PHYSEC
SECURITY FOR THINGS

Von Regulierung zu Resilienz:
CRA, CER und die Zukunft cyber-physischer Sicherheit

Prof. Dr. Christian Zenger

Bochum, Juni 2026

TLP:CLEAR

www.physec.de

Meet our CEO

Prof. Dr. Christian Zenger

Co-Gründer und Geschäftsführer

Seine Vision: Mit PHYSEC ein vertrauensvolles Internet der Dinge (IoT) realisieren und Bochum als führenden Standort für IT und IT-Sicherheit stärker in den Fokus rücken

- Gründer und Geschäftsführer der PHYSEC GmbH
- Professor an der Ruhr Universität Bochum und Teil des Vorstands des Horst-Görtz-Instituts für IT-Sicherheit
- Promotion (s.c.l.) auf dem Gebiet der Physical Layer Security für IoT an der Ruhr-Universität Bochum
- Co-Autor des CASA-Excellence Clusters
- NRW-Innovationspreisträger 2024
- MIT Innovator under 35
- Preisträger des deutschen IT-Sicherheitspreises
- Nominierter für den deutschen Zukunftspreis

TLP:CLEAR

PHYSEC

Wie groß ist ein µController?

µController

CMOS
140 nm

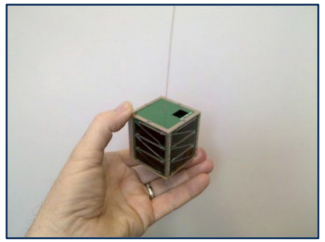
CMOS
40 nm

TLP:CLEAR

PHYSEC

Wo stecken µController drin?

Jedes Objekt – oder „Ding“ –, das über Funk mit einem Internet-Netzwerk verbunden werden kann

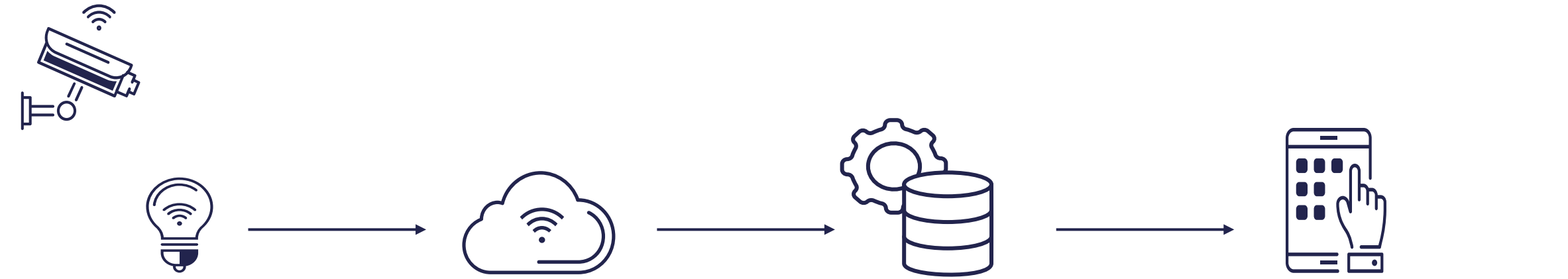


TLP:CLEAR

PHYSEC

Wie funktioniert das Internet der Dinge (IoT)?

Nahtlose Integration zwischen Technologie und dem Erleben des Menschen



TLP:CLEAR

PHYSEC

Klassische IT vs. IoT Verbindungen

73 Zettabyte*
= 73 Billionen Gigabyte

= 5.000 Diskettenstapel bis zum Mond und zurück

* IDC, https://dataprot.net/statistics/iot-statistics/:~:text=In%202021,%20there%20were%20more,to%20the%20internet%20per%20minute.

TLP:CLEAR

PHYSEC

Warum digitalisieren wir?

Umsatzpotenzial

Beispiele:

- Pay-per-Use / Equipment-as-a-Service
- Datenbasierte Zusatzservices
- ...

Kosteneinsparung

Beispiele:

- Predictive Maintenance
- Energieoptimierung durch Digital Twin
- ...

Verbesserte Nutzererfahrung

Beispiele:

- AR-gestützte Instandhaltung
- Mobile HMI / Dashboards
- ...

