SOFTWARE-SCHWACHSTELLEN:

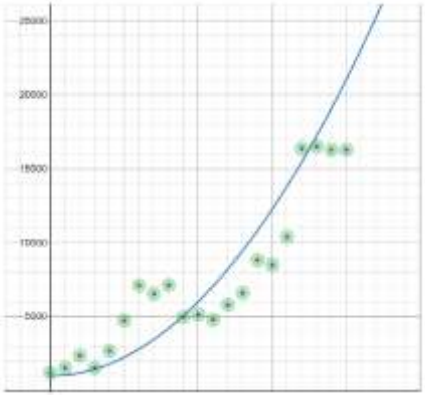
ZUKÜNFTIGE HERAUSFORDERUNGEN

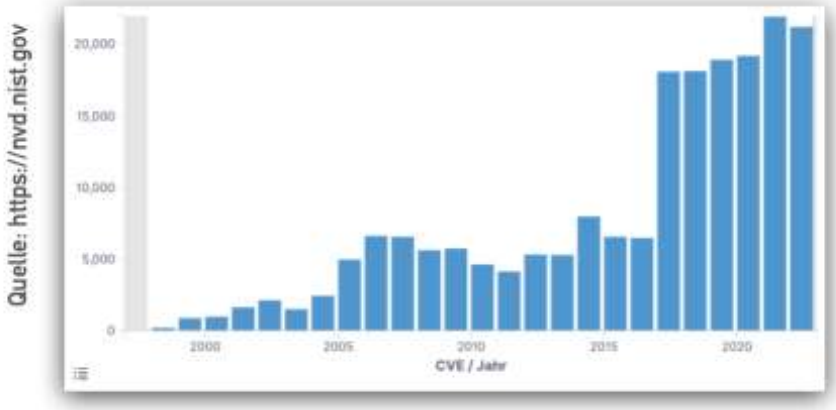
Andreas Harner
Abteilungsleiter CERT@VDE

Web: https://cert.vde.com
Twitter: https://twitter.com/certvde?lang=de

VDE CERT

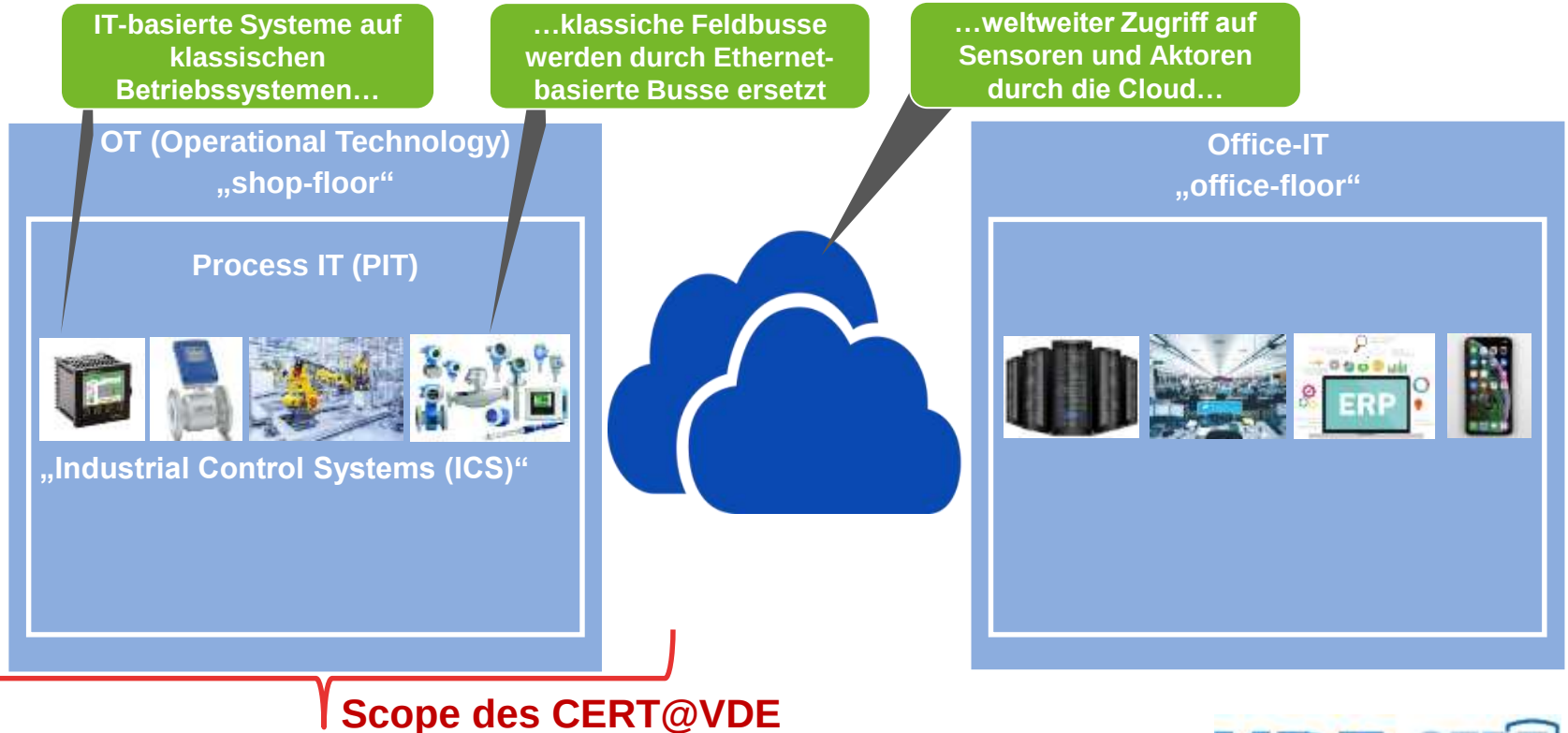
„….Die Anzahl von Schwachstellen steigt…“





https://opensourcesecurity.io/2021/03/30/its-time-to-fix-cve/

Industrie 4.0, Smart xxx…..



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 62443-4-1:** DM-1: Empfang von Meldungen über sicherheitsbezogene Probleme
- **IEC 81001-5-1** Secure Health SW Lifecycle Process
- **IEC 60601-4-5:** Medical electrical equipment –Part 4-5: Guidance and interpretation – Safety-related technical security specifications (referenziert auf IEC 62443)

IEC 62443: Anforderungen zum Umgang mit Schwachstellen

General	Policies & Procedures	System	Component
1-1 Concepts and models	2-1 Security program requirements for IACS asset owners	3-1 Security technologies for IACS	4-1 Secure product development lifecycle requirements
1-2 Master glossary of terms and abbreviations	2-2 IACS secuity program ratings	3-2 Security risk assessment and system design	4-2 Technical security requirments for IACS components
1-3 System security conformance metrics	2-3 Patch management in the IACS environment	3-3 System security requirements and security levels	
1-4 IACS security lifecycle and use-cases	2-4 Security program requirements for IACS service providers		
	2-5 Implementation guidance for IACS asset owners		

Published

Work in progress

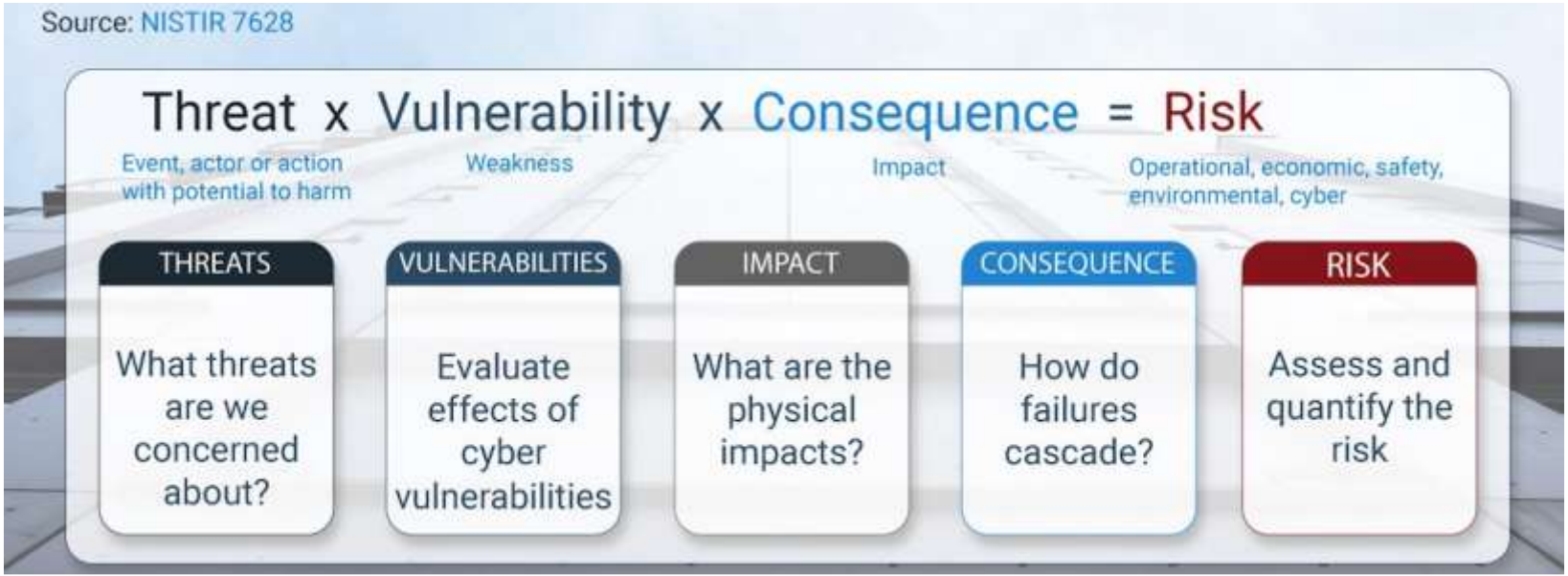
Gesetzliche Anforderungen: Umgang mit Schwachstellen

- **Heute:** bereits im deutschen Recht verankert

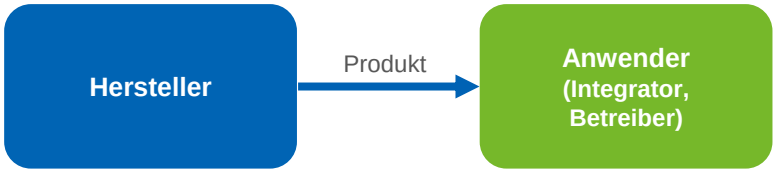
- **Zukünftig: EU-CRA**
  - CE-Kennzeichen für digitale Produkte,
  - Security-Anforderungen werden verpflichtend!
  - ohne dürfen die Produkte im EU-Binnenmarkt dann nicht mehr verkauft werden.

- **CRA: 3 Handlungsstränge:**
  - SBOMs
  - **Schwachstellen & CERTs**
  - Zertifizierung

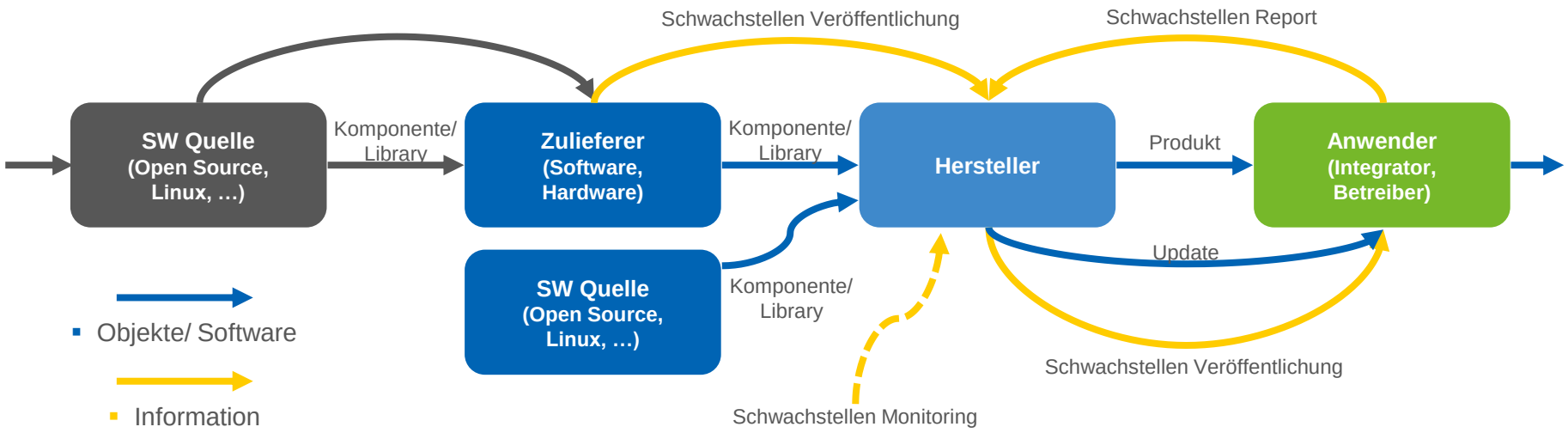
Schwachstellen veröffentlichen:
…damit mein Kunde sein Risiko kennt!



Beziehung Hersteller - Kunde → traditionell: „ Einbahnstraße“

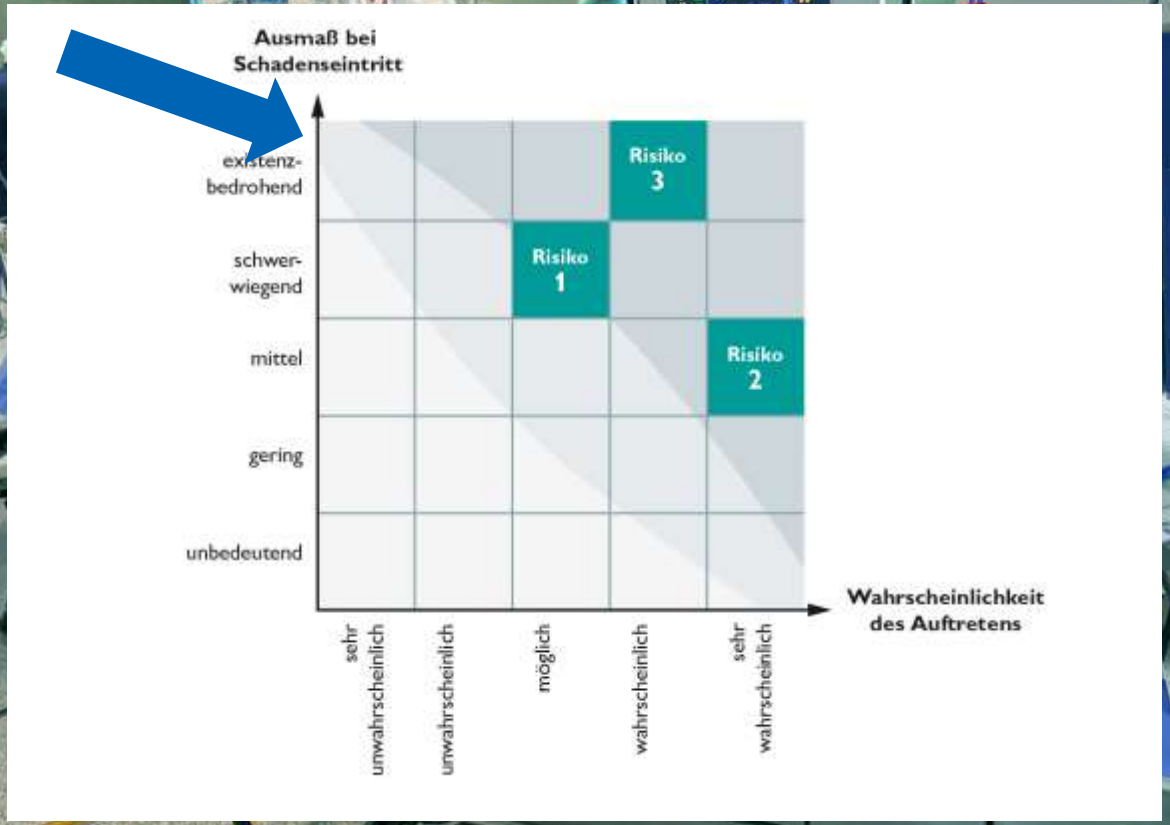


Beziehung Hersteller - Kunde → heute: Netzwerk



Angriffsziel OT: Herausforderung Risikobewertung

Angriffsziel „Krankenhaus-OT“: Herausforderung Risikobewertung

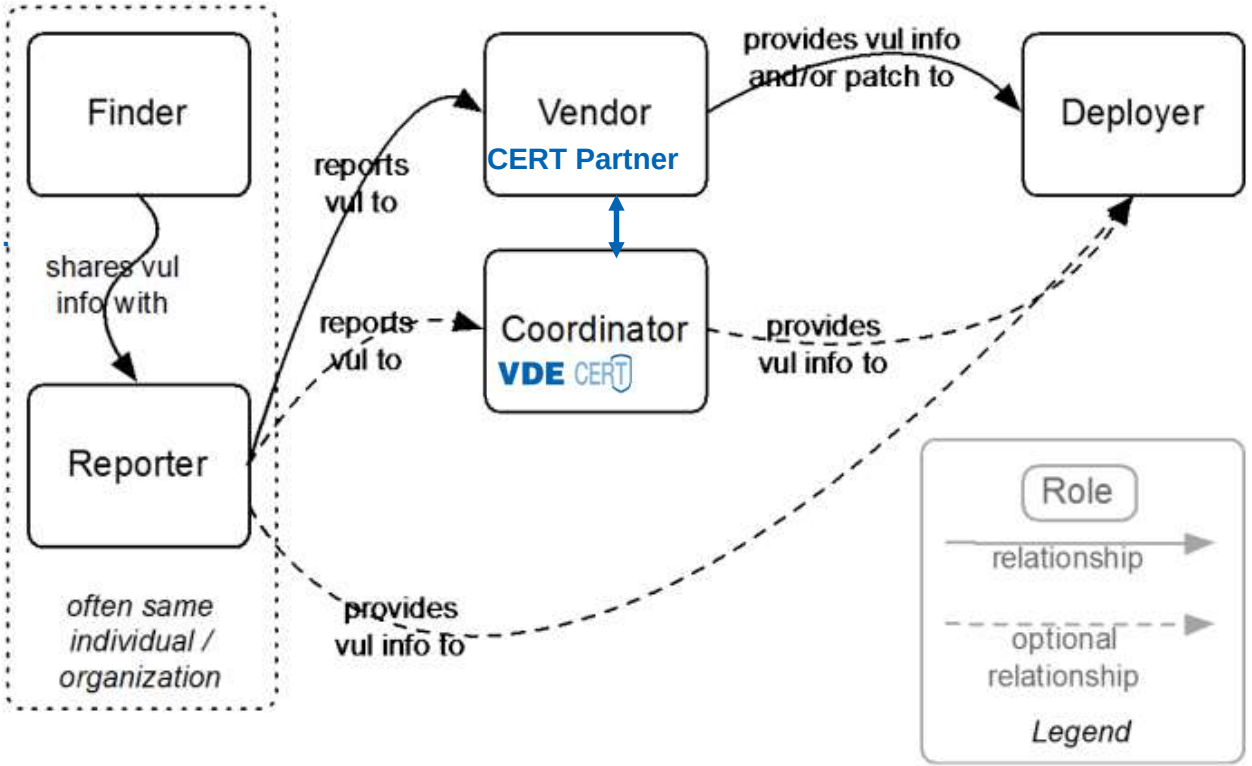



jeder Lieferant,
jede Automatisierungskomponente
jeder Mensch
…stellt ein mögliches Risiko dar.
Die Verantwortung geht damit auch auf
jeden Lieferanten über!!!

Coordinated Vulnerability Disclosure Prozess(CVD):

(Quelle: CMU)

Kunde,
Hacker,
Betreiber,
Forscher,
Hochschule
Konkurrenten…



Kunde, Betreiber, Anwender…

Coordinated Vulnerability Disclosure (CVD):

„Der CVD Prozess startet damit, dass mindestens eine Person Kenntnis von einer Schwachstelle in einem Produkt erlangt!“

→ **Sofortige Zweiteilung der Welt:**

Gruppe 1: …die, die von der Schwachstelle wissen

Gruppe 2: …die, die nix davon wissen

→ **Gruppe 1 muss sich mit folgenden 2 Fragen beschäftigen:**

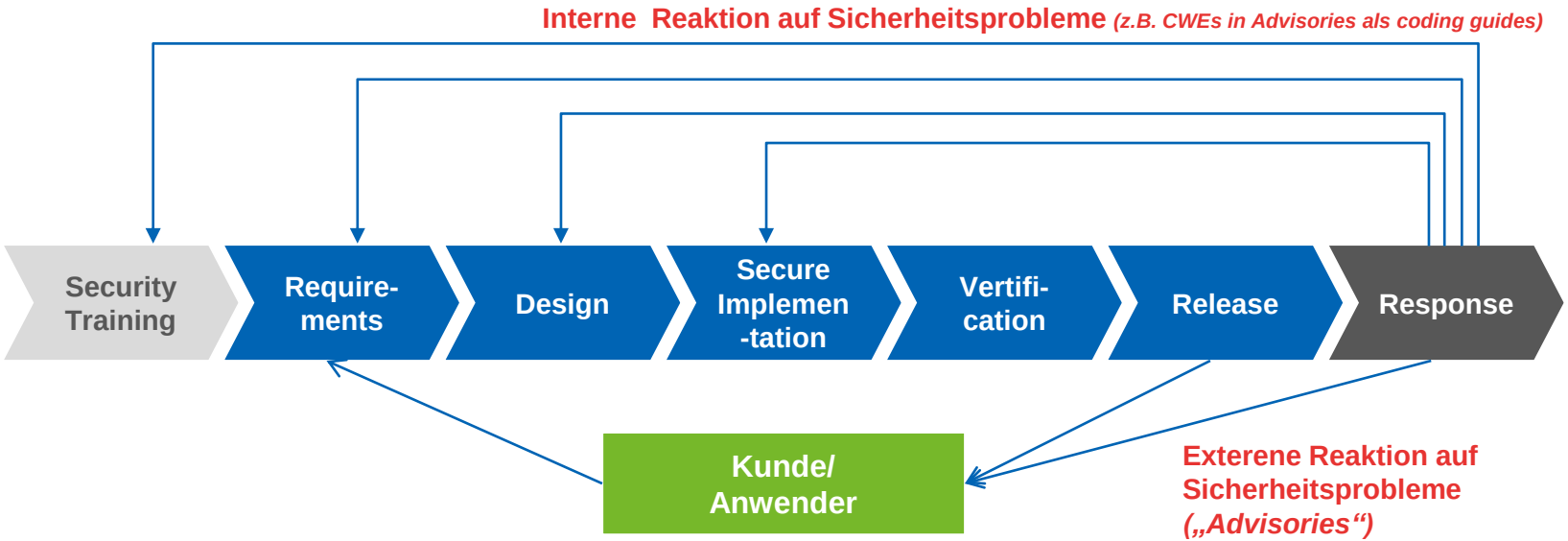
Was muss als Antwort auf die Schwachstelle getan werden? **„NICHTS“**

Wen muss man zusätzlich mit welcher Information versorgen? **„NIEMANDEN“**

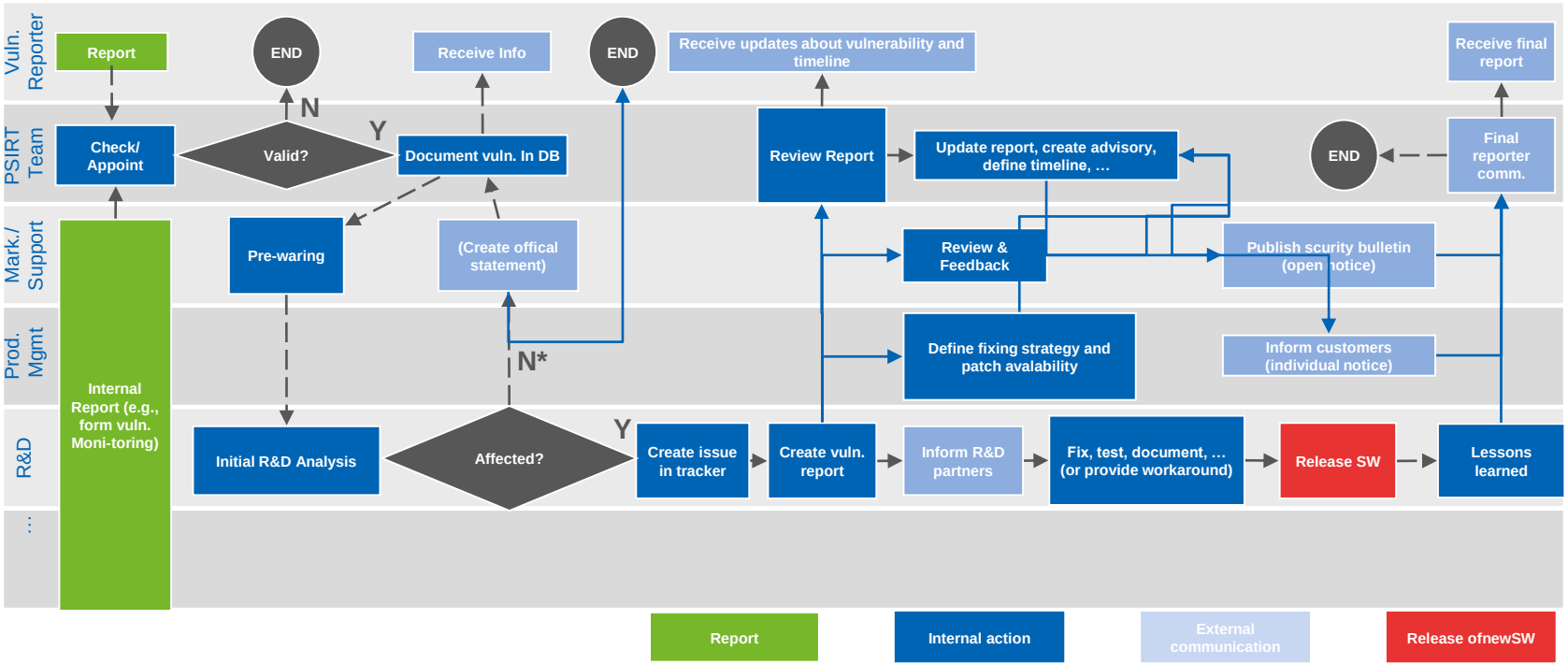
→ **CVD Prozess läuft, solange die beiden Antworten „NICHTS“ und „NIEMANDEN“ lautet!**

Interne und externe Reaktionen

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

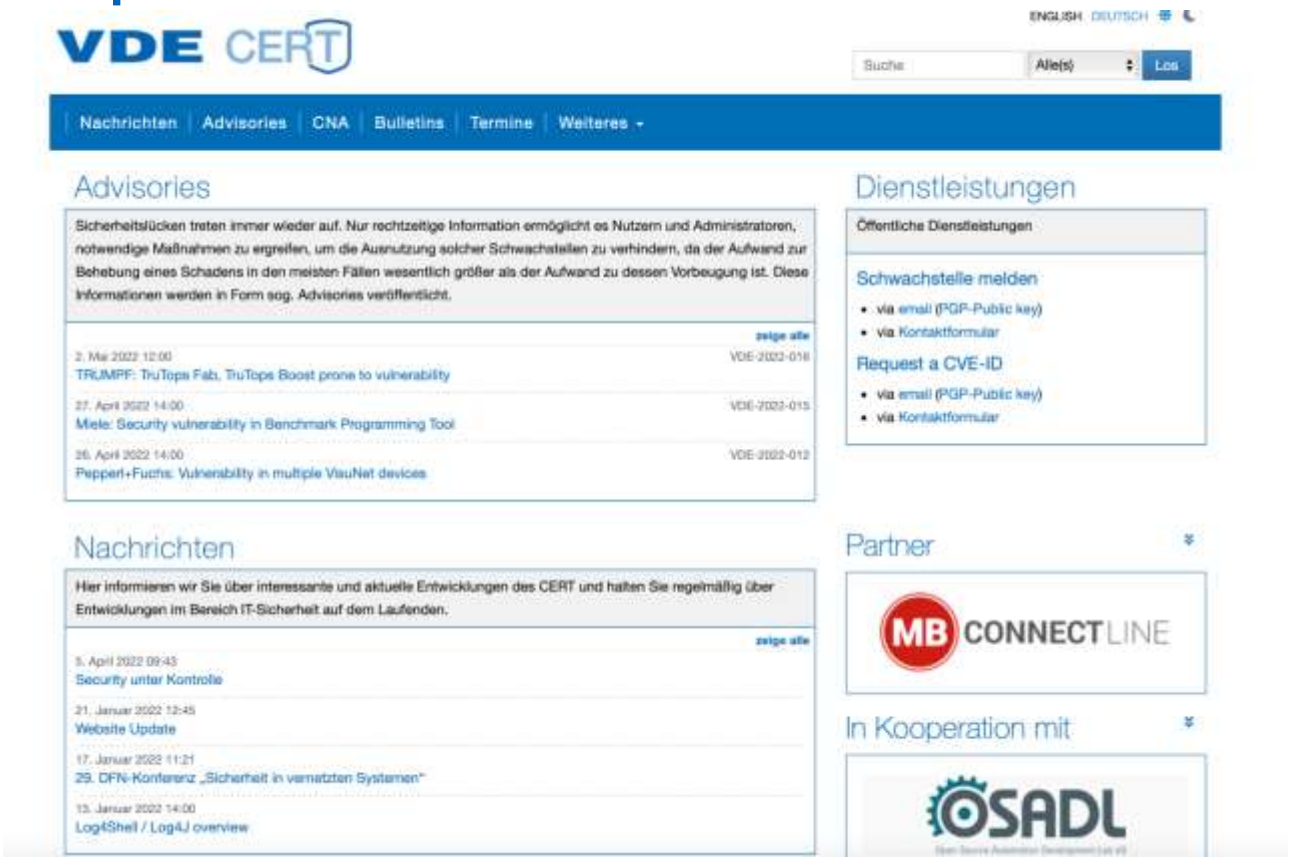


CERT@VDE – Response Process im kritischen Zeitfenster

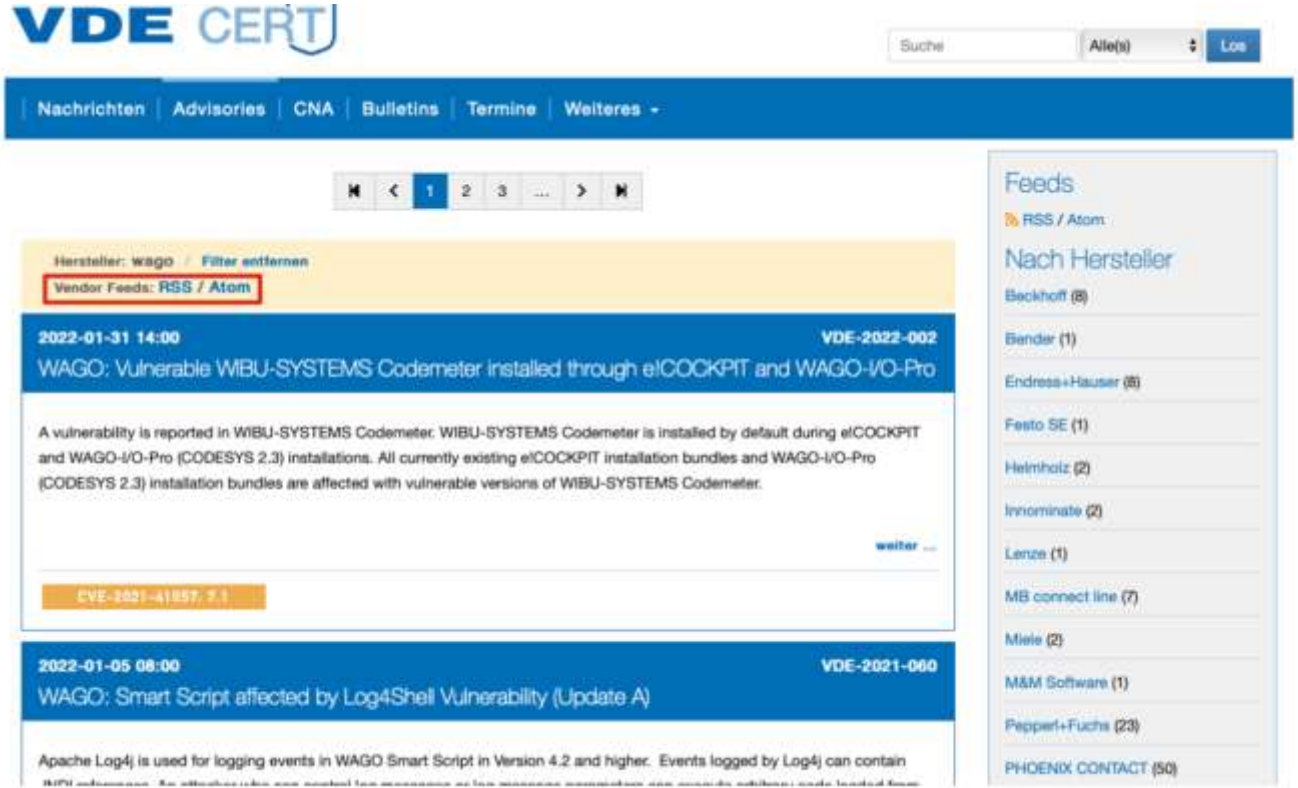


* Not affected or cannot be fixed (accepted)

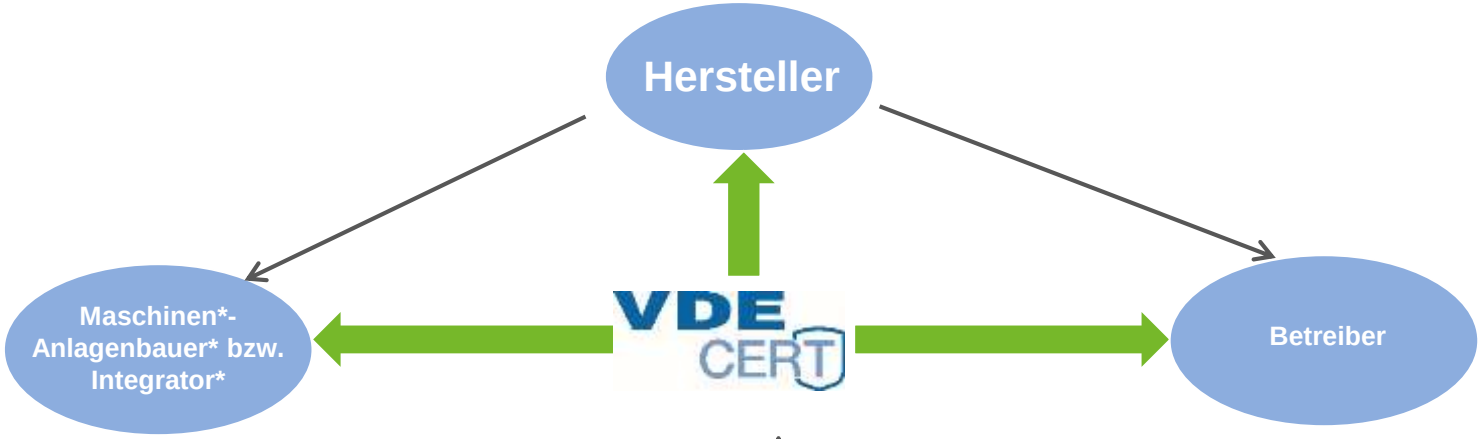
https://cert.vde.com



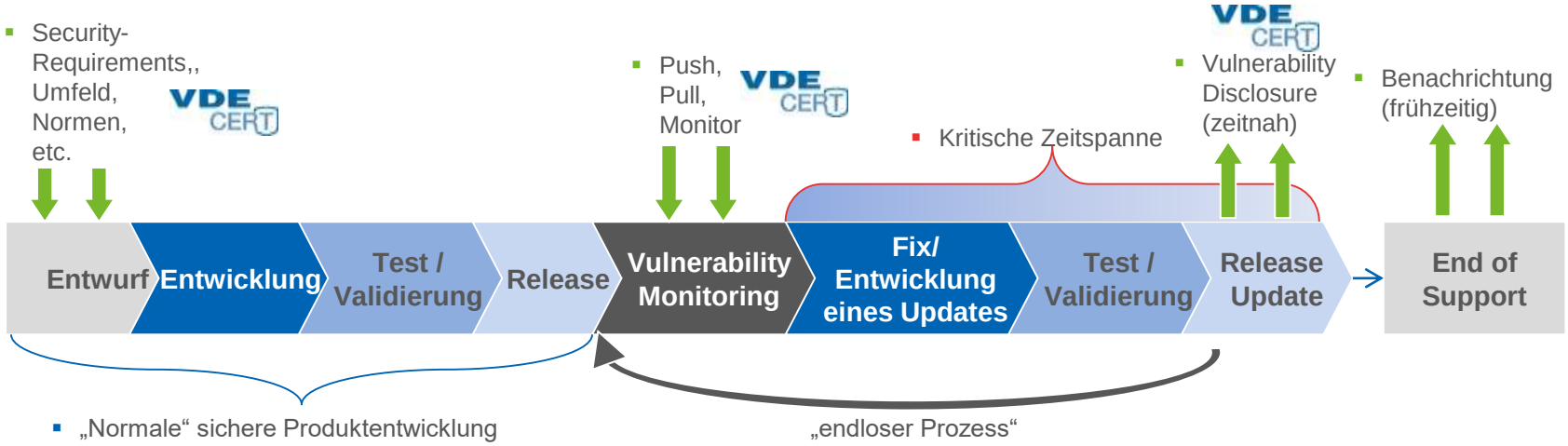
https://cert.vde.com



CERT@VDE: koordinierendes Produkt-CERT (PSIRT)



Produktlebenszyklus...und wo das CERT@VDE hilft



Konsumenten der CERT@VDE Informationen

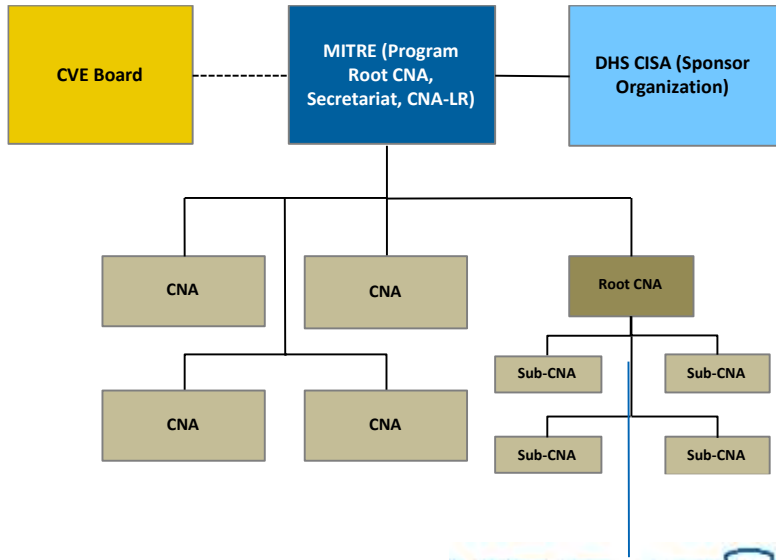
CERT@VDE ist anerkannte “CVE Numbering Authority (CNA)“: Vergabe von CVE Nummern!

Vorteile

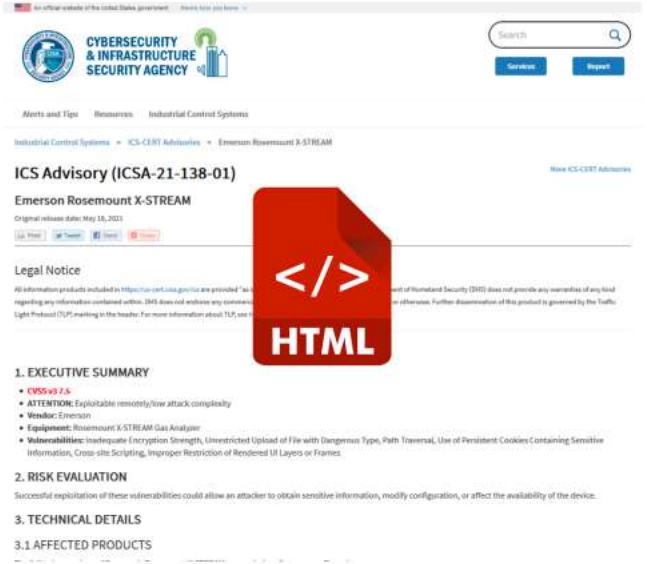
- Kontrolle des kompletten CVE-Veröffentlichungsprozess aus dem Scope des CERT@VDE
- ***Kein Teilen von Embargoinformationen mit anderer CNA notwendig!***
- Beschleunigter Vulnerability Disclosure Prozess

Voraussetzung:

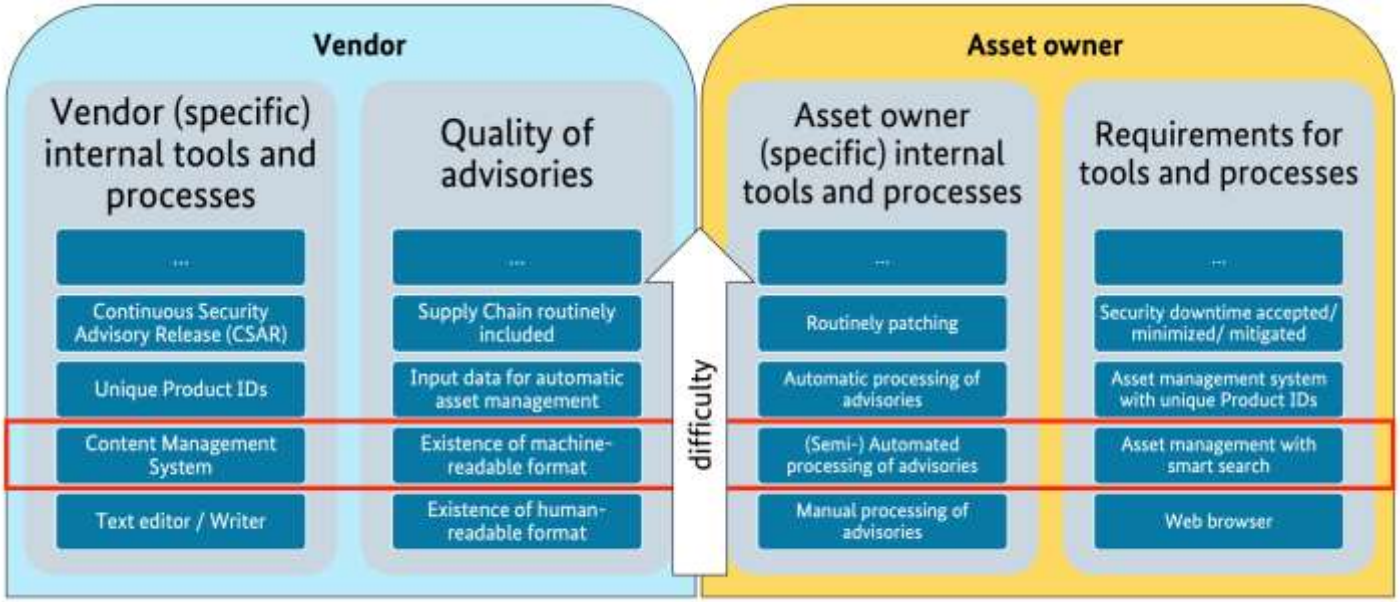
- Öffentlich zugängliche Disclosure Policy
- Positives Durchlaufen des CNA Anerkennungsprozesses bei MITRE
- Anerkennung und Beherrschen der CNA Regularien und Prozesse



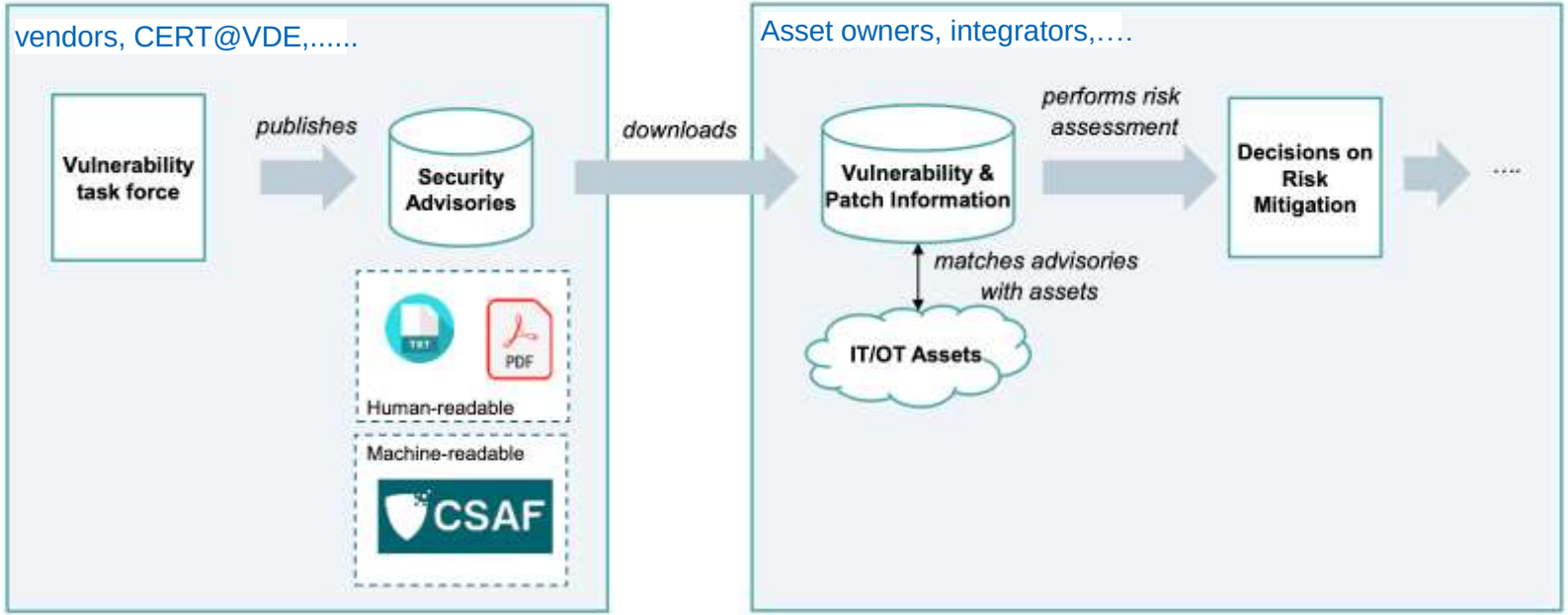
Status quo: wie CERTs heute arbeiten…



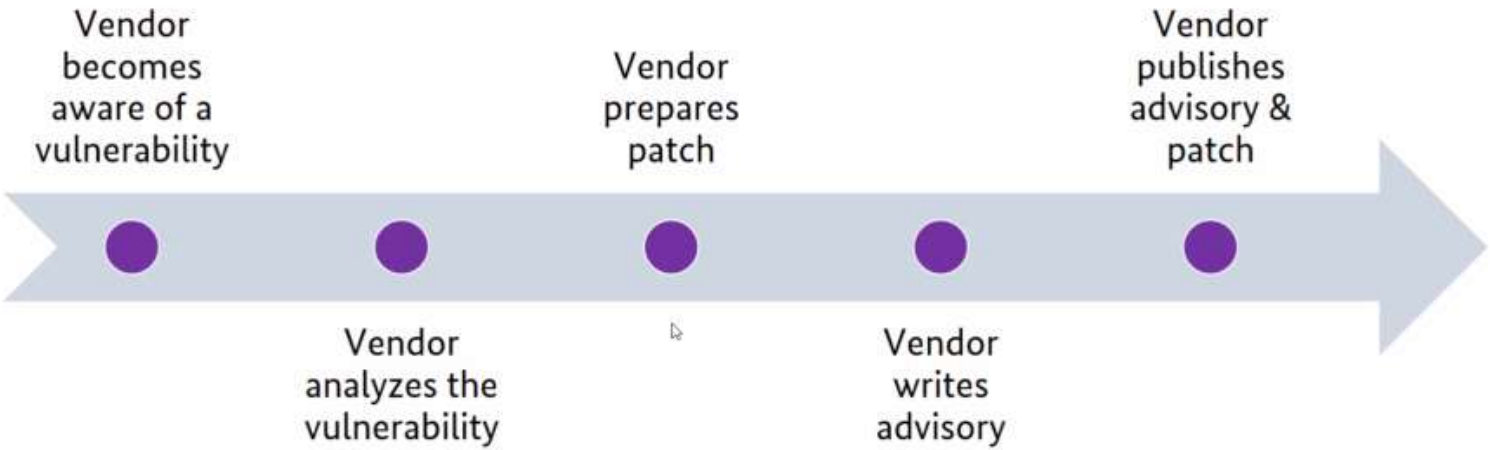
Nächster Schritt mit CSAF



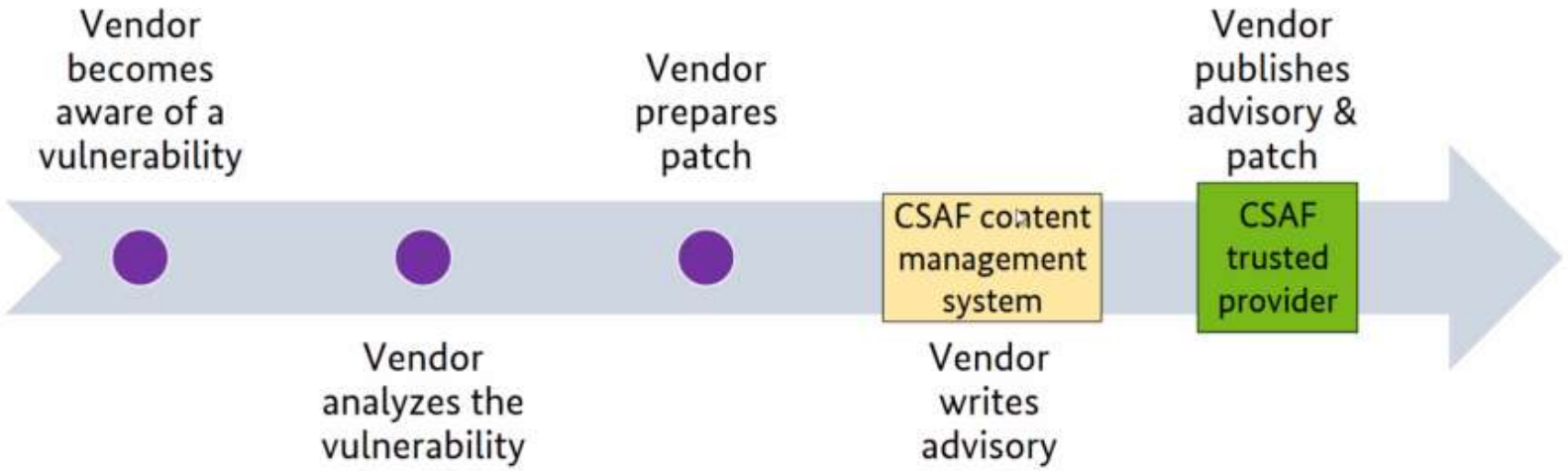
CSAF (Common Security Advisory Framework): → maschinenlesbares Advisory Format!



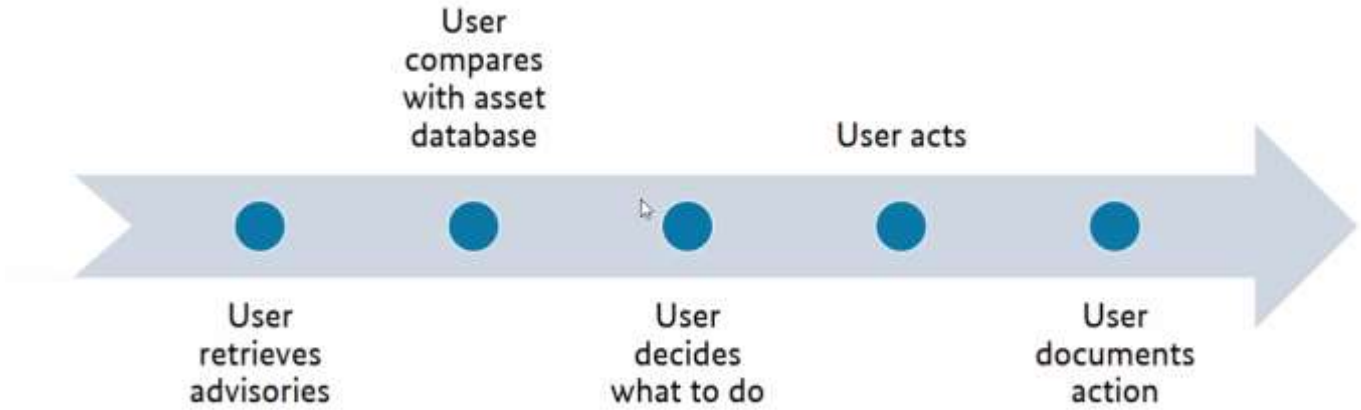
Hersteller - heute *Source: Thomas Schmidt (BSI)*



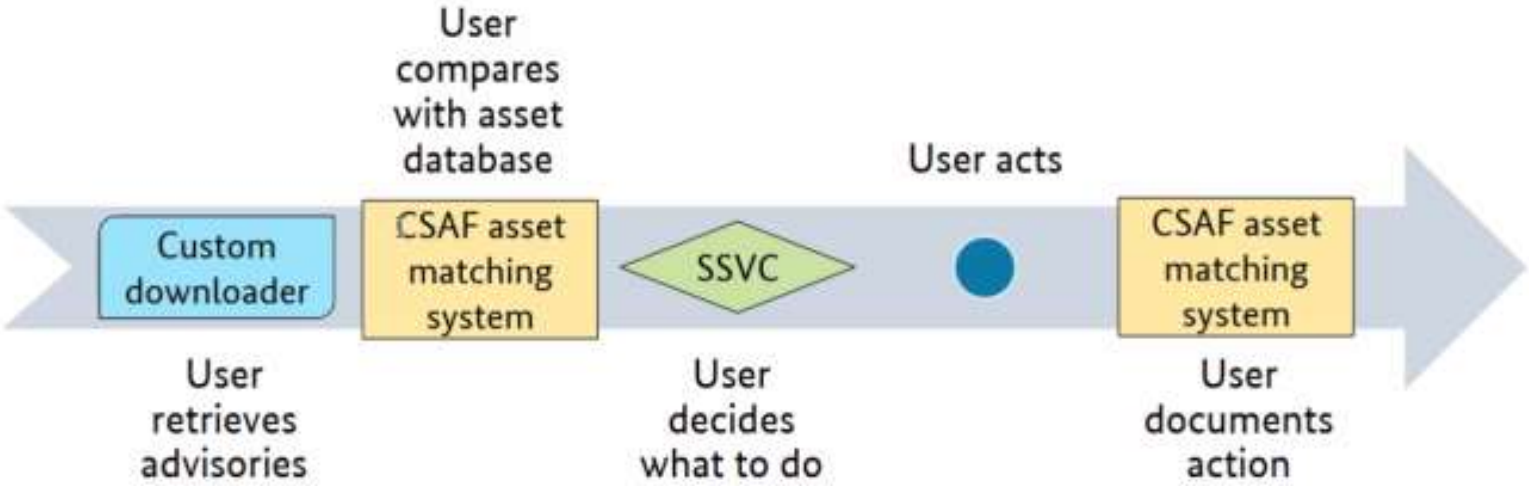
Hersteller - zukünftig *Source: Thomas Schmidt (BSI)*



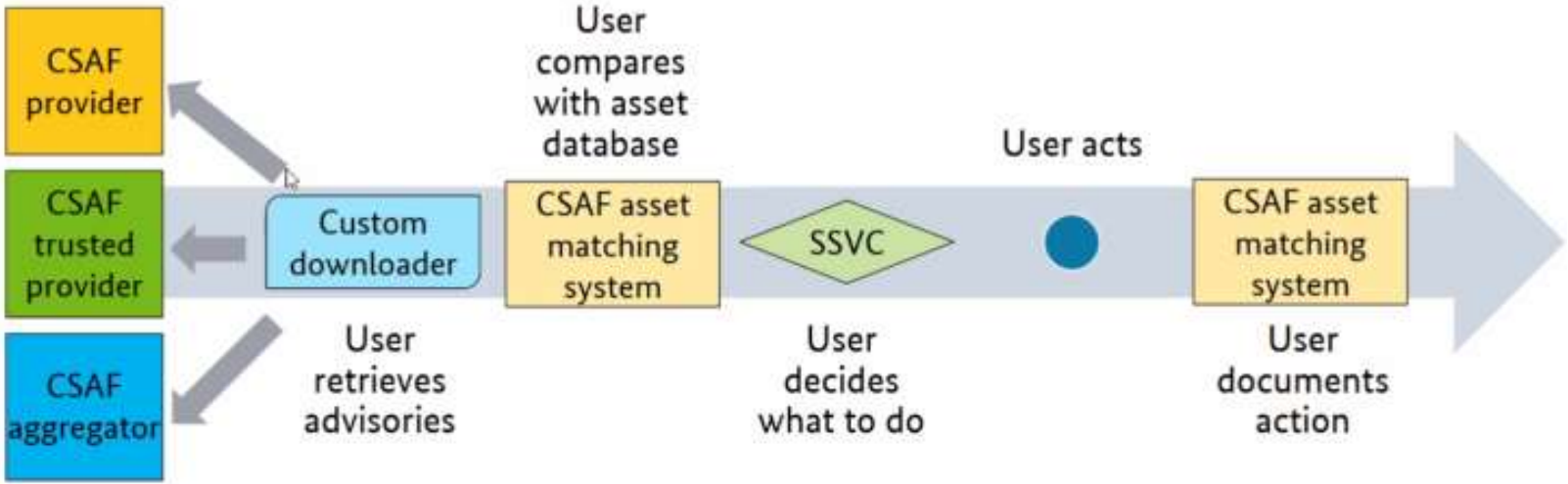
Betreiber - heute *Source: Thomas Schmidt (BSI)*



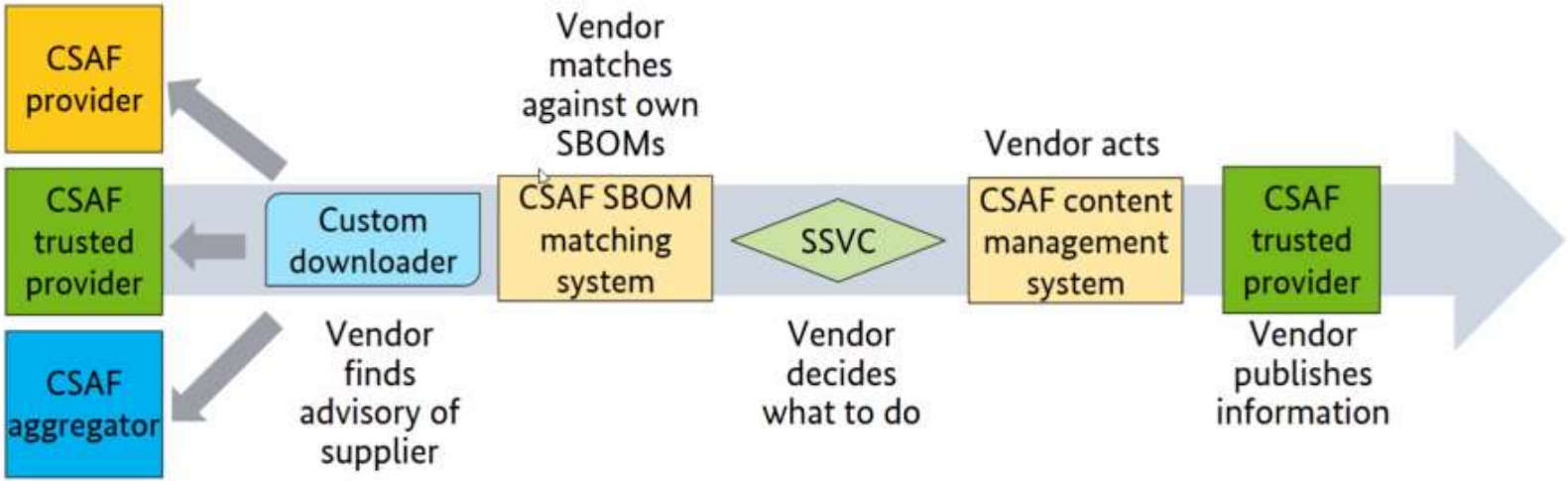
Betreiber - zukünftig *Source: Thomas Schmidt (BSI)*



Betreiber - zukünftig *Source: Thomas Schmidt (BSI)*

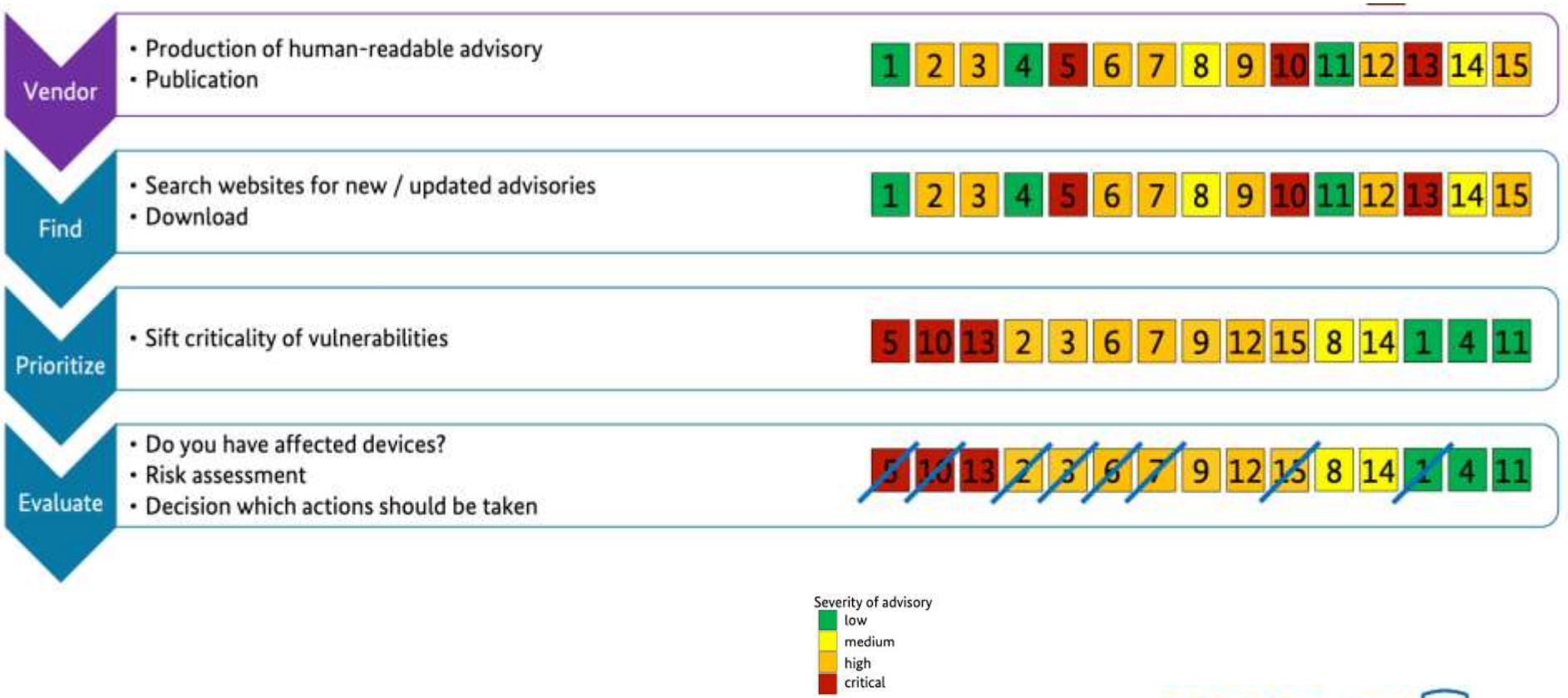


Hersteller ist auch Integrator und Betreiber!



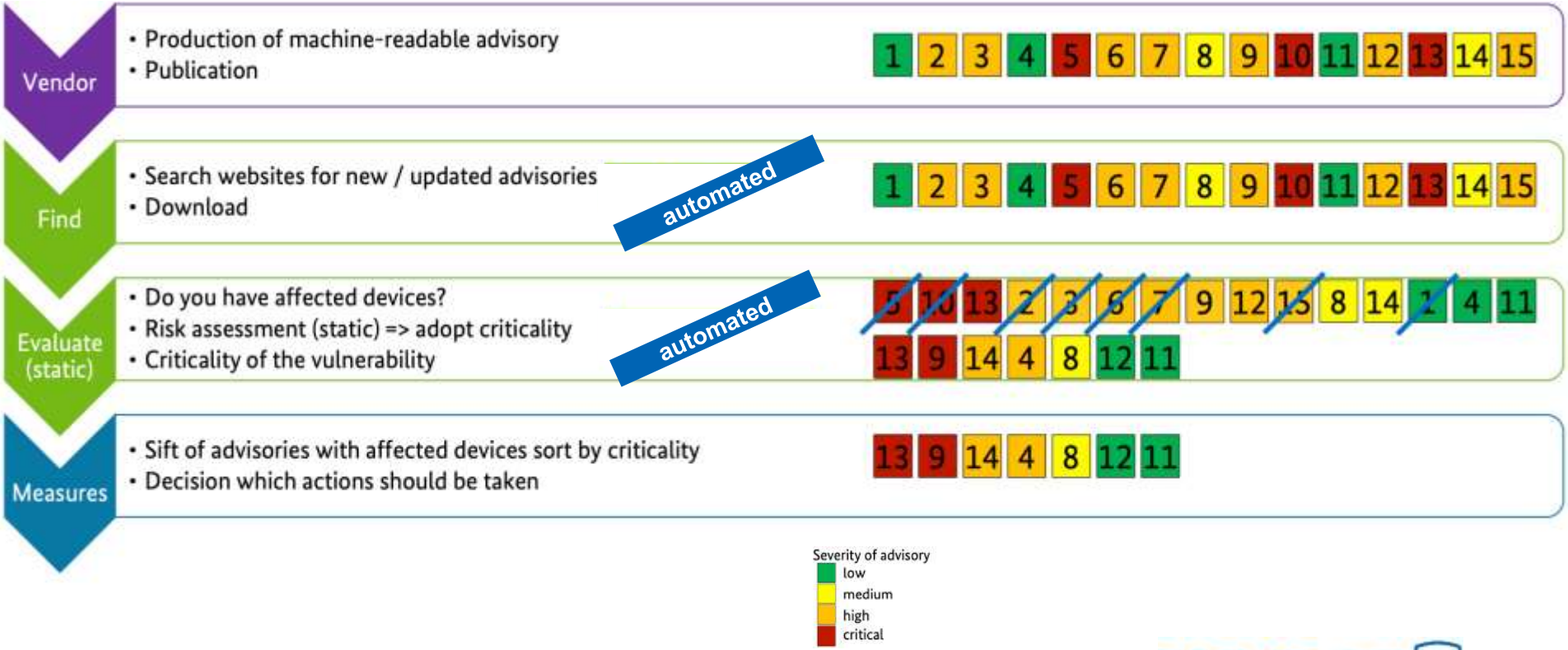
Schwachstellen-Handling: manuelle Prozesse bei Anwendern!

Source: Thomas Schmidt (BSI)



Schwachstellen-Handling mit CSAF…

Source: Thomas Schmidt (BSI)



Resümee

- Sicherheit wird „nicht weggehen“
- Sicherheit ist nicht nur **Produkt/Technik, sondern viel Prozess**
- Es ist Arbeit und berührt alle Bereiche eines Unternehmens
- … aber: Jeder kann es umsetzen..
  → Teile der Arbeiten können/müssen **automatisiert** werden
  → man muss **nicht alles selbst** tun: CERT@VDE

Resümee

…..

- **Risikominimierung durch …**

  - ***klare Kommunikation, nachvollziehbare Prozesse und operativer Austausch („Community der Handelnden“)***
  - ***CERT ist „Informationsmanagement“: zielgruppenorientiert!***
  - ***Frühwarnung***
  - ***Best Practices***
  - ***CVD: Offener Umgang mit Schwachstellen***
  - ***CERT ist „Krisenstab“ und nicht die „Eingreiftruppe“!***
  - ***CERT organisiert Hilfe-zur-Selbsthilfe → „organisationales Lernen“***

CERT@VDE

Zentrale Kontaktstelle...

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

Frühwarnsystem und Wissensvorsprung

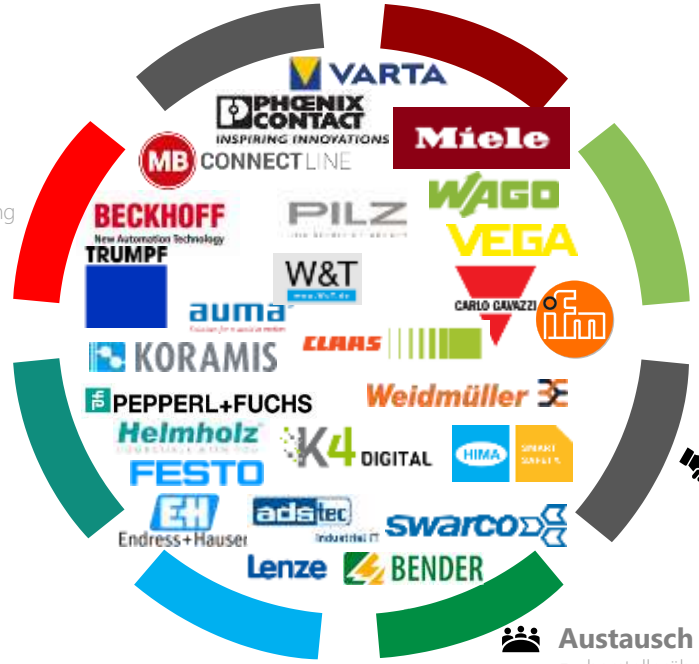
Frühzeitigeres Erkennen von Schwachstellen ermöglicht Partnern eine bessere Einschätzung!
...und dadurch eine schnelle, strukturierte Reaktion auf aktuelle Bedrohungen!

Minimierung Haftungsrisiken

- Best Practices des CERT@VDE unterstützen die Einhaltung von rechtlichen Vorgaben hinsichtlich „im Verkehr erforderliche Sorgfalt" und „Stand der Technik"
- Vertragliche und gesetzliche Produktbeobachtungs-pflichten der Partner werden unterstützt
- Das CERT@VDE hilft auch bei Kritis-Fällen, um die richtigen Wege zu gehen

Positives Firmenimage bei den Kunden

Teilnehmende Partner dokumentieren verantwortungsbewussten Umgang mit IT-Sicherheit



Advisory-Service – und CNA

Unterstützung der Partner durch routinierte Security-Experten:

- CVD Prozess: koordinierte, abgestimmte Veröffentlichung
- Interaktion in deutscher und englischer Sprache
- Koordination mit anderen CERTs (z. B. ICS-CERT)
- CERT@VDE ist eine von Mitre anerkannte CNA (CVE Numbering authority) und übernimmt für seine Partner die entsprechenden Aufgaben
- Zukünftig CSAF Publisher/Provider/Aggregator

Security Development Lifecycle

Partner können Schwachstelleninformationen über CWEs in Planung, Entwicklung und Modellierung neuer Produkte berücksichtigen ("Security-by-Design")

Partnerschaften und Akkreditierung

- CERT@VDE ist akkreditiert durch den europäischen Trusted Introducer
- CERT@VDE ist Mitglied im Deutschen CERT Verbund

Prozesse – Erfüllung von normativen Anforderungen

- 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
- anonymisiert (auf Wunsch) und in gleicher Zeitzone
- gemeinsame Workshops und Best Practices und operative Arbeit in TLP:RED Fokusgruppen
- Informationsmanagement und Interessensvertretung für die Partner in Richtung der (inter)nationalen CERT-Community

Vielen Dank für Ihre Aufmerksamkeit!

Ihr Ansprechpartner:

Andreas Harner

Leiter CERT@VDE

Tel. +49 69 6308-392

andreas.harner@cert.vde.com

VDE CERT