Effektive Risikominimierung für Betreiber, Integratoren und Hersteller durch CERT@VDE

Andreas Harner
Leiter 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

VDE CERT

CERT: Computer Emergency Response Team

- group von cybersecurity experts… for emergency & prevention

- ***Netze, Rechner, Anwendungen:*** *Computer Security Incident Response Team* ***(CSIRT)***
- ***Produkte:*** *Product Security Incident Response Team (****PSIRT)***

- ***CERT@VDE*** *befasst sich mit* ***Produkten der Automatisierung („OT“)*** *(koordinierendes PSIRT):*
  - → Koordinator
  - → Herausgabe von Warnungen vor Sicherheitslücken in Produkten und von Lösungsansätzen (engl.: „advisories“)
  - → Prävention durch Information *(“Schwachstellen-Informationsservice“)*

Industrie 4.0/Smart Grid/Smart Traffic/Smart Water….

IT-basierte Systeme auf klassischen Betriebssystemen…

…klassiche Feldbusse werden durch Ethernet-basierte Busse ersetzt

…weltweiter Zugriff auf Sensoren und Aktoren durch die Cloud…

OT (Operational Technology)
„shop-floor“

Process IT (PIT)

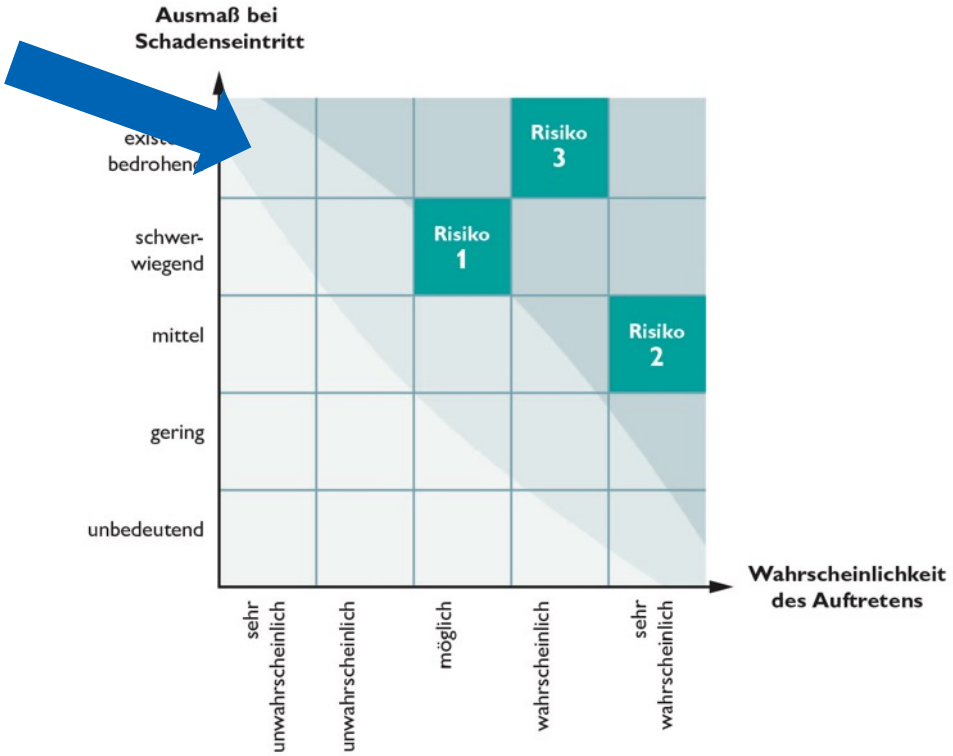
„Industrial Control Systems (ICS)“

Office-IT
„office-floor“

Scope des CERT@VDE

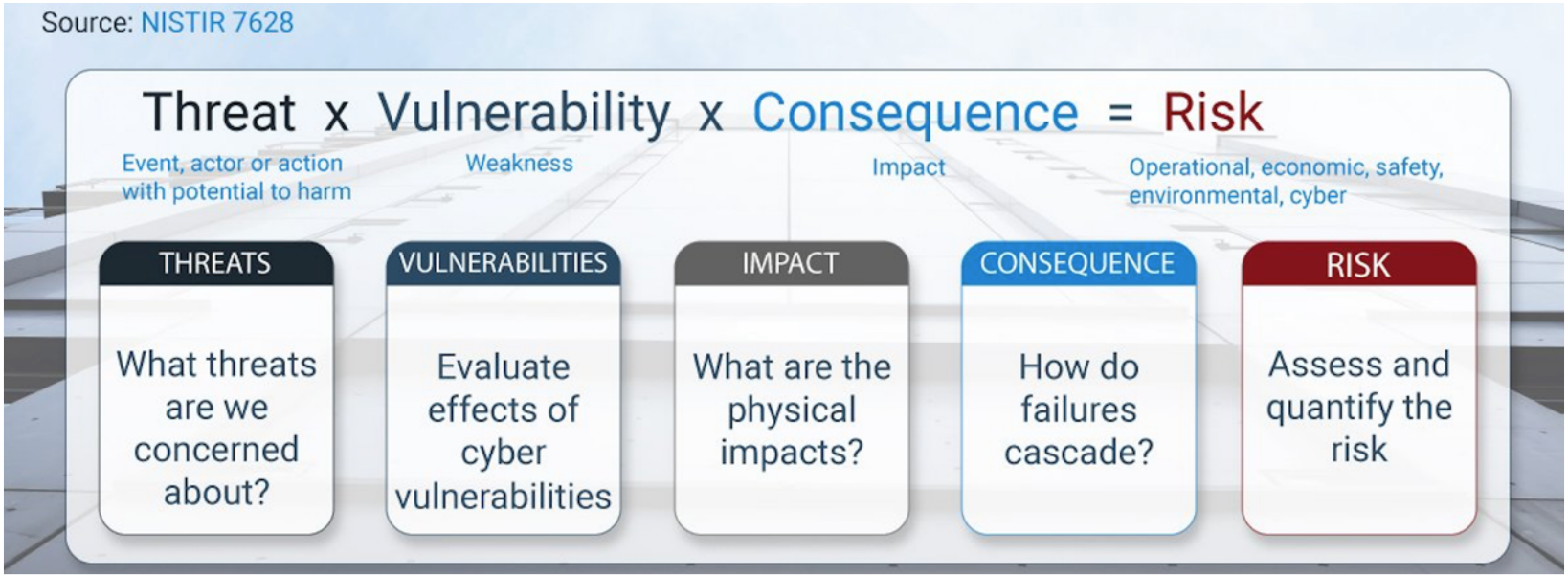
VDE CERT

Angriffsziel OT: Herausforderung Risikobewertung




jeder Lieferant,
jede Automatisierungskomponente
jeder Mensch
…stellt ein mögliches Risiko dar.
Die Verantwortung geht damit auch auf
jeden Lieferanten über!!!

Gleiche Grundprobleme: Wie „berechne“ ich mein Risiko?