Remote Access Operations

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY — AMERICA'S CYBER DEFENSE AGENCY

BLOG

The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years

Released: May 07, 2023

Jen Easterly, CISA Director

STATEMENTS & RELEASES

Statement from the Press Secretary

FOREIGN POLICY | Issued on: February 15, 2018

In June 2017, the Russian military launched the most destructive and costly
attack in history.

BBC | Sign in | Home | News | Sport | Earth | Reel

NEWS

Home | Israel-Gaza war | War in Ukraine | Climate | Video | World | UK | Business | Tech | Science

Tech

Ukraine power cut 'was cyber-attack'

11 January 2017

npr — NEWSLETTERS | SIGN IN | NPR SHOP

NEWS | CULTURE | MUSIC | PODCASTS & SHOWS | SEARCH

BUSINESS

Flights were grounded across the U.S. as the FAA scrambled to fix a system outage

JANUARY 12, 2023 · 7:13 AM ET

HEARD ON MORNING EDITION

3-Minute Listen | + PLAYLIST

President Biden ordered an investigation into what happened. NPR's Dwane Brown talks to Leslie Josephs, an airline reporter with CNBC, about theissue with a pre-flight safety notification system.

BBC | BBC iD | Menu

NEWS

Home | Video | World | US & Canada | UK | Business | Tech | Science | Magazine | Ent

World | Africa | Asia | Australia | Europe | Latin America | Middle East

Stuxnet worm hits Iran nuclear plant staff computers

26 September 2010 | Middle East | Share

, causing billions o
lt was part of the
strates ever more
was also a reckless
onal consequences

WIRED — SECURITY | POLITICS | GEAR | BACKCHANNEL | BUSINESS | SCIENCE | CULTURE | IDEAS | MERCH

ANDY GREENBERG — SECURITY — JUN 20, 2017 6:00 AM

How an Entire Nation Became Russia's Test Lab for Cyberwar

Blackouts in Ukraine were just a trial run. Russian hackers are learning to sabotage infrastructure—and the US could be next.

ILLUSTRATION: CURT MERLO

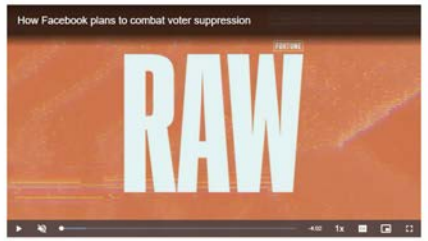
SEARCH — FORTUNE — Subscribe Now — SIGN IN

