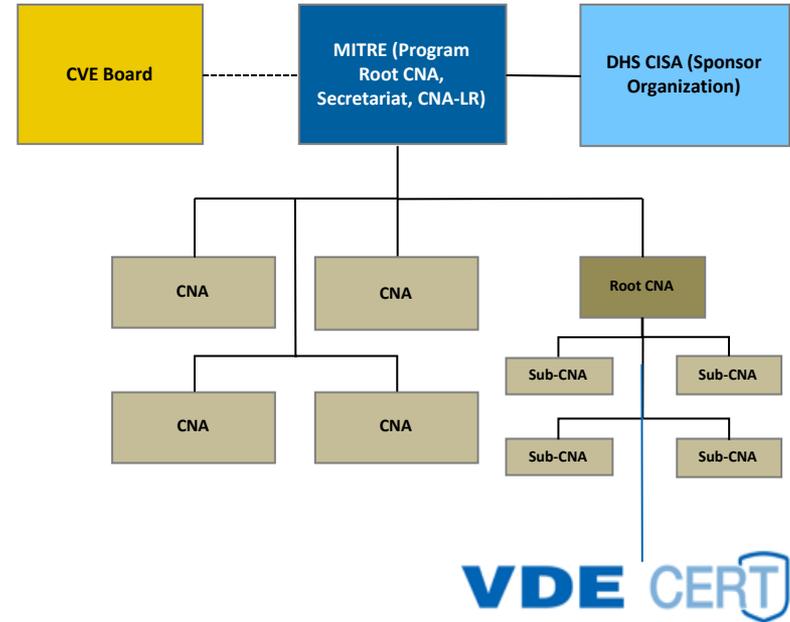
CERT@VDE ist anerkannte “CVE Numbering Authority (CNA)“: Vergabe von CVE Nummern!

Vorteile

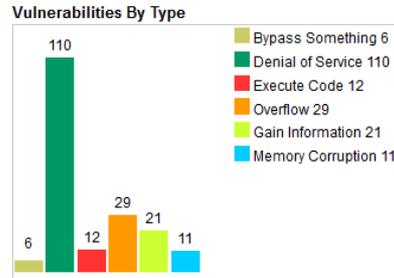
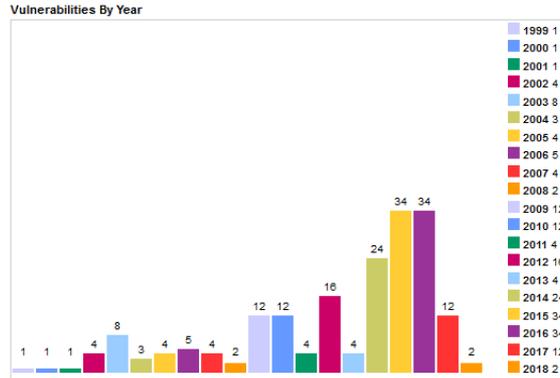
- Kontrolle des kompletten CVE-Veröffentlichungsprozess aus dem Scope des CERT@VDE
- **Kein Teilen von Embargoinformationen mit anderer CNA notwendig!**
- Beschleunigter Vulnerability Disclosure Prozess

Voraussetzung:

- Öffentlich zugängliche Disclosure Policy
- Positives Durchlaufen des CNA Anerkennungsprozesses bei MITRE
- Anerkennung und Beherrschen der CNA Regularien und Prozesse



Schwachstellen Monitoring: Frühwarnsystem des CERT@VDE



- Verwendete Software Komponenten können Schwachstellen enthalten
 - **Push-Verfahren:**
der Hersteller einer Softwarekomponente/Library informiert den Gerätehersteller (Anwender) direkt. (Aktive Beziehung notwendig!)

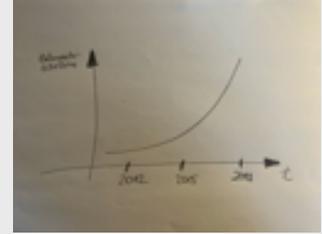
→ **Pull Verfahren:**
der **Gerätehersteller** informiert sich eigenständig über Schwachstellen in von ihm verwendeten Softwarekomponenten/Libraries...

Aber wo????

Quelle: https://www.cvedetails.com/product/383/Openssl-Openssl.html?vendor_id=217...

Resümee

- Sicherheit wird „nicht weggehen“
- Sicherheit ist nicht nur **Produkt/Technik, sondern viel Prozess**
- **Negativ:** Es ist Arbeit und berührt alle Bereiche eines Unternehmens, aber
- **Positiv:** Jeder kann es umsetzen..
 - Teile der Arbeiten können/müssen **automatisiert** werden
 - man muss **nicht alles selbst** tun: CERT@VDE
- Risikominimierung nur durch eine durchgängige Sicherheitskette möglich:
 - erfordert **klare Kommunikation, nachvollziehbare Prozesse und Austausch (Community)**
 - **man braucht ein CERT!**
- **Offener Umgang (d.h. Schwachstellen veröffentlichen)** mit dem Thema Sicherheit ist essentiell und heißt:
 - „vertrauenswürdige Firma...hat Prozesse im Griff!“
 - „ Melder ist keine Bedrohung“



Vielen Dank für Ihre Aufmerksamkeit!

Ihr Ansprechpartner:

Andreas Harner

Leiter CERT@VDE

Tel. +49 69 6308-392

andreas.harner@cert.vde.com