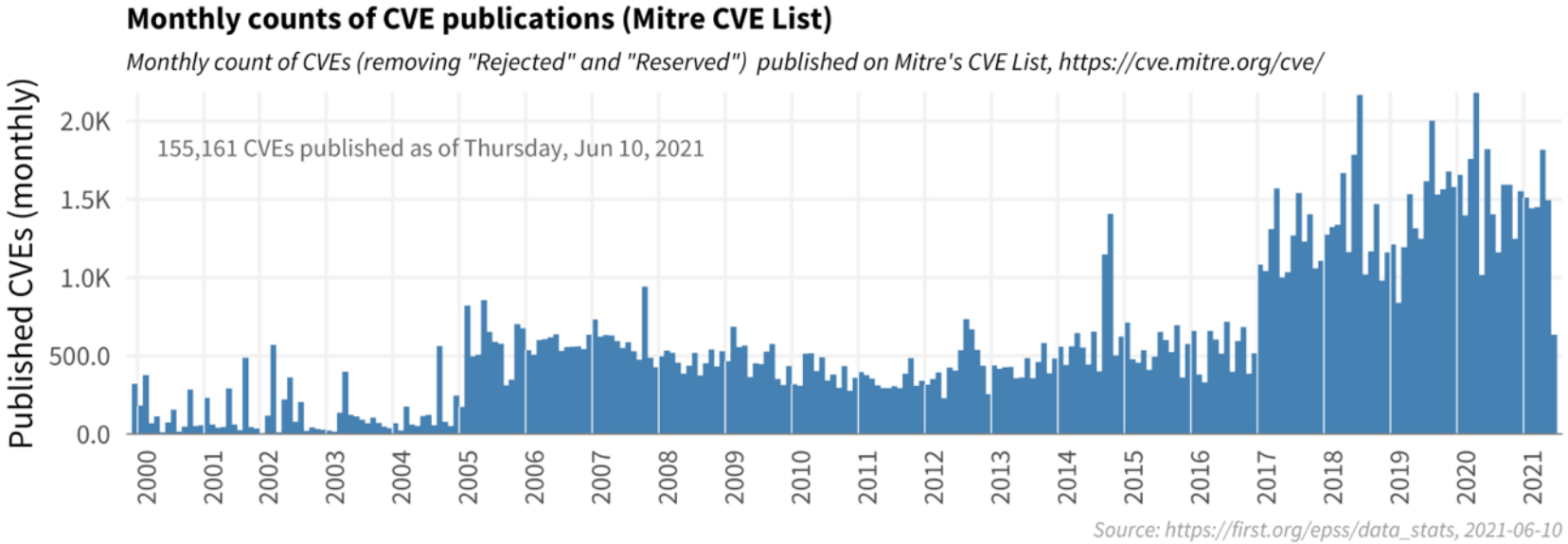


Warum wurde CERT@VDE seitens der Industrie initiiert?

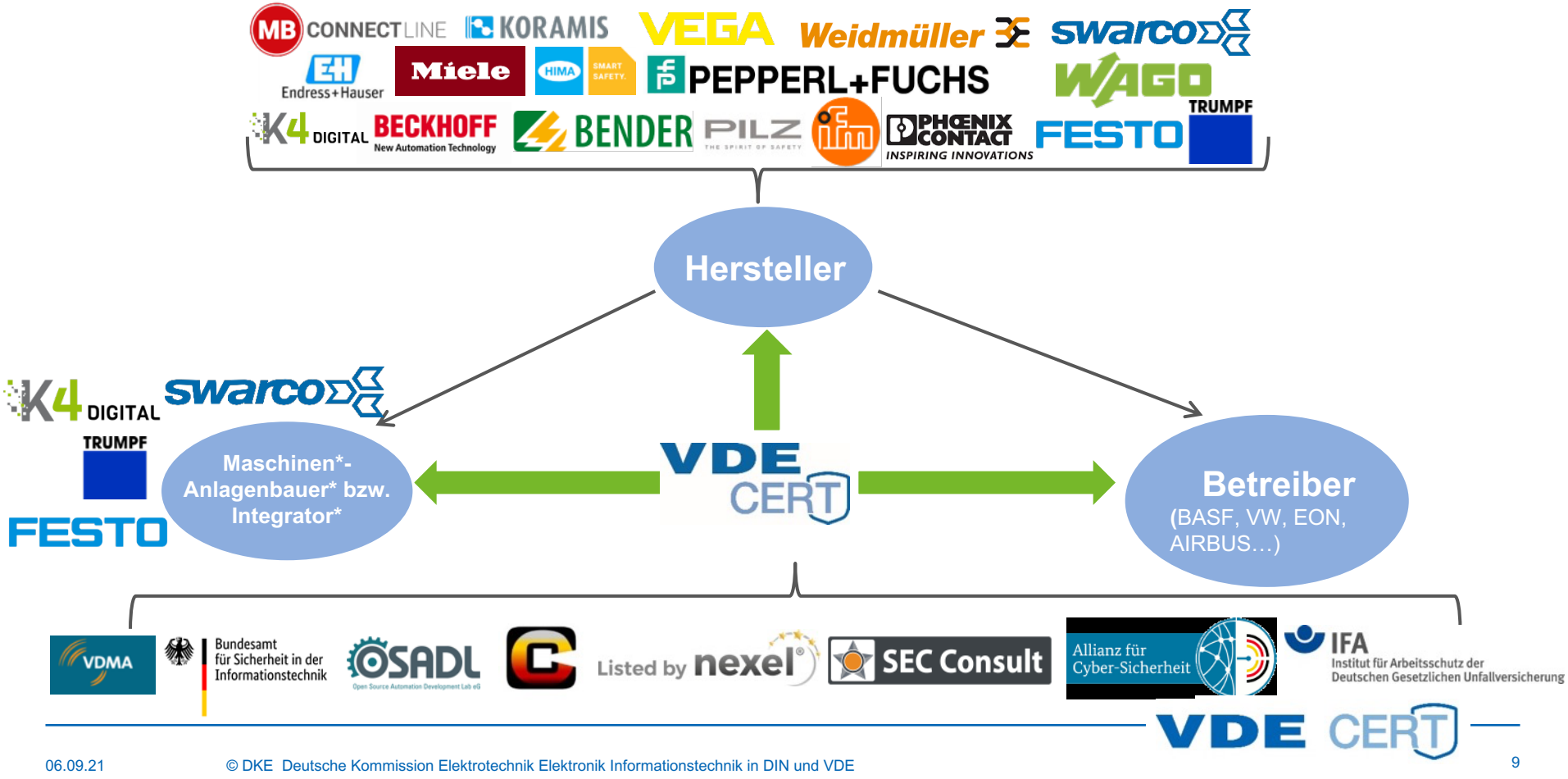
KEINER KÜMMERT SICH IN DEUTSCHLAND & EUROPA…
es fehlen:
Information (Know-How), Austausch, Unterstützung, Vernetzung, Routine, ….