Home | News | Tech | Finance | Leadership | Well | Recommends | Fortune 500

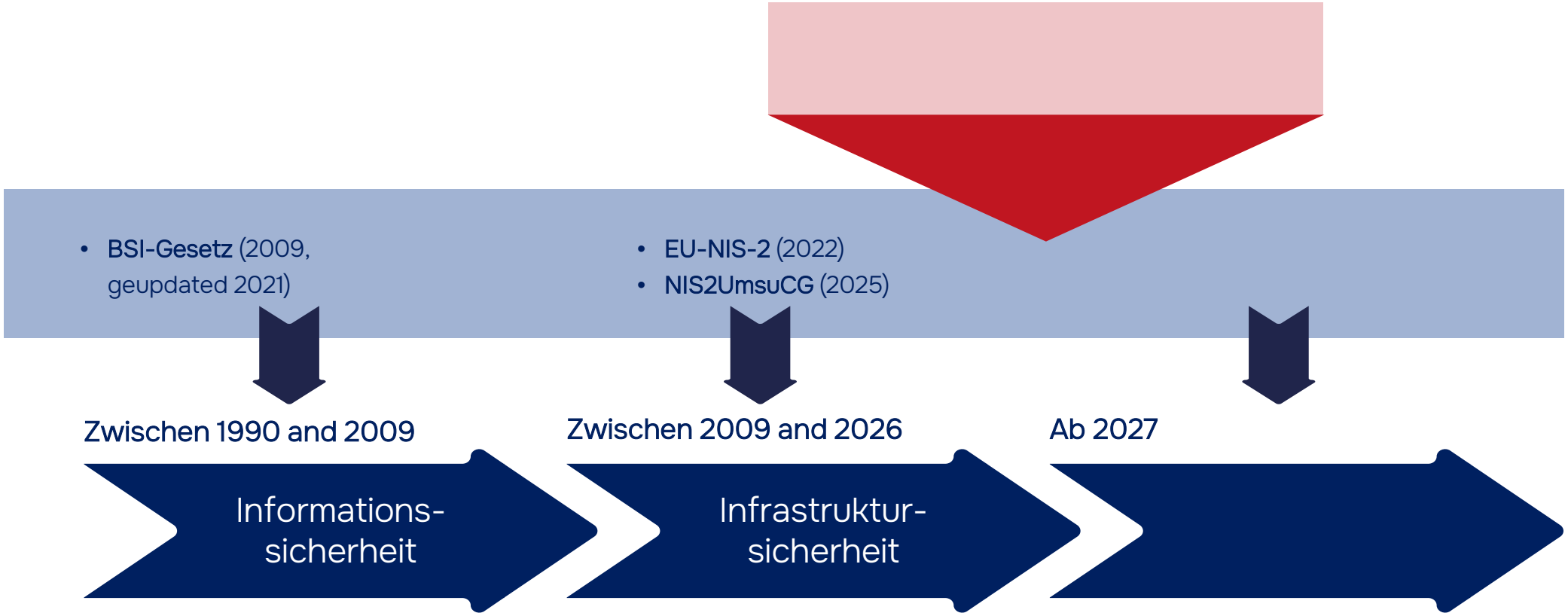
TECH - VOTERS AND VOTING

Voting software in some states is vulnerable to hacking, U.S. cyber agency says

BY KATE BRUMBACK AND THE ASSOCIATED PRESS



Cybersecurity Regulation History



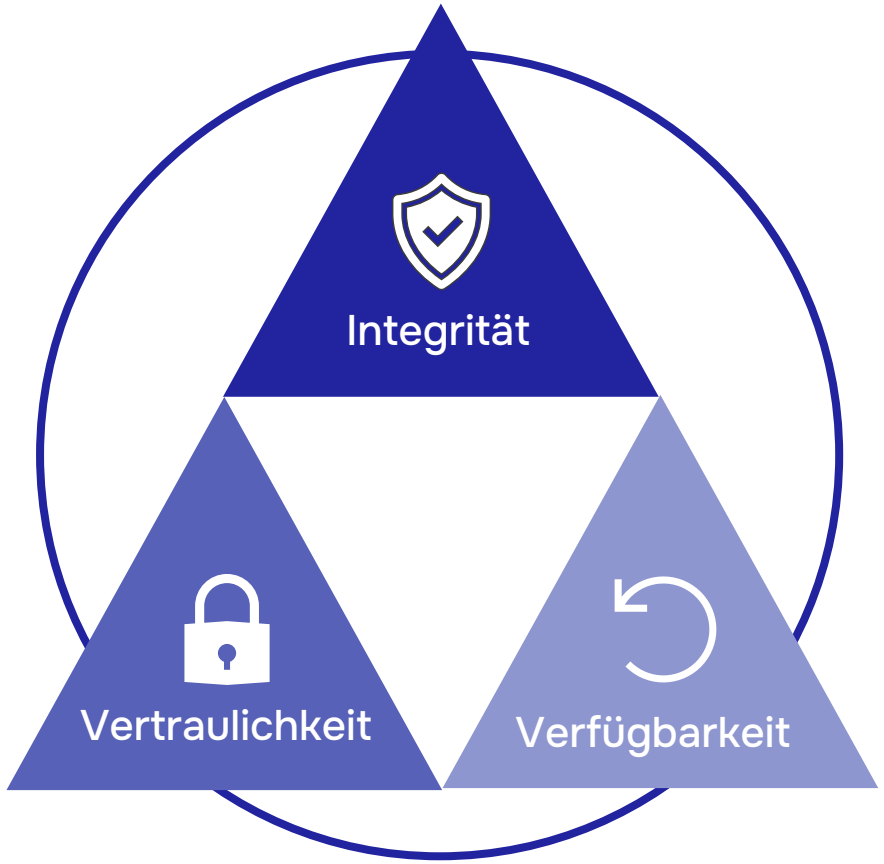
TLP:CLEAR

PHYSEC

Schutzziele der Cyber-Sicherheit

Vertraulichkeit, Integrität und Verfügbarkeit

