# Cyberdome als ganzheitlicher Schutzschirm für eine Nation.
# Von Idee, Vision zur technischen Realisierung

Jens Wiesner, BSI

Bundesamt
für Sicherheit in der
Informationstechnik

Bild: © AdobeStock/Nirut

# Motivation:
# Beschleunigte Bedrohungslage

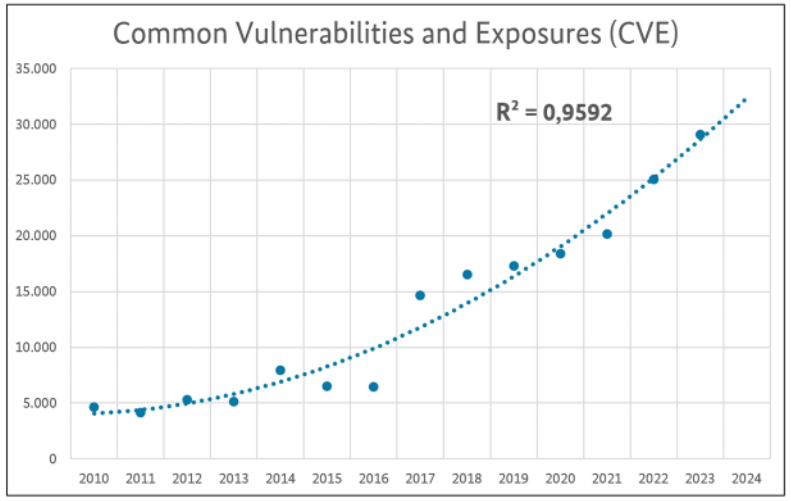


Bild: © AdobeStock/Azazul

# Von Schwachstellenmanagement - 2024

The sailing route

## Navigate through ~ 80 vulnerabilities/day



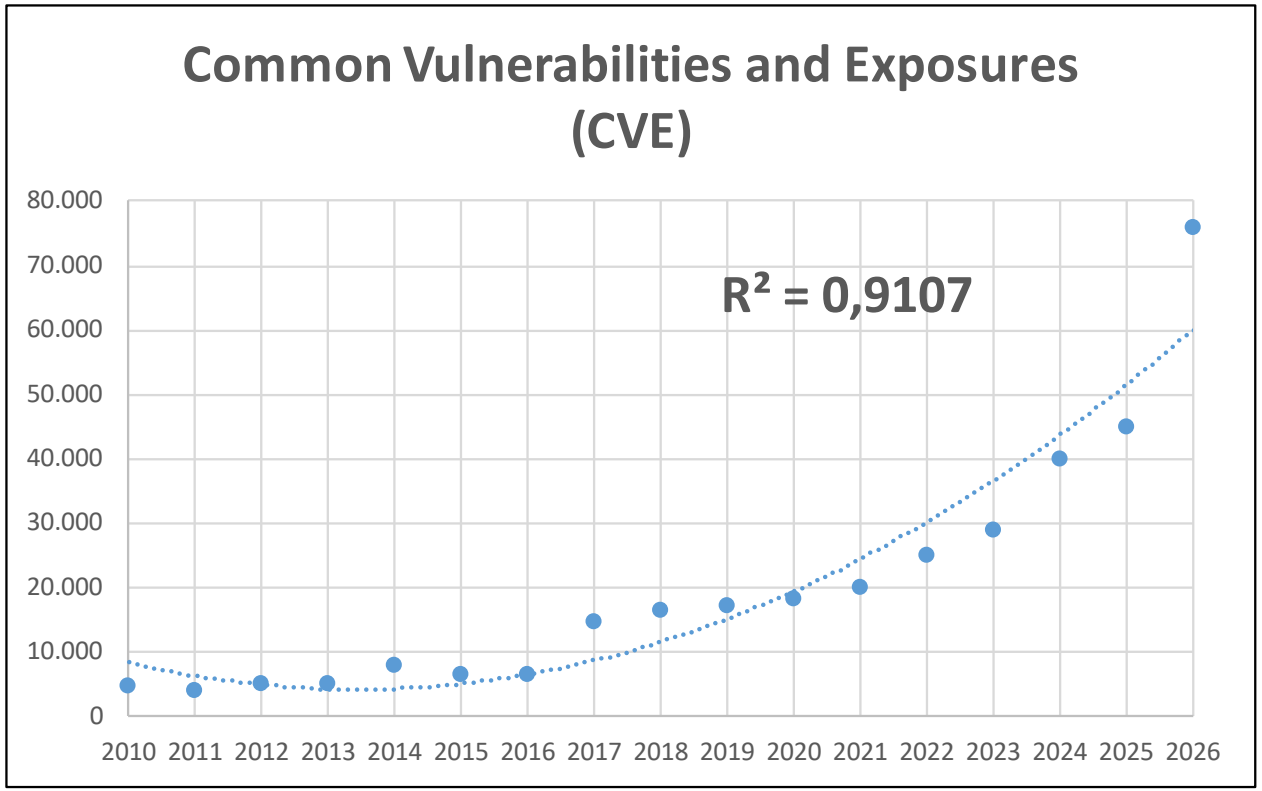

| Jahr | Anzahl der CVE |
|---|---|
| 2010 | 4.639 |
| 2011 | 4.150 |
| 2012 | 5.288 |
| 2013 | 5.142 |
| 2014 | 7.948 |
| 2015 | 6.494 |
| 2016 | 6.457 |
| 2017 | 14.645 |
| 2018 | 16.512 |
| 2019 | 17.308 |
| 2020 | 18.375 |
| 2021 | 20.161 |
| 2022 | 25.059 |
| 2023 | 29.065 |
| 2024 | ~ 33.000 |

Federal Office
for Information Security

# Increasing Problem - 2025

How many reported vulnerabilities can we expect in the coming years?

1. **Number of security-related vulnerabilities on the rise**
2. **Legal requirements** (BSIG, CRA, NIS 2, etc.)
3. **Vulnerability management vs. manual effort** (comparison with your own systems and infrastructure, assessment of criticality, impact, etc.)




| Year | Σ CVE |
|---|---|
| 2010 | 4.639 |
| 2011 | 4.150 |
| 2012 | 5.288 |
| 2013 | 5.142 |
| 2014 | 7.948 |
| 2015 | 6.494 |
| 2016 | 6.457 |
| 2017 | 14.645 |
| 2018 | 16.512 |
| 2019 | 17.308 |
| 2020 | 18.375 |
| 2021 | 20.161 |
| 2022 | 25.059 |
| 2023 | 28.961 |
| 2024 | 40.077 |
| 2025 | 44.845 |
| 2026* | 75.958 |

* Estimate

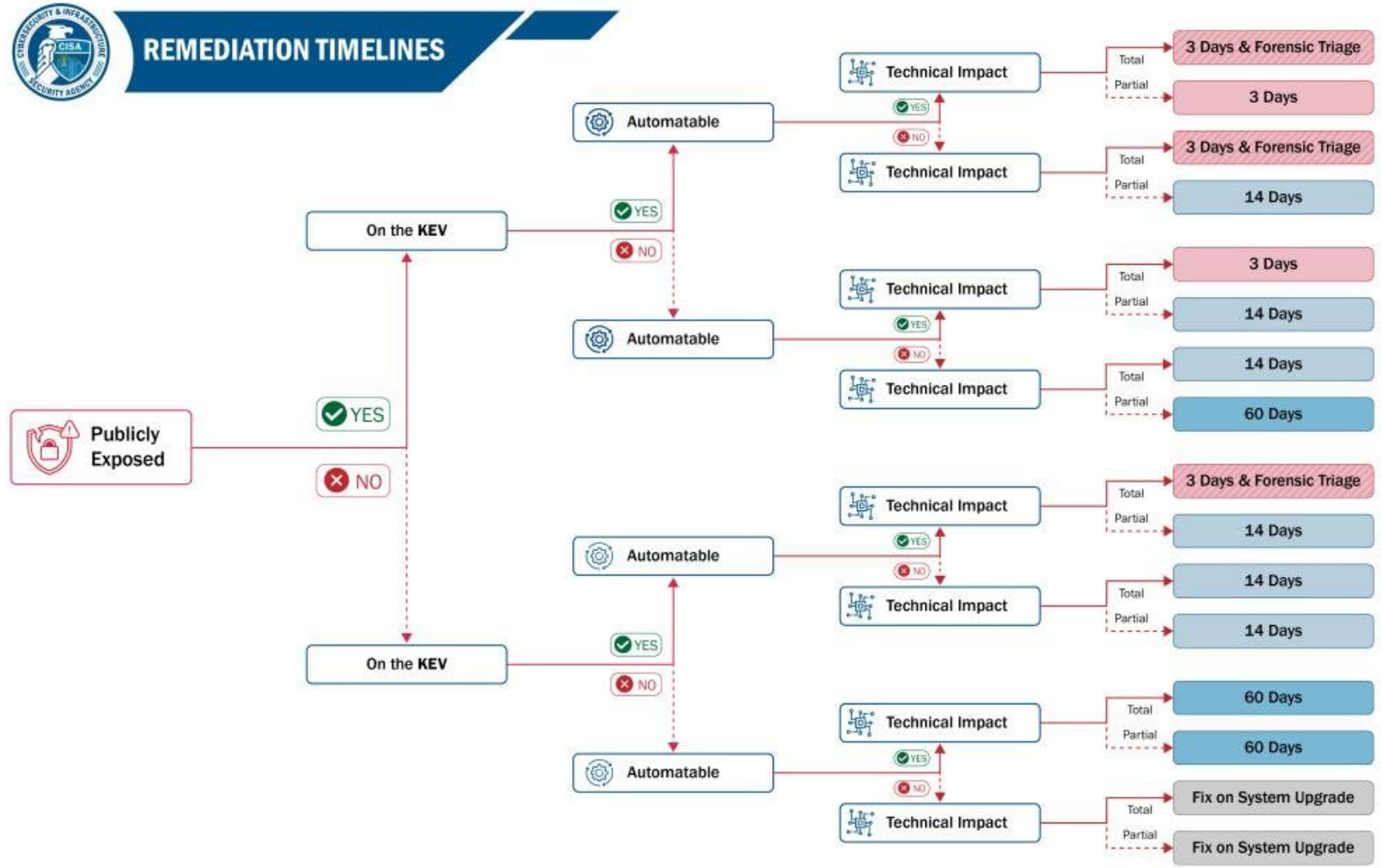
Data source: https://cve.mitre.org

# Zu Vulnpocalypse - 2026



# Konsequenzen: immer mehr Kompromittierungen

## CISA BOD 26-04: Prioritizing Security Updates Based on Risk

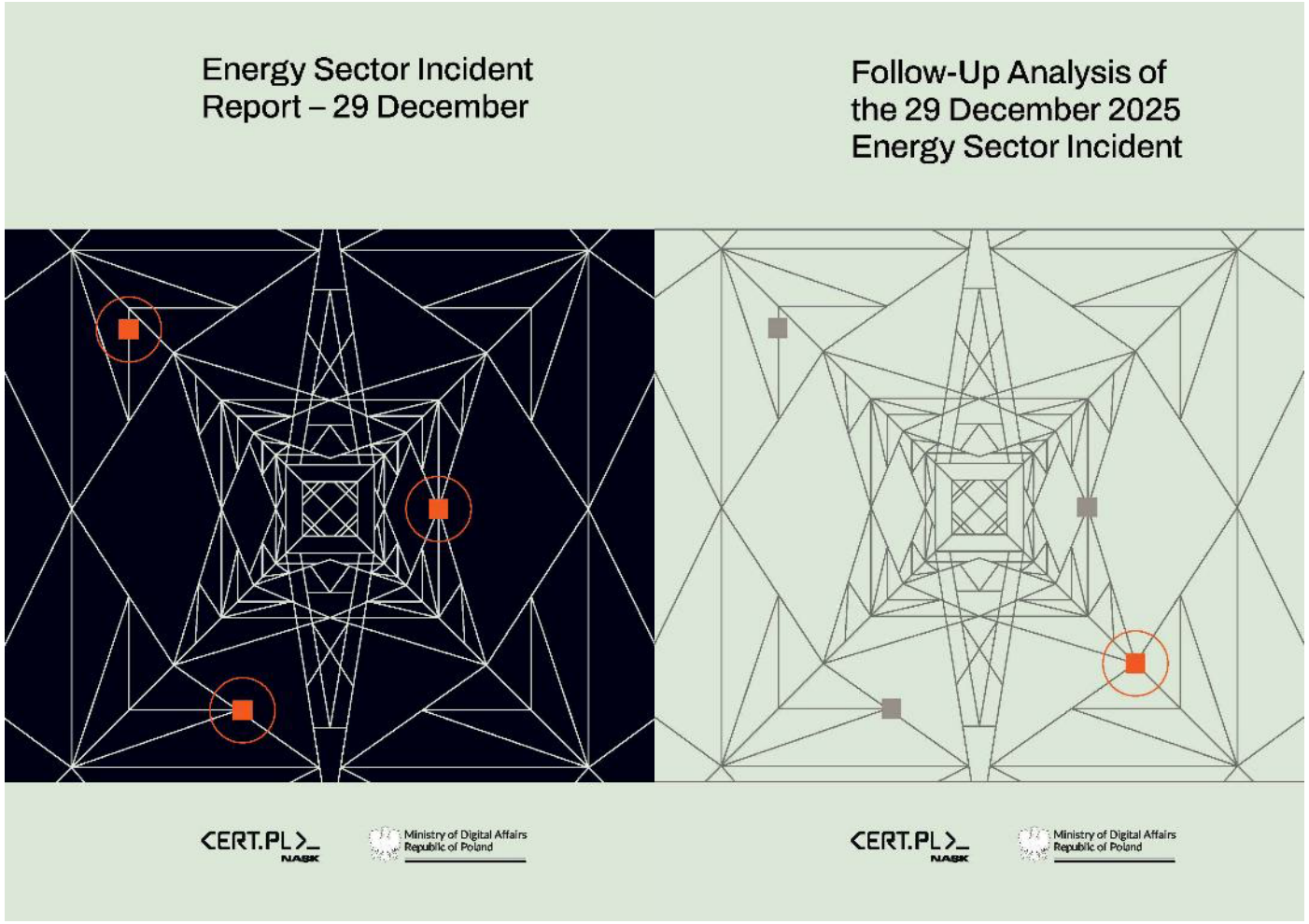


# Erfolgreiche Angriffe auf OT



Bild: © AdobeStock/Azazul

# Mehr Vorfälle mit Fokus OT






MINNESOTA MULTI-MUNICIPALITY WATER SYSTEM CYBERATTACK: COMPREHENSIVE INCIDENT ANALYSIS

*Incident Report — July 26–28, 2026 Coordinated OT Intrusion Campaign*

**Prepared:** July 28, 2026 | 21:28 CDT
**Classification:** UNCLASSIFIED // UNLIMITED-DISTRIBUTION — Draft Release Version
**Report Identifier:** IC-SCID-00150-2026.08.02.01
**Distribution:** PUBLIC RELEASE - DRAFT
**Prepared By:** infracritical
**Version:** 1.0 INITIAL [DRAFT] — Subject to Revision as Investigation Progresses

⚠ DRAFT — UNCLASSIFIED // UNLIMITED-DISTRIBUTION




NEWS

**UK and Allies urge critical sectors to improve defences against Russian intelligence targeting**

New advisory highlights Russian state cyber actors' global exploitation of poorly configured routers

# Gemeinsamkeiten der Angriffe

- Relativ „einfach“ (low hanging fruits), geringe Ressourcen und Reifegrad bei den Betreibern für OT-Sicherheit
- Direkt mit dem Internet verbundene Systeme mit keiner oder einer vorgelagerten Schutzfunktion (die dann versagt hat)
  - Oft LTE Modem außerhalb des bekannten IP Adressbereich des Betreibers
  - Private APNs erlaubten trotzdem lateral movement innerhalb des APNs
- Kein Monitoring der kritischen Systeme
- Zurücksetzen auf Auslieferungszustand oder Wiper
- Längere Zeitdauer bis zum Erkennen der Angriffe und noch länger für eine forensische Analyse
- Wiederherstellung eher in Wochen als in Stunden
- Unzureichende Blaupausen der Integratoren (Bad practices haben sich vervielfacht)

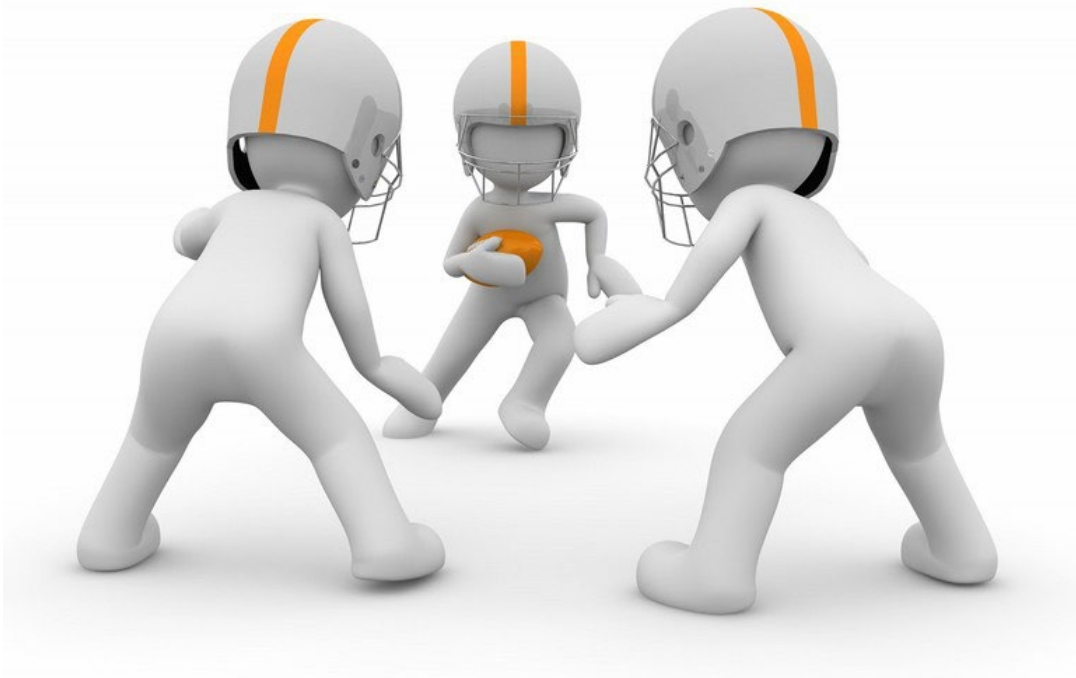
# Angriff oder Fehlfunktion?

## Über die Rolle des Supports

Wie merkt ein Betreiber einen fortschrittlichen Angriff?

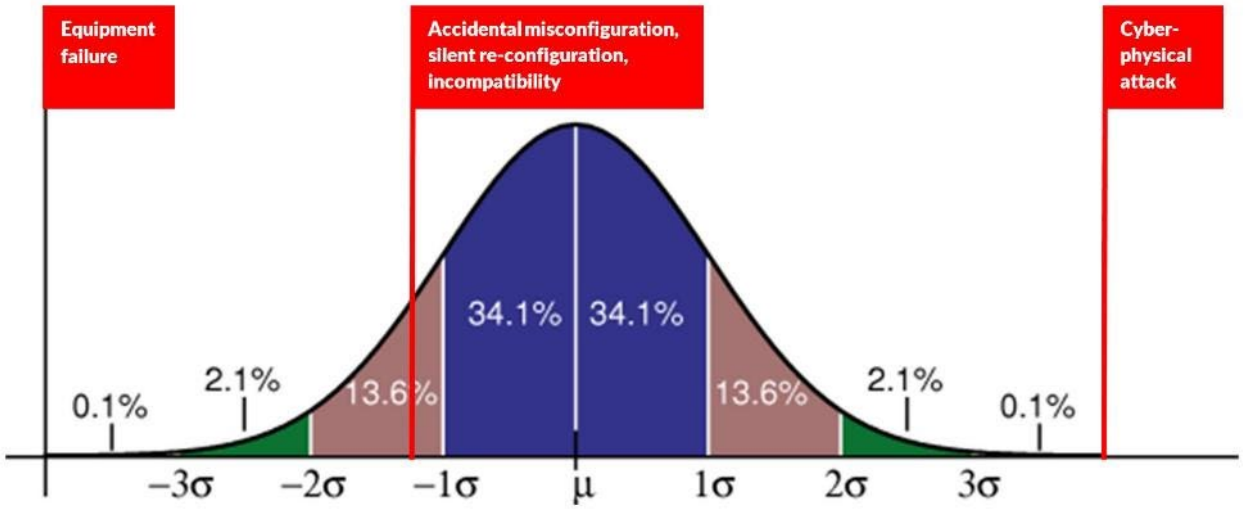
a. Gar nicht

b. Etwas tut nicht



**Postulat:**

- Viele Angriffe werden Hersteller als Supportfall gemeldet
- Hat Hersteller Ressourcen?
- Hat Hersteller Mandat, dies zu analysieren?
- Ist das überhaupt gewünscht? Meldepflichten nach CRA!



# Was kann ein Cyberdome hier tun?



Bild: © AdobeStock/Azazul

# Cyberdome



Bundesamt
für Sicherheit in der
Informationstechnik

# Warum braucht Deutschland den Cyberdome?



**Die Zahl von Cyberangriffen nimmt zu:**
Sie werden komplexer und wirkungsvoller. Sie treffen staatliche Institutionen, Kritische Infrastrukturen & Unternehmen und können so Wirtschaft und Gesellschaft insgesamt beeinträchtigen.



**Der Cyberdome ist Deutschlands Antwort darauf:**
Eine nationale Schutzinfrastruktur, die Bedrohungen früher erkennen, gemeinsam analysieren und schneller verhindern soll.



**Gemeinsamkeit macht stark:**
Bisher schützen sich Organisationen jeweils einzeln gegen Angriffe. Der Cyberdome verbindet diese Einzelmaßnahmen zu einem stärkeren gemeinsamen Schutzsystem.

# Wie funktioniert der Cyberdome?

**Die Sensorik**
erkennt verdächtige Aktivitäten, Angriffe und Schwachstellen möglichst früh.

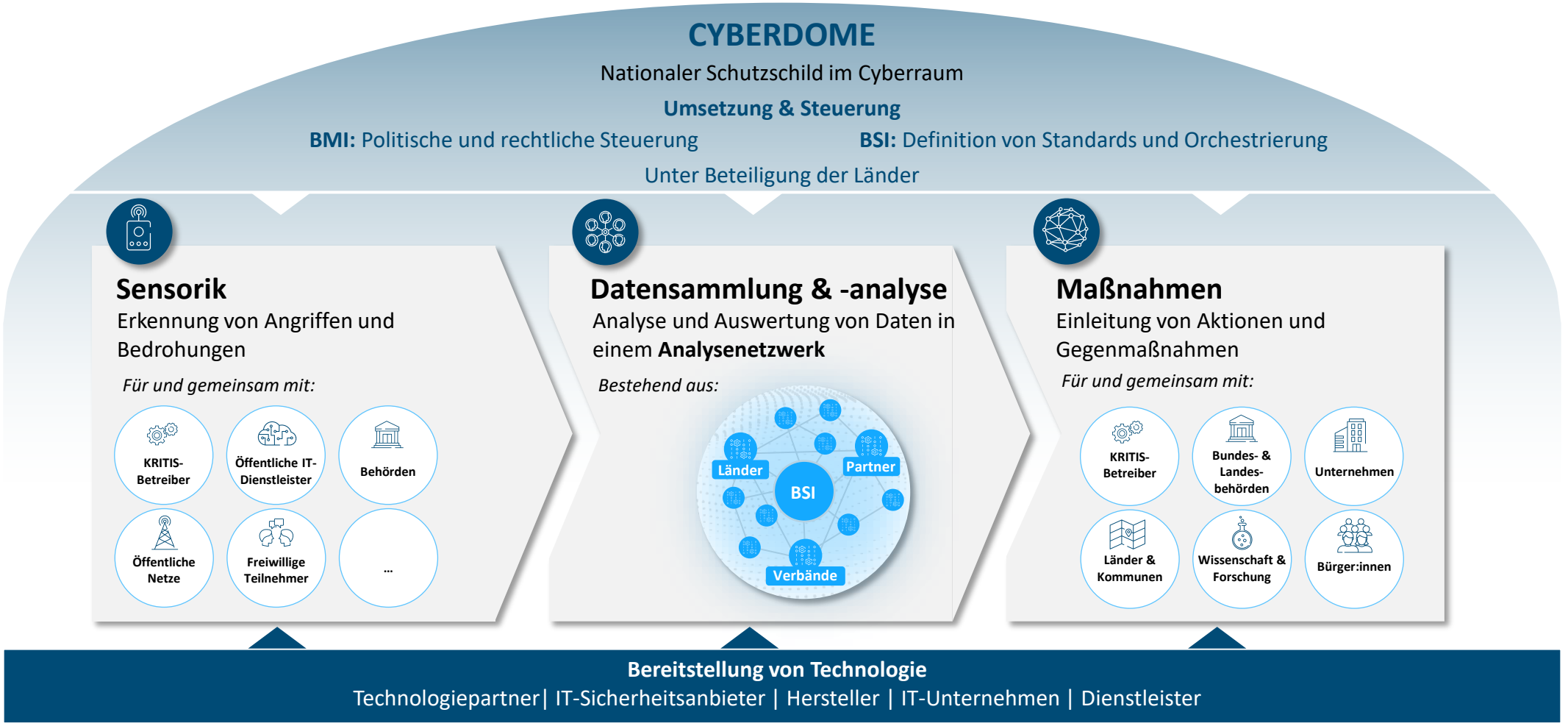
**Der Analyseverbund**
führt Informationen zusammen, erkennt Zusammenhänge und schafft ein gemeinsames Lagebild.

**Das offene Ökosystem**
verbindet unterschiedliche Akteure, Technologien und Sicherheitssysteme über gemeinsame Standards und Schnittstellen.



Das Prinzip dahinter: Wird eine Bedrohung an einer Stelle erkannt, können andere Beteiligte schneller gewarnt werden und Schutzmaßnahmen einleiten. **Aus vielen einzelnen Signalen wird gemeinsames Wissen. Aus gemeinsamem Wissen wird schnellerer Schutz.**

# Der Cyberdome für Deutschland wird mit Partnern gemeinsam umgesetzt



# Der Cyberdome funktioniert nur gemeinsam.

- Der Cyberdome ist kein geschlossenes Einzelsystem, sondern ein wachsendes Ökosystem, in dem unterschiedliche Akteure ihre Fähigkeiten und Erkenntnisse zusammenbringen. Die Teilnahme basiert auf Freiwilligkeit.

**Bund:**
BMI und BSI treiben den Cyberdome politisch, strategisch und technisch voran.

**Länder und Kommunen**:
Sie sind wichtige Partner beim Aufbau und der Erprobung, beispielsweise durch den Deutschland-Scan.

**Wirtschaft und KRITIS:**
Unternehmen und Betreiber Kritischer Infrastrukturen profitieren vom gemeinsamen Wissen, schnelleren Warnungen und Gegenmaßnahmen.

**Wissenschaft und Technologiepartner:**
Sie bringen Innovationen und neue Lösungen für Erkennung, Analyse und Abwehr ein.

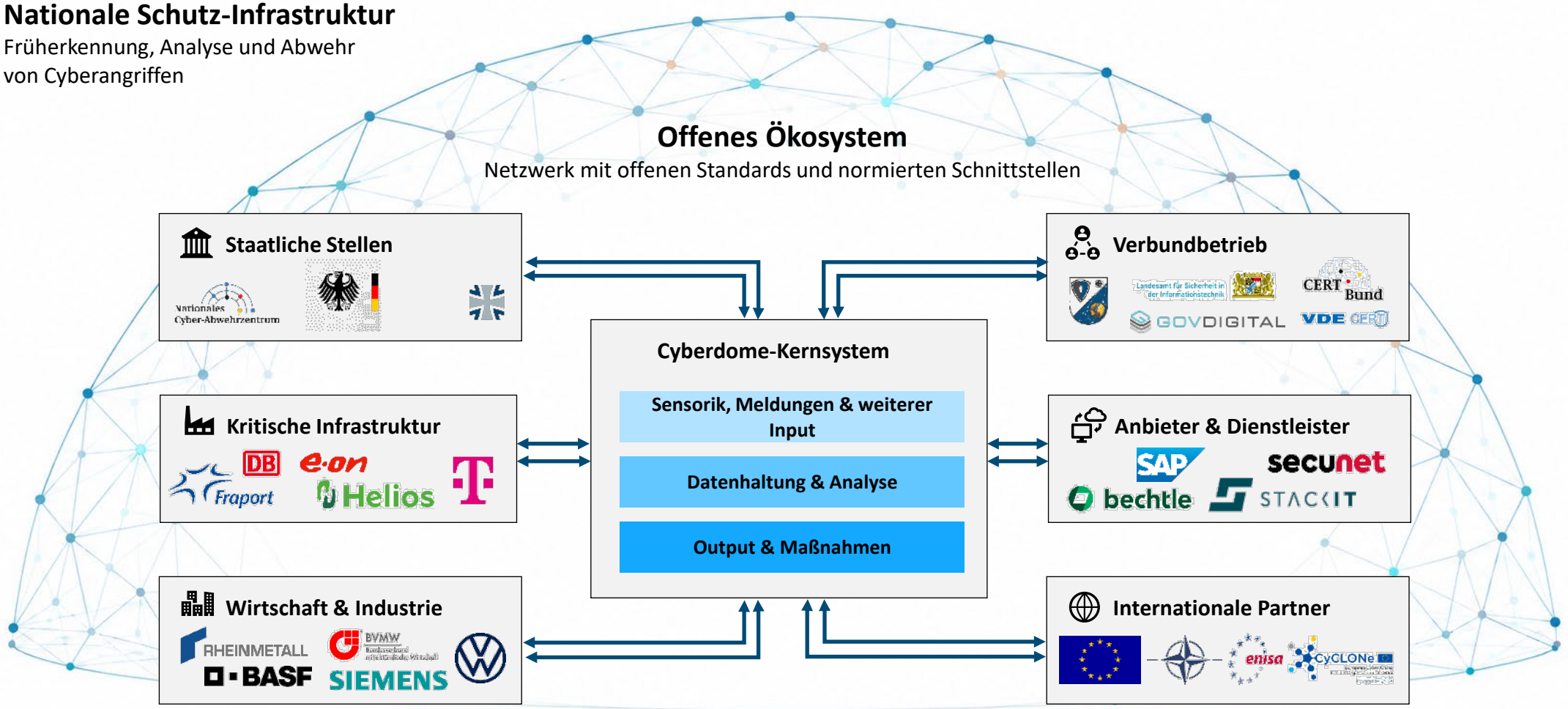
**Viele Partner, ein gemeinsames Ziel: Deutschland widerstandsfähiger machen.**

# Architekturvision Cyberdome: Ökosystem-Sicht

Bundesamt für Sicherheit in der Informationstechnik

**Nationale Schutz-Infrastruktur**
Früherkennung, Analyse und Abwehr von Cyberangriffen

**Offenes Ökosystem**
Netzwerk mit offenen Standards und normierten Schnittstellen




→ Meldungen, Sensordaten, Angriffsindikatoren, Schwachstellen, Lageinformationen, Maßnahmenstatus

→ Warnungen, Lagebilder, Erkenntnisse, IoCs und Erkennungsregeln, Schutz- und Abwehrmaßnahmen

**Hinweis:** Die dargestellten Organisationen und deren Logos dienen ausschließlich der **beispielhaften** Veranschaulichung relevanter Akteursgruppen. Die Auswahl ist nicht abschließend und impliziert weder eine Beteiligung oder Partnerschaft noch eine Unterstützung, Empfehlung oder sonstige Verbindung mit dem Cyberdome. Sämtliche Rechte an den dargestellten Marken und Logos liegen bei den jeweiligen Rechteinhabern.

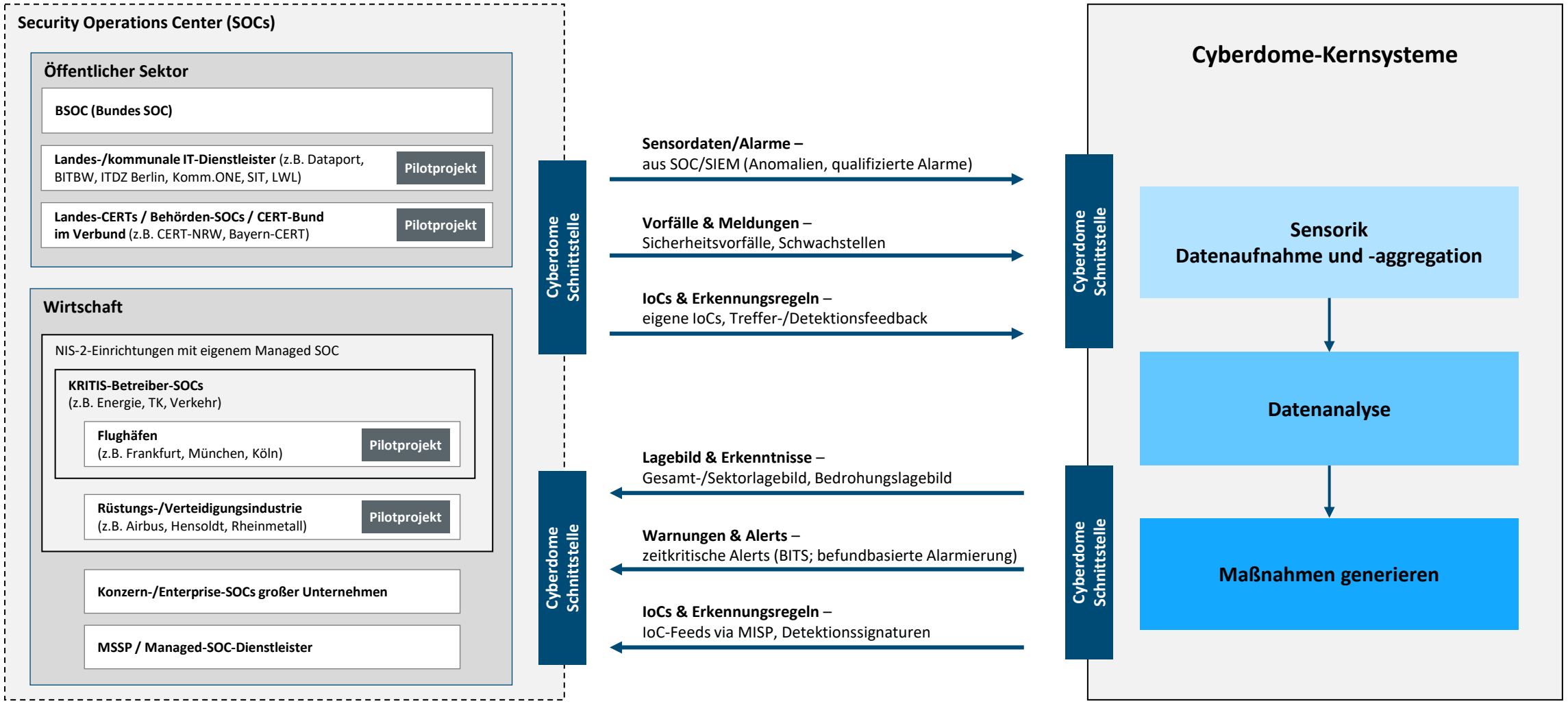
# Bis Ende 2028 soll der Cyberdome in drei aufeinander aufbauenden Phasen iterativ entwickelt werden

## Phasenkonzept Cyberdome im Überblick

| Cyberdome 1.0 – Initiierung bis Ende 2026 | Cyberdome 2.0 – Realisierung bis Ende 2027 | Cyberdome 3.0* – Erweiterung 2028 |
|---|---|---|
| **Ziele** | | |
| Tragfähiges Fundament konzeptionieren | Anwendung in die Breite tragen | Nationales Schutz-Ökosystem etablieren |
| Operative Wirksamkeit beweisen | Übergreifende Wirkung erzeugen | Gesamtstaatliche und europäische Wirkung erzeugen |
| **Maßnahmen** | | |
| Use Cases initial umsetzen und Architektur etablieren | Fähigkeiten und Use Cases sektoral ausbauen | Integration und Automatisierung erhöhen |
| Fachbereich Cyberdome im BSI gründen | Analysenetzwerk und -plattform aufbauen | Analysenetzwerk und -plattform erweitern |
| Informative Einbindung der Länder und Partner verankern | Länder technisch und organisatorisch einbeziehen | Beteiligung verstetigen |

* Der Cyberdome 3.0 stellt dabei keinen Endzustand dar

# Ökosystem-Beispiel Interaktion mit externen SOCs



# Relevante Fähigkeiten in jeweils drei Kern- und Querschnittsbereichen



# Kritische Innensicht



Bild: © AdobeStock/Azazul

# Heutige fragmentierte Lage- und Maßnahmenlandschaft zwischen BSI und Stakeholdern

# Heutige fragmentierte Lage- und Maßnahmenlandschaft zwischen BSI und Stakeholdern



# Heutige fragmentierte Lage- und Maßnahmenlandschaft zwischen BSI und Stakeholdern






# Heutige fragmentierte Lage- und Maßnahmenlandschaft zwischen BSI und Stakeholdern









# Heutige fragmentierte Lage- und Maßnahmenlandschaft zwischen BSI und Stakeholdern

## 1 Kein übergreifendes Lagebild

BSI sieht Regierungsnetze, aber keine Lage aus KRITIS oder NIS2.



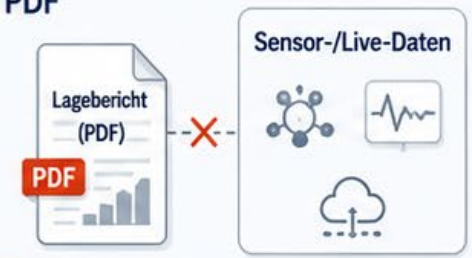

## 2 Schwachstellen: Advisories, Warnungen und Scans

Infos in verschiedenen Systemen und manuell per E-Mail an Betroffene




## 3 Lagebild per PDF

keine Echtzeit-integration von Sensordaten.




## 4 IOCs via MISP

BSI teilt heute schon IOCs via MISP. Aber keine Integration in Schutzsysteme, kein Rückkanal zu Detektionen.



# Heutige fragmentierte Lage- und Maßnahmenlandschaft zwischen BSI und Stakeholdern

## 1 Kein übergreifendes Lagebild

BSI sieht Regierungsnetze, aber keine Lage aus KRITIS oder NIS2.



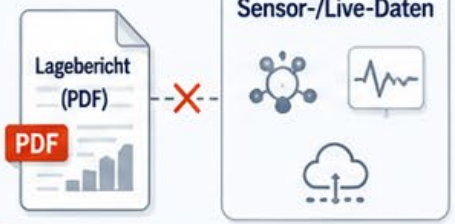

## 2 Schwachstellen: Advisories, Warnungen und Scans

Infos in verschiedenen Systemen und manuell per E-Mail an Betroffene




## 3 Lagebild per PDF

keine Echtzeit-integration von Sensordaten.




## 4 IOCs via MISP

BSI teilt heute schon IOCs via MISP. Aber keine Integration in Schutzsysteme, kein Rückkanal zu Detektionen.




## 5 Keine durchgehenden Wirkungsketten

von Sensor, Analyse und Maßnahmen zwischen BSI und Stakeholdern.



# Heutige fragmentierte Lage- und Maßnahmenlandschaft zwischen BSI und Stakeholdern

## 1 Kein übergreifendes Lagebild

BSI sieht Regierungsnetze, aber keine Lage aus KRITIS oder NIS2.



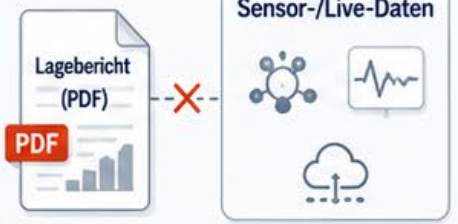

## 2 Schwachstellen: Advisories, Warnungen und Scans

Infos in verschiedenen Systemen und manuell per E-Mail an Betroffene




## 3 Lagebild per PDF

keine Echtzeit-integration von Sensordaten.




## 4 IOCs via MISP

BSI teilt heute schon IOCs via MISP. Aber keine Integration in Schutzsysteme, kein Rückkanal zu Detektionen.




## 5 Keine durchgehenden Wirkungsketten

von Sensor, Analyse und Maßnahmen zwischen BSI und Stakeholdern.




## 6 Keine niedrigschwelligen Kommunikationsmethoden

kein Chat zwischen BSI und Stakeholdern.



# Heutige fragmentierte Lage- und Maßnahmenlandschaft zwischen BSI und Stakeholdern

## 1 Kein übergreifendes Lagebild

BSI sieht Regierungsnetze, aber keine Lage aus KRITIS oder NIS2.



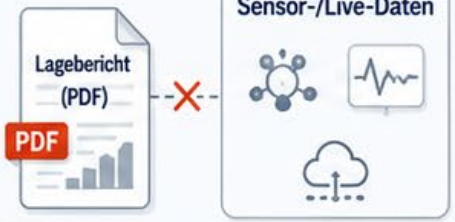

## 2 Schwachstellen: Advisories, Warnungen und Scans

Infos in verschiedenen Systemen und manuell per E-Mail an Betroffene




## 3 Lagebild per PDF

keine Echtzeit-integration von Sensordaten.




## 4 IOCs via MISP

BSI teilt heute schon IOCs via MISP. Aber keine Integration in Schutzsysteme, kein Rückkanal zu Detektionen.




## 5 Keine durchgehenden Wirkungsketten

von Sensor, Analyse und Maßnahmen zwischen BSI und Stakeholdern.




## 6 Keine niedrigschwelligen Kommunikationsmethoden

kein Chat zwischen BSI und Stakeholdern.



## 7 Verschiedene Portale und Anlaufstellen

für Stakeholder.



# Heutige fragmentierte Lage- und Maßnahmenlandschaft zwischen BSI und Stakeholdern

## 1 Kein übergreifendes Lagebild

BSI sieht Regierungsnetze, aber keine Lage aus KRITIS oder NIS2.



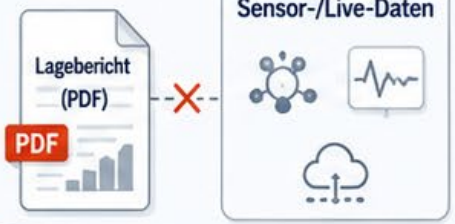

## 2 Schwachstellen: Advisories, Warnungen und Scans

Infos in verschiedenen Systemen und manuell per E-Mail an Betroffene




## 3 Lagebild per PDF

keine Echtzeit-integration von Sensordaten.




## 4 IOCs via MISP

BSI teilt heute schon IOCs via MISP. Aber keine Integration in Schutzsysteme, kein Rückkanal zu Detektionen.




## 5 Keine durchgehenden Wirkungsketten

von Sensor, Analyse und Maßnahmen zwischen BSI und Stakeholdern.




## 6 Keine niedrigschwelligen Kommunikationsmethoden

kein Chat zwischen BSI und Stakeholdern.



## 7 Verschiedene Portale und Anlaufstellen

für Stakeholder.

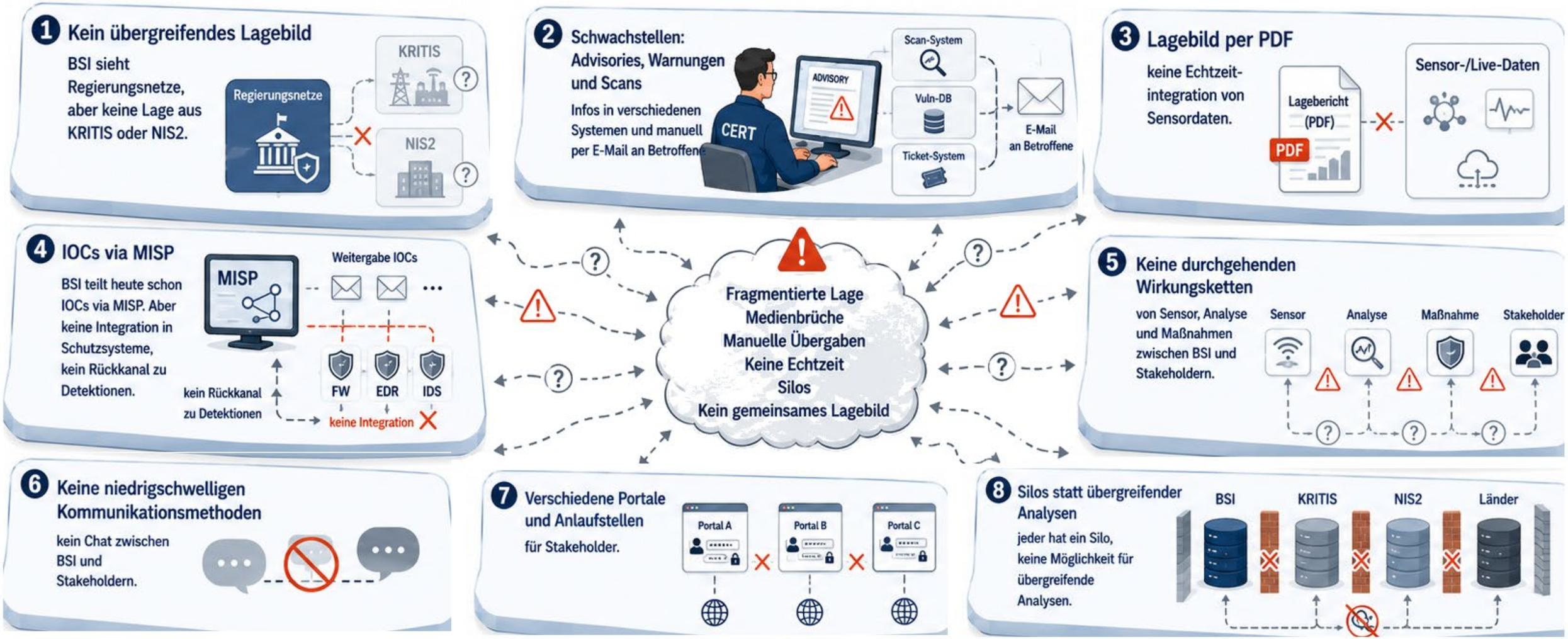



## 8 Silos statt übergreifender Analysen

jeder hat ein Silo, keine Möglichkeit für übergreifende Analysen.



# Heutige fragmentierte Lage- und Maßnahmenlandschaft zwischen BSI und Stakeholdern



# Heutige fragmentierte Lage- und Maßnahmenlandschaft zwischen BSI und Stakeholdern

## 1 Kein übergreifendes Lagebild

BSI sieht Regierungsnetze, aber keine Lage aus KRITIS oder NIS2.



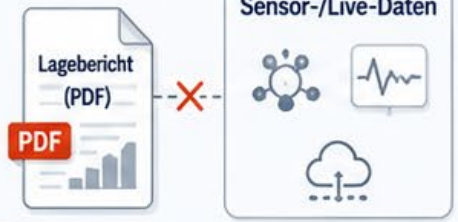

## 2 Schwachstellen: Advisories, Warnungen und Scans

Infos in verschiedenen Systemen und manuell per E-Mail an Betroffene




## 3 Lagebild per PDF

keine Echtzeit-integration von Sensordaten.




## 4 IOCs via MISP

BSI teilt heute schon IOCs via MISP. Aber keine Integration in Schutzsysteme, kein Rückkanal zu Detektionen.




**Fragmentierte Lage**
**Medienbrüche**
**Manuelle Übergaben**
**Keine Echtzeit**
**Silos**
**Kein gemeinsames Lagebild**

## 5 Keine durchgehenden Wirkungsketten

von Sensor, Analyse und Maßnahmen zwischen BSI und Stakeholdern.




## 6 Keine niedrigschwelligen Kommunikationsmethoden

kein Chat zwischen BSI und Stakeholdern.



## 7 Verschiedene Portale und Anlaufstellen

für Stakeholder.




## 8 Silos statt übergreifender Analysen

jeder hat ein Silo, keine Möglichkeit für übergreifende Analysen.




**Heute:** viele isolierte Informationen, manuelle Übergaben und keine integrierte Wirkungskette

- kein Gesamtlagebild
- PDF statt Echtzeit
- Silos
- kein durchgängiger Austausch

# Rechtliche Voraussetzungen



Bild: © AdobeStock/Azazul

# Der Weg eines Gesetzes

Gesetz

GESETZ · 27.02.2026

## Gesetzesentwurf zur Stärkung der Cybersicherheit

Angemessene Regelungen für die verbesserte Detektion und Abwehr von Cyberangriffen

### Umsetzungsstand



Referentenentwurf ist veröffentlicht [PDF, 636KB]

27.02.2026

Regierungsentwurf ist verabschiedet [PDF, 985KB]

27.05.2026

Gesetz noch nicht verkündet

https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/CI1/cyberabwehr.html

# „Cyber Abwehrgesetz“

[…]

Für das BSI sieht der Entwurf zur Stärkung der Cybersicherheit u.a. Verbesserungen für den Betrieb des Schadprogramm-Erkennungssystems (SES) zum Schutz der Kommunikation des Bundes, Anordnungsbefugnisse des BSI gegenüber DNS- und digitalen Diensteanbietern sowie Verpflichtung von TK- und digitalen Diensteanbietern, dem BSI sicherheitsrelevante Informationen zur Verfügung zu stellen, und im **Bereich KRITIS** die **automatisierte Ausleitung von Verfügbarkeitsindikatoren** für kritische Anlagen ("**Heartbeat**") und **Informationen zur Angriffserkennung an BSI** vor.

# Mittels Heartbeat erhält das BSI kontinuierlich Verfügbarkeits-informationen von kritischen Dienstleistungen in Deutschland

Bundesamt für Sicherheit in der Informationstechnik

## Vertiefung: § 31 Abs. 3 Nr. 1 BSIG

### Zentrales Verständnis



**Heartbeat**
§31
Absatz 3
Nr. 1

- **Aggregierte Ampellogik**:
  kontinuierliche Übermittlung des aggregierten und priorisierten Betriebsstatus der kritischen Dienstleistung (KDL)
- **Rückwirkungsfreie Übermittlung:**
  keine direkte Reaktion (Anweisungen oder Schaltbefehle) seitens BSI oder anderer Behörden möglich
- **Quantitative Ergänzung:**
  quantitative Verfügbarkeitsinformation zu den eingesetzten Prozessmitteln können mit übermittelt werden
- **Zusätzliche Detailinformationen:**
  der Verfügbarkeitsindikator kann, auch nachträglich, um zusätzliche Informationen ergänzt werden, z. B.:
  - Geplant: Wartung oder Reduktion aufgrund geringer Nachfrage
  - Ungeplant aber erklärbar: Reduktion aufgrund eines Defekts
  - Ungeplant und nicht erklärbar: plötzlicher Stillstand der Anlage

**Beispiel**: *Gaskraftwerk liefert nominal 1200 MW mit 3 Blöcken à 400 MW*

- 🟢 *Alle drei Blöcke des Kraftwerks laufen (Leistung 1200 MW)*
- 🟡 *Geplante Routinewartung von Block 1 (Leistung 800 MW)*
- 🟠 *Technischer Defekt in Block 1 und 2 (Leistung 400 MW)*
- 🔴 *Alle 3 Blöcke fallen spontan aus (Leistung 0 MW)*

# Zukünftig sollen Verfügbarkeitsindikatoren und Angriffs-informationen automatisch an das BSI gesendet werden

## Übersicht: § 31 Abs. 3 Nr. 1 und 2 BSIG

### Entwurf § 31 BSIG *(Stand 21.05.2026)*

(3) Betreiber kritischer Anlagen sind verpflichtet, […] folgendes **an das Bundesamt automatisiert zu übermitteln**:

1. **kontinuierlich Verfügbarkeitsindikatoren der** informationstechnischen **Systeme, Komponenten** und **Prozesse,** die für die **Funktionsfähigkeit** der von ihnen betriebenen **kritischen Anlagen maßgeblich** sind, und

2. **Indikatoren** zu **tatsächlichen** und **potentiellen Angriffen** sowie **Informationen zu Schwachstellen**, die in Systemen zur Angriffserkennung nach Absatz 2 **zu erheblichen Bedrohungen, Störungen oder Beeinträchtigungen** der Sicherheit in der Informationstechnik anfallen

### Zusammenfassung

**Heartbeat**
§ 31
Abs. 3
Nr. 1

**Was wird an das BSI gesendet?**
Branchenspezifische Verfügbarkeitsindikatoren zu IT/OT-Infrastruktur

**Wie wird es an das BSI gesendet?**
Kontinuierlich und automatisiert nach Aggregation und Priorisierung

**Warum wird es an das BSI gesendet?**
Um allgemeine und branchenspezifische Echtzeit-Lagebilder zu erzeugen

**SzA-Infos**
§ 31
Abs. 3
Nr. 2

Detektion von Prepositioning, APT, Supply-Chain-Angriffen, Zero-Day Schwachstellen

**Was wird an das BSI gesendet?**
Ereignisdaten aus Systemen zur Angriffserkennung (SzA)

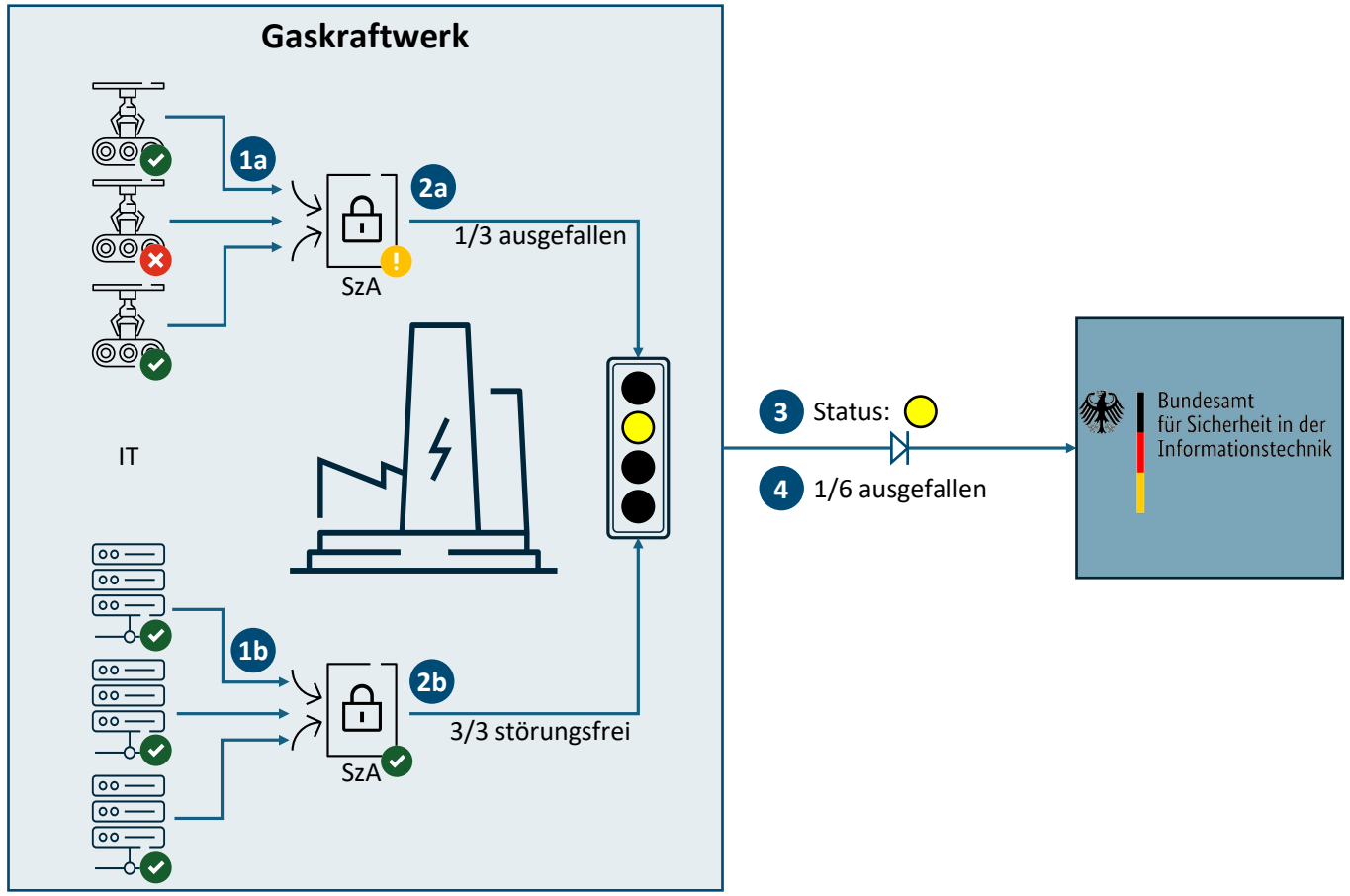
**Wie wird es an das BSI gesendet?**
Automatisiert und ereignisbezogen durch Filterregeln von Betreiber und BSI

**Warum wird es an das BSI gesendet?**
Erkennung von Deutschland- und branchenweiten Auffälligkeiten und Mustern

# Heartbeat beruht auf akkumulierten Indikatoren, die durch die KRITIS-Betreiber direkt an das BSI gesendet werden

Beispiel: § 31 Abs. 3 Nr. 1 BSIG

## Visualisierung




## Erläuterung

**1a** Im ersten Strang fällt eine von drei überwachten Komponenten spontan aus

**1b** Im zweiten Strang laufen alle drei IT-Komponenten störungsfrei

**2a** Das erste SzA detektiert den Ausfall und meldet eine Warnung (1/3 ausgefallen)

**2b** Das andere SzA meldet keine Auffälligkeiten (3/3 störungsfrei)

**3** Gelber Status an das BSI als Akkumulation von IT-Störung und IT-Normalzustand;

**4** *Optionaler Schritt: Information an BSI, dass 1/6 IT-Komponenten ausgefallen ist*

# Angriffsinformationen werden an das BSI gesendet, wobei die Filterung der Ereignisse über vom BSI geteilte Regeln stattfindet

## Vertiefung: § 31 Abs. 3 Nr. 2 BSIG

### Zentrales Verständnis



**SzA-Infos**
§ 31
Abs. 3
Nr. 2

- **Automatisierte Übertragung:** aus den SzA werden automatisch gefilterte und normalisierte Angriffsdaten an das BSI gesendet
- **BSI-Beschreibungen:** das BSI stellt technische Beschreibungen zur Ver-arbeitung von erheblichen Bedrohungen oder Beeinträchtigungen bereit
- **Sektorübergreifendes Lagebild:** mit den SzA-Infos bekommt das BSI ergänzend zum Meldewesen ein sektorübergreifendes Lagebild
- **Erweiterte Detektion:** BSI erkennt sektorübergreifende Angriffe, die bei einzelnen Betreibern unentdeckt blieben
- **Weiternutzung SzA:** Informationen können aus den verpflichtend vorhandenen SzA entnommen werden (Pflicht nach § 32 Abs. 2 BSIG)

**Beispiel:**
*Regionaler Verband von Wasserwerken betreibt Sensorik und SIEM-Systeme in den Wasserwerken und ist an ein Sektor-SOC angeschlossen*

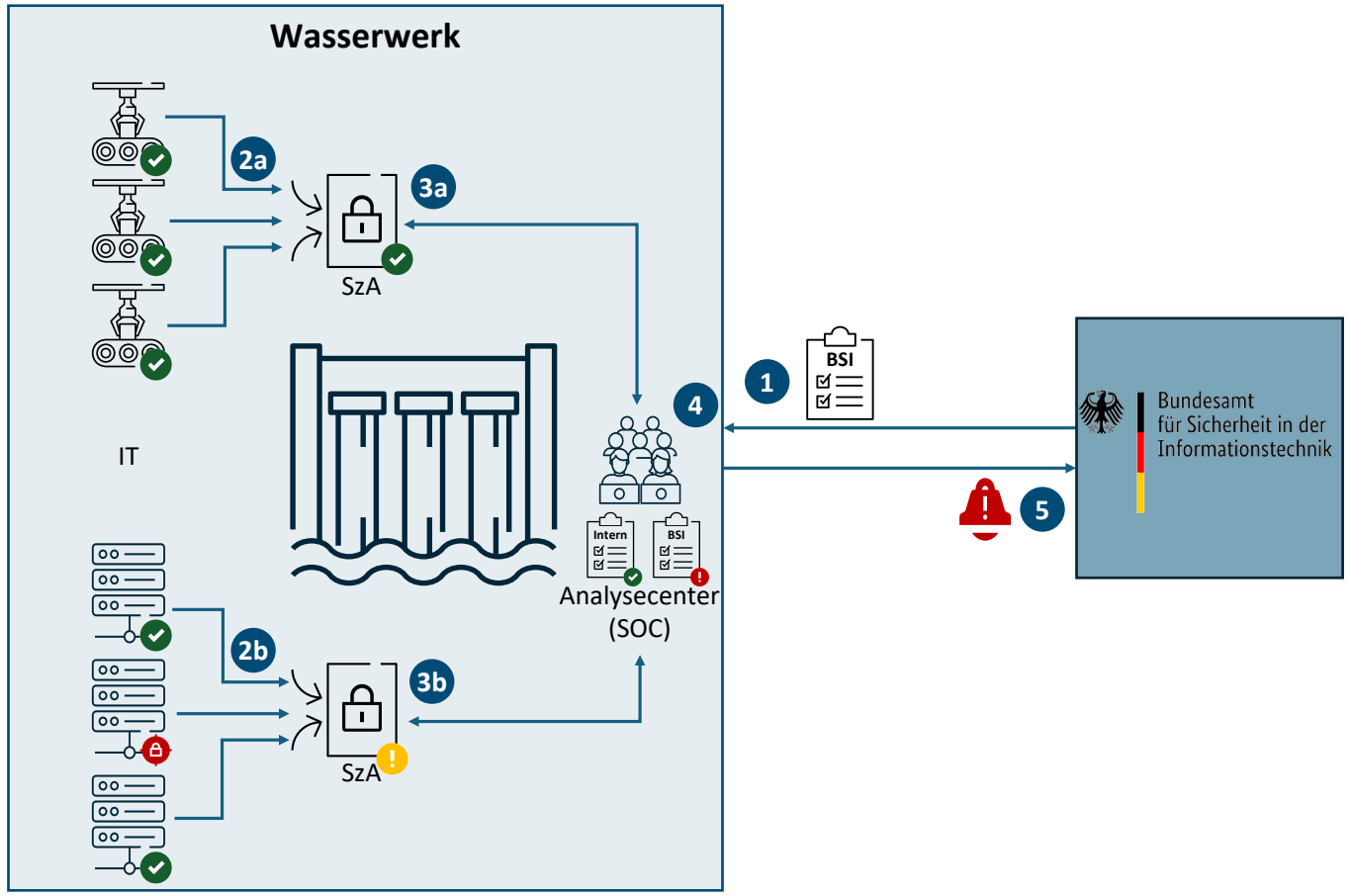
*Fall 1: Alarm von einer Betreiber-Regel im Sektor-SOC;*
*kleinere Betriebsstörung, daher keine Meldung an das BSI*

*Fall 2: Alarme einer BSI-Regel bei mehreren Wasserwerken;*
*Sektor-SOC leitet Alarm automatisch an das BSI weiter*

# Bei Unternehmen mit eigenem Analysecenter findet der Austausch der Angriffsinformationen direkt mit dem BSI statt

Beispiel: § 31 Abs. 3 Nr. 2 BSIG mit eigenem Analysecenter (SOC)

## Visualisierung



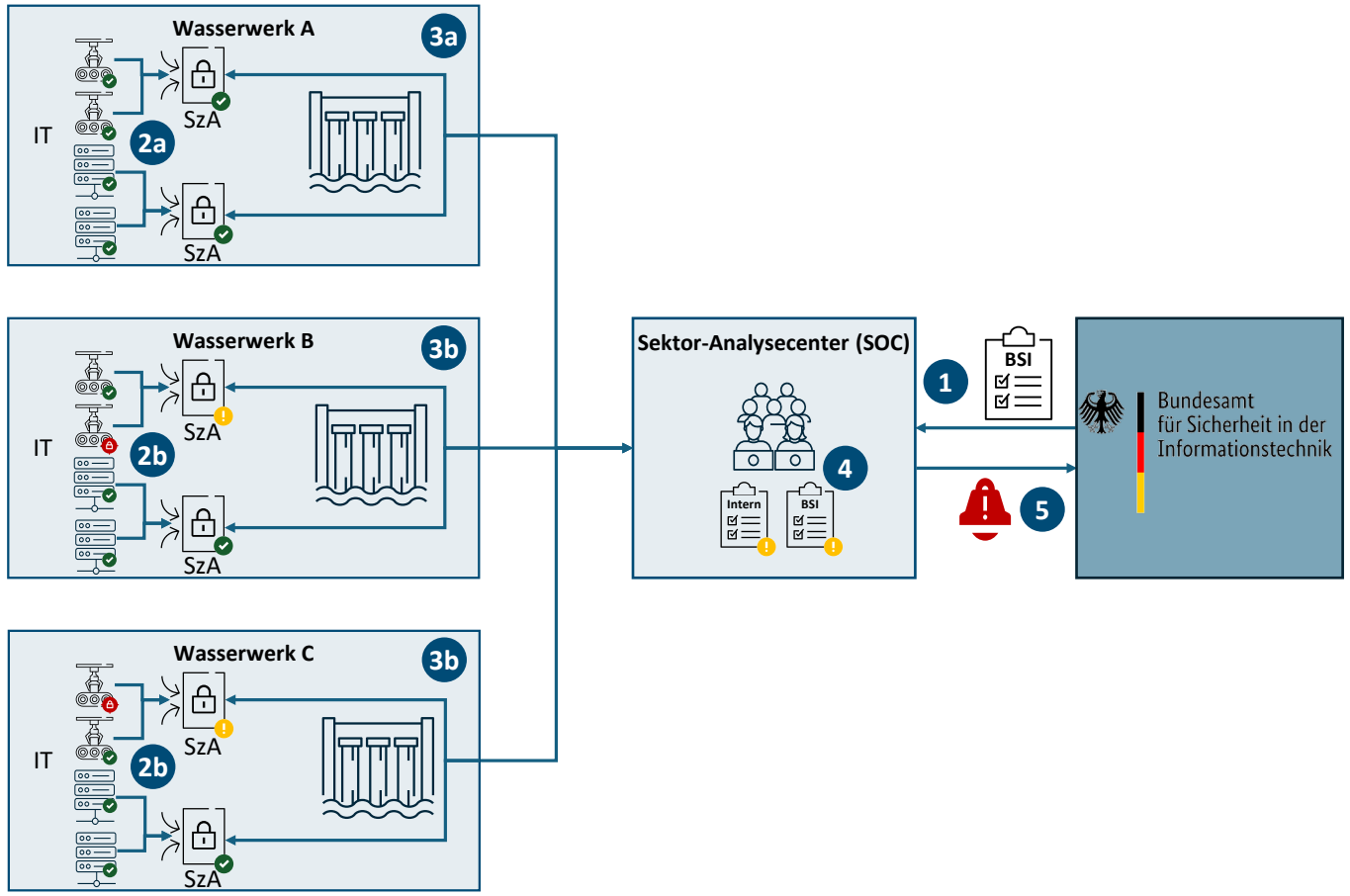

## Erläuterung

1. Das BSI stellt techn. Beschreibungen für das Analysecenter (SOC) bereit
2a. Im ersten Strang laufen alle Komponenten planmäßig
2b. Im zweiten Strang meldet eine der Komponenten einen Fehler
3a. Das SzA meldet keine Auffälligkeiten an das Analysecenter (SOC)
3b. Das SzA detektiert den Fehler und leitet diesen weiter
4. Im Analysecenter (SOC) schlägt eine der vom BSI übermittelten Regeln an
5. Das Analysecenter (SOC) übermittelt Alarm inkl. Angriffsinformationen an BSI

# Sind mehrere Unternehmen an ein Sektor-Analysecenter angeschlossen, sendet dieses Angriffsinformationen an das BSI

Beispiel: § 31 Abs. 3 Nr. 2 BSIG mit Sektor-Analysecenter (SOC)

## Visualisierung




## Erläuterung

1. Das BSI stellt techn. Beschreibungen für das Sektor-Analysecenter (SOC) bereit
2a. Die Systeme von Wasserwerk A melden keine Auffälligkeiten
2b. Einzelne IT-Komponenten von Wasserwerk B und C melden Fehler
3a. Die SzA von Wasserwerk A melden keine Auffälligkeiten
3b. Die SzA von Wasserwerk B und C erkennen die Fehler und leiten sie weiter
4. Im Sektor-Analysecenter (SOC) schlagen die internen und die BSI-Regeln an
5. Das Sektor-Analysecenter (SOC) sendet Alarm und Angriffsinformationen an BSI

# Der Cyberdome entfaltet seinen Mehrwert durch konkrete Use Cases – zwei exemplarische Anwendungsfälle

Use Case Überblick

## 1. Schwachstellenscans externer Systeme

Der Use Case schafft ein **integriertes Echtzeit-Lagebild** zu **kritischen Schwachstellen**, **verknüpft Lageinformationen, Scans und Detektion** und macht Betroffenheit sowie Ausnutzung für BSI und Betreiber kritischer Infrastrukturen sichtbar.




## 2. Heartbeat-Meldung von KRITIS-Anlagen

Der Use Case schafft ein **Echtzeit-Lagebild** zur **Verfügbarkeit von KRITIS-Anlagen**, erkennt Ausfälle und Muster frühzeitig und ermöglicht **gezielte Warnungen** bei **potenziellen Kaskadeneffekten.**




Später soll es **50+ Use Cases** als Teil des Cyberdome geben

+ ...

# Pilot Deutschland Scan

# Der Deutschland-Scan ist der regelmäßige Fitness-Check, um die Sicherheit des deutschen Internets zu prüfen

## WAS IST DER DEUTSCHLAND-SCAN?

### Das steckt dahinter:

**Ein Sicherheits-Check des BSI**
Das BSI prüft regelmäßig, wie sicher das deutsche Internet ist, ähnlich einem Fitness-Check

**Monatlich und automatisiert**
Jeden Monat werden Millionen öffentlich erreichbarer Systeme im deutschen Internet überprüft

**Gesetzlich verankert[1]**
Der Scan ist gesetzlich geregelt; das BSI hat den Auftrag, das deutsche Internet sicherer zu machen

1) Rechtsgrundlagen: § 3 Abs. 1 Nr. 2 BSIG, § 7d BSIG, § 19 TDDDG

### Der Scan im Überblick:

**Rund 13 Millionen Systeme im Blick**
Der Scan erfasst aktuell etwa drei Viertel aller deutschen Internet-Adressen (.de-Domains)

**100 Millionen Prüfergebnisse pro Woche**
Aus diesen Daten entsteht ein Gesamtbild der Sicherheit des deutschen Internets

**Prüfung typischer Sicherheits-Einstellungen**
Untersucht werden zum Beispiel die Verschlüsselung von Webseiten und die Absender-Sicherheit von E-Mails

**Prüfung nur von außen**
Der Scan ist wie ein Blick in ein Schaufenster; er umgeht keine Sicherheitsbarrieren und testet keine Passwörter

**Bereits heute im Einsatz**
Der Scan läuft im Regelbetrieb, liefert laufend neue Ergebnisse und kann zeitliche Veränderungen feststellen


44

# Der Deutschland-Scan macht das Internet sicherer und schützt damit alle, die es nutzen

## WARUM SCANNEN WIR?

**Diese Fragen beantwortet der Deutschland-Scan:**

- Wie „fit“ ist das deutsche Internet insgesamt?
- Wie viele Webseiten nutzen verschlüsselte Verbindungen?
- Wie viele E-Mail-Server setzen sichere Verschlüsselung ein?
- Wie schnell werden Sicherheits-Updates eingespielt?
- Wie ernst nehmen Betreiber die Sicherheit ihrer Seiten?

**Was Bürgerinnen und Bürger davon haben:**

**Schwachstellen werden entdeckt**
Angreifbare Systeme fallen auf, bevor Angreifer sie ausnutzen und Schäden entstehen

**Betroffene werden gewarnt**
Das BSI informiert Betreiber gezielt über gefundene Lücken, damit diese schnell geschlossen werden

**Systeme werden sicherer**
Mehr Sicherheit im Alltag, ob Online-Banking, Behördengang oder E-Mail

Vorbeugen statt reagieren – das ist der Kern des Deutschland-Scans

# Der Deutschland-Scan arbeitet in drei Schritten: Scannen – Erkennen – Warnen

## WIE FUNKTIONIERT DER SCAN?



### 1. Scannen
in der Breite

Das BSI-Werkzeug „KATTI“ besucht automatisiert öffentlich erreichbare Webseiten und Systeme – ohne Sicherheitsbarrieren zu umgehen.

Geprüft wird, ob Systeme dem Stand der Technik entsprechen.



### 2. Erkennen
in der Tiefe

Bei neu bekannten Schwach-stellen prüft das BSI genauer nach: Ist ein System betroffen? Und wenn ja: wie?

Grundlage ist dabei der Breitenscan aus Schritt 1.



### 3. Warnen
der Betreiber

Findet der Scan eine Auffälligkeit, warnt das BSI die betroffenen Betreiber, damit sie die Lücke schließen können.

Kontakt erfolgt bevorzugt über die security.txt der Webseite.

# Gemeinsam sicherer: Die Mitwirkung der Betreiber und der Ausbau des Scans machen das deutsche Internet sicherer

## WIE GEHT ES WEITER?

### So können Betreiber die Wirkung stärken:



**Domains und IP-Adressen ans BSI melden**
Unternehmen und andere Betreiber können ihre öffentlichen Systeme aktiv beim BSI hinterlegen. So erreicht eine Warnung schneller die richtige Stelle.
Für NIS-2-Unternehmen ist diese Meldung Pflicht. Für alle anderen ist sie freiwillig, aber sehr hilfreich.

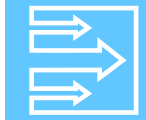


**security.txt auf Webseiten hinterlegen**
Die security.txt ist eine kleine Standard-Kontaktdatei (nach RFC 9116), die einem Sicherheitsteam sagt, wen es im Ernstfall kontaktieren soll.
Aktueller Stand: Nur 1,8 % der geprüften Domains haben eine security.txt hinterlegt.

### Was das BSI plant:



**Kooperation mit dt. Cloudprovider**
Gemeinsam mit Cloudprovider wird der Deutschland-Scan technisch weiter ausgebaut: Künftig soll er alle zwei Wochen laufen statt monatlich.
So werden neue Schwachstellen schneller entdeckt und Betreiber früher gewarnt.



**Neue Erfassungs- und Auswertungsverfahren**
Das BSI baut sein Werkzeug KATTI weiter aus, z. B., um ab 2027 auch die Verbreitung bestimmter Produkte im deutschen Internet messen zu können.
So wird das Lagebild der IT-Sicherheit in Deutschland noch aussagekräftiger.

Gemeinsam machen wir das deutsche Internet sicherer und widerstandsfähiger – Schritt für Schritt.


47

# Ziel: Deutschland gemeinsam schützen

## A Wirksam skalieren

- **(Teil-)automatisierung** als strategisches Prinzip zur breiten Skalierung
- Fähigkeiten und Prozesse **systematisch industrialisieren**
- Erkenntnisse **schneller** erfassen, auswerten und nutzbar machen

+

## Gemeinsam handeln B

- **Silos abbauen** und Akteure in einem gemeinsamen Analyseverbund verbinden
- Partner aus **allen Stakeholdergruppen** koordiniert zusammenbringen
- **Zusammenarbeit** über Ebenen, Zuständigkeiten und Organisationen hinweg

## Gemeinsam Deutschland schützen

# Das geht nur zusammen

Jens Wiesner

Referatsleiter
Industrielle Steuerungs- und Automatisierungssysteme

jens.wiesner@bsi.bund.de

www.bsi.bund.de/ics

Bundesamt
für Sicherheit in der
Informationstechnik

Follow us:

Bild: © AdobeStock/Nirut