Schwachstellen: Ein paar Zahlen…

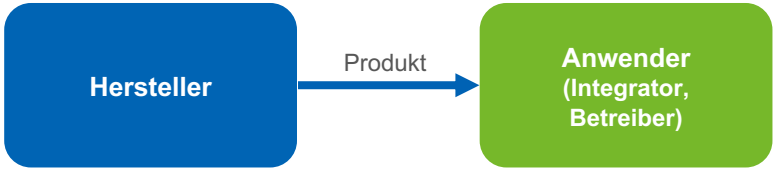
„Behauptung: „Die Anzahl von Schwachstellen steigt kontinuierlich an?“



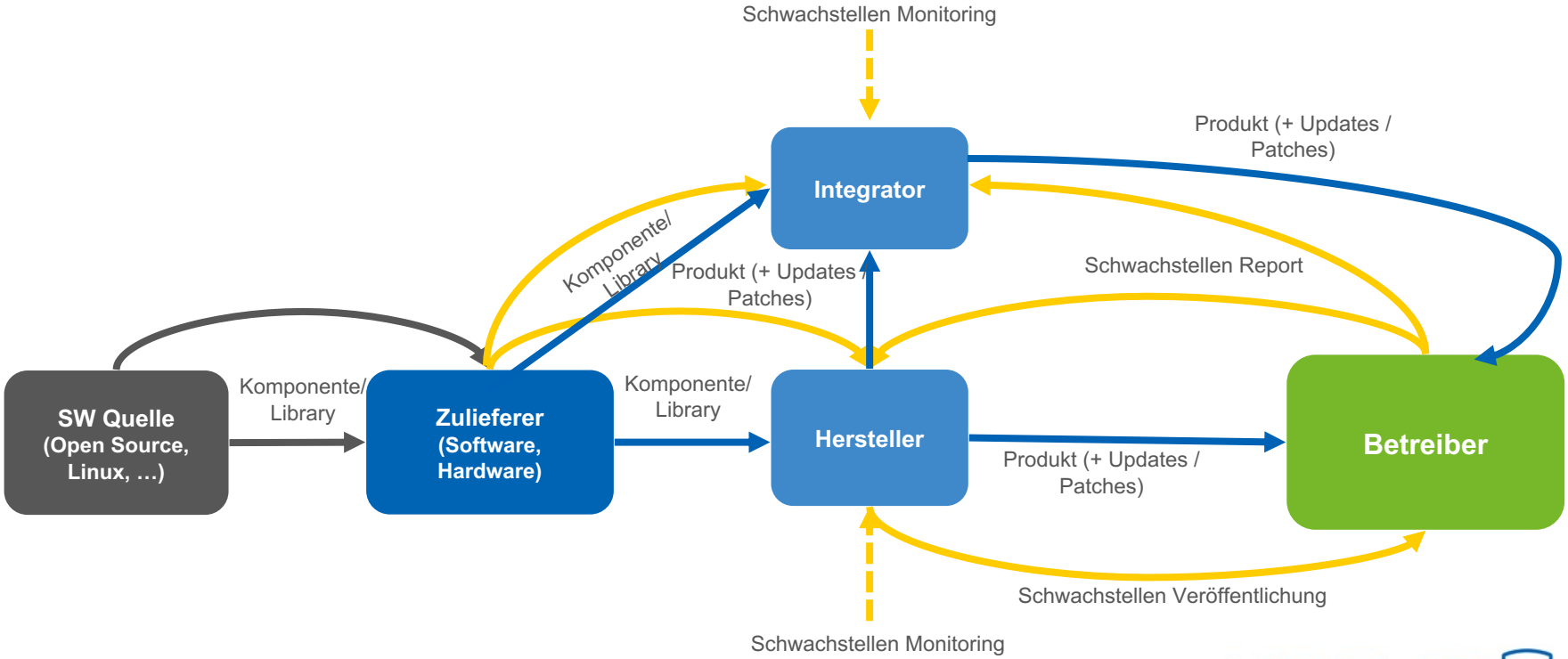
CERT@VDE: Netzwerk für Lösungen



Gleiche Grundprobleme…
Beziehung Hersteller – Betreiber:
Traditionell → „Einbahnstraße“



Gleiche Grundprobleme…
Beziehung Hersteller – Betreiber: heute „Netzwerk“



Bewerten von Schwachstellen: Betreiber können helfen…

Eigene Betroffenheit

- Produkt und Version im Einsatz?
- Was ist mit Komponenten von Drittanbietern?

Auswirkungen auf lokale Umgebung

- Kann die Schwachstelle in der lokalen Umgebung ausgenutzt werden?
- Was sind die Auswirkungen?
- Gibt es „Nebenwirkungen“?

Ableitung der Dringlichkeit

- Müssen Maßnahmen ergriffen werden?
- Wenn ja, welche und wann?
- Was ist mit Exploit-Chains?

Risikominimierung durch Schwachstellenbehandlung: Bedarf an Unterstützung durch CERT@VDE

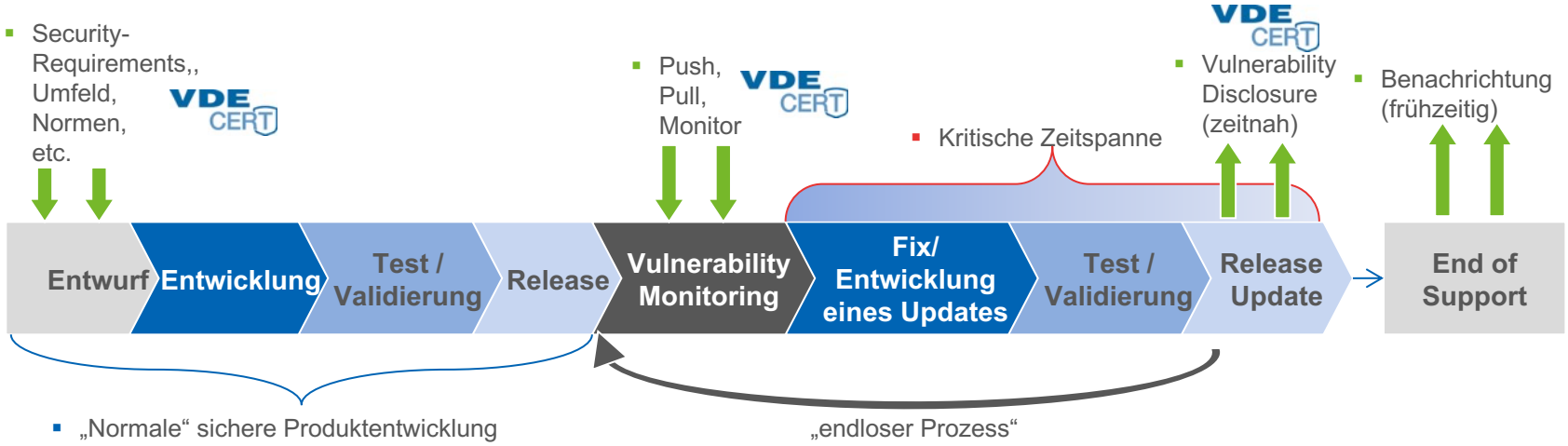
Aufgaben Unternehmen

- Interne Koordination der Problembehandlung
- Fehleranalyse mit CERT@VDE
- Fehlerbehebung
- Einbindung der Zulieferer
- Bereitstellung Patch/Workaround
- Bereitstellung Advisory & Abstimmung mit CERT@VDE
- Integration und Überwachung von Vulnerability-Feeds des CERT@VDE

Aufgaben CERT@VDE

- Meldungen zu Schwachstellen entgegennehmen
- Koordination & Kommunikation mit externem Melder
- Schwachstellen bewerten und beheben (“CVSS“)
- Koordination mit anderen CERTs & Behörden
- CVE Vergabe und Schnittstelle in das „Trusted Introducer Netzwerk“
- Begleitung und Support im Prozess & Review
- Abgestimmte Veröffentlichung und Verbreitung
- Kunden der Partner erreichen
- Lessons learned & Best Practices Frühwarnung durch Bereitstellung von Vulnerability Feeds
- Zulieferkomponenten der Partner beobachten
- Kunden der Partner erreichen

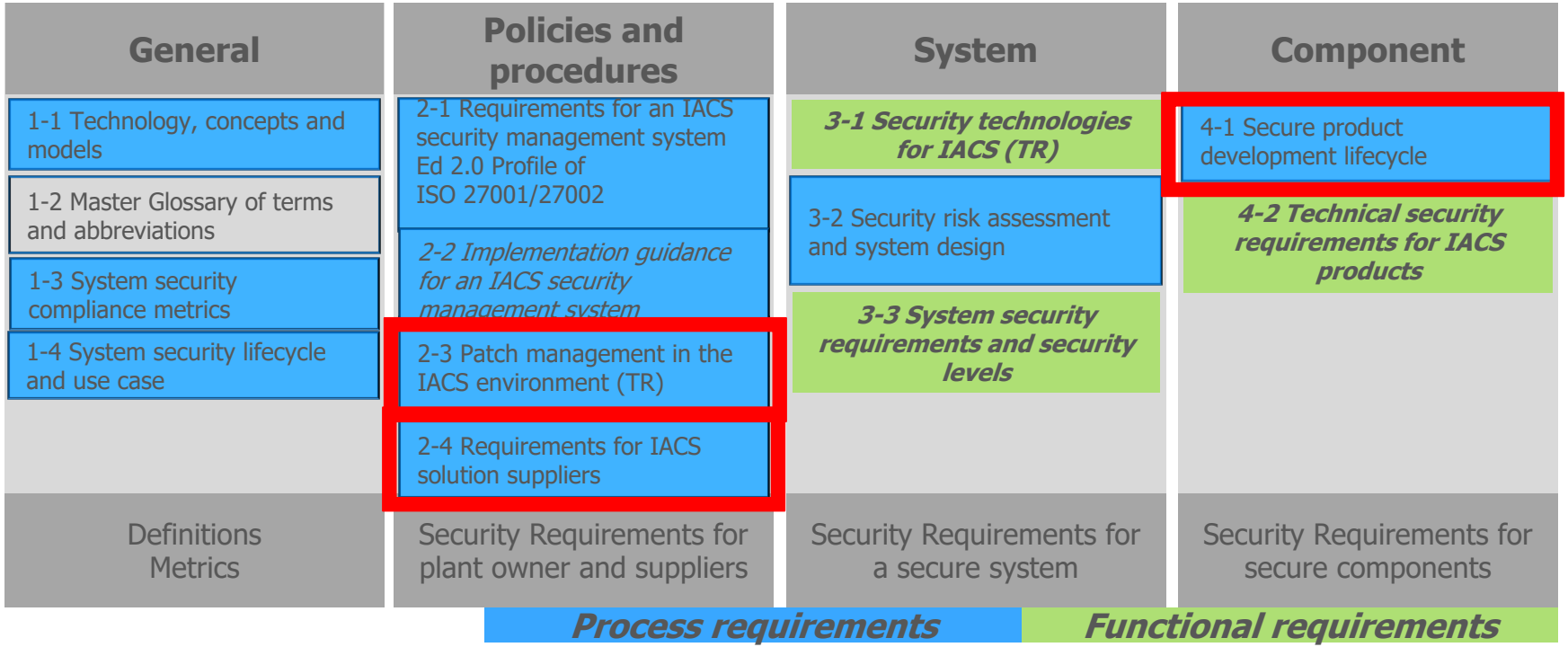
Produktlebenszyklus...und wo das CERT@VDE hilft



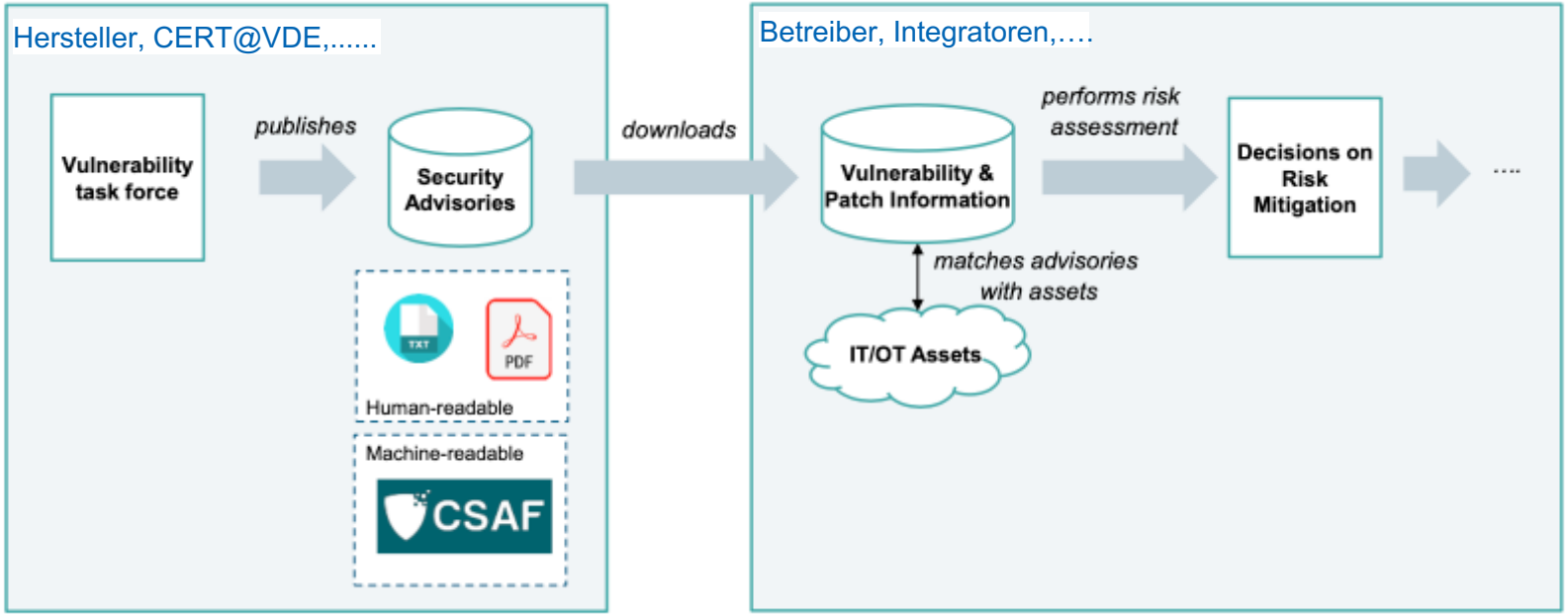
Skalierbarkeit: Bedarf an Unterstützung durch CERT@VDE

Roles / Phases	Finder	Reporter	Vendor	Coordinator	Deployer
Discovery	Finds vulnerabilities				
Reporting	Prepares report	Reports vuls to vendor(s) and/or coordinators	Receives reports	Receives reports Acts as reporter proxy	
Validation and Triage			Validates reports received Prioritizes report for response	Validates reports received Prioritizes report for response	
Remediation		Confirms fix	Prepares patches Develops advice, workarounds	Coordinates multiparty response Develops advice, workarounds	
Public Awareness	Publishes report	Publishes report	Publishes report	Publishes report	Receives report
Deployment					Deploys fix or mitigation

IEC 62443: Normative Anforderungen

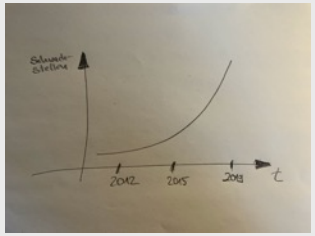


Betreiber-Hersteller: Zustand heute & was wird sich ändern?



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"

CERT@VDE – Synergien für mehr Sicherheit

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

Frühwarnsystem durch Wissensvorsprung

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

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")

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

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)

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

Austausch - Vernetzung - Hilfe

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

Vielen Dank für Ihre Aufmerksamkeit!

Wir gestalten die e-diale Zukunft.
Machen Sie mit.

Ihr Ansprechpartner:

Andreas Harner
Leiter CERT@VDE

Tel. +49 69 6308-392
andreas.harner@cert.vde.com

VDE CERT

Vertrauen durch Partnerschaften und Akkreditierung

- TI bietet als internationales Verzeichnis von Sicherheitsteams übersichtlich und aktuell akkurate Informationen für Teilnehmer
- **CERT@VDE ist akkreditiert** durch Trusted Introducer und unterwirft sich damit freiwillig den gemeinsam definierten Qualitätsstandards und Anforderungen (Akkreditierungszyklus: 1 Jahr)
- Die *European Network and Information Security Agency* **(ENISA)** der EU fördert diese Aktivitäten

→ **CERT@VDE ist Schnittstelle zum TI für seine Partner!**

Vertrauen durch Partnerschaften und Akkreditierung

- CERT@VDE ist Mitglied im **„Deutschen CERT Verbund (CV)“** und repräsentiert seine Kooperationspartner
- Der erprobte Aufnahmeprozess des CV garantiert Teams mit ähnlichen Fähigkeitsniveaus:

  → Damit ist ein **fachlicher Austausch auf Augenhöhe** möglich
  → Durch ein NDA wird die **Vertraulichkeit untereinander** zugesichert
  → Durch die **regelmäßigen Arbeitstreffen** wird das institutionelle Vertrauen aus dem Aufnahmeprozess zügig abgelöst durch ein **persönliches Vertrauen**

Vertrauen durch Partnerschaften und Akkreditierung

- CERT@VDE ist **Teilnehmer der "Allianz für Cybersicherheit (ACS)"**
- CERT@VDE besitzt den Sonderstatus „INSI" **(„Institutionen im besonderen staatlichen Interesse")**

→ **CERT@VDE erhält zusätzliche Angebote und einen erweiterten, vertraulichen Pool an Informationen**

→ CERT@VDE streut Informationen im Bedarfsfall über die ACS, wenn diese für sehr viele Anwender gerade in Hinblick auf Anlagen im häuslichen Bereich oder bei Mittelständlern relevant sind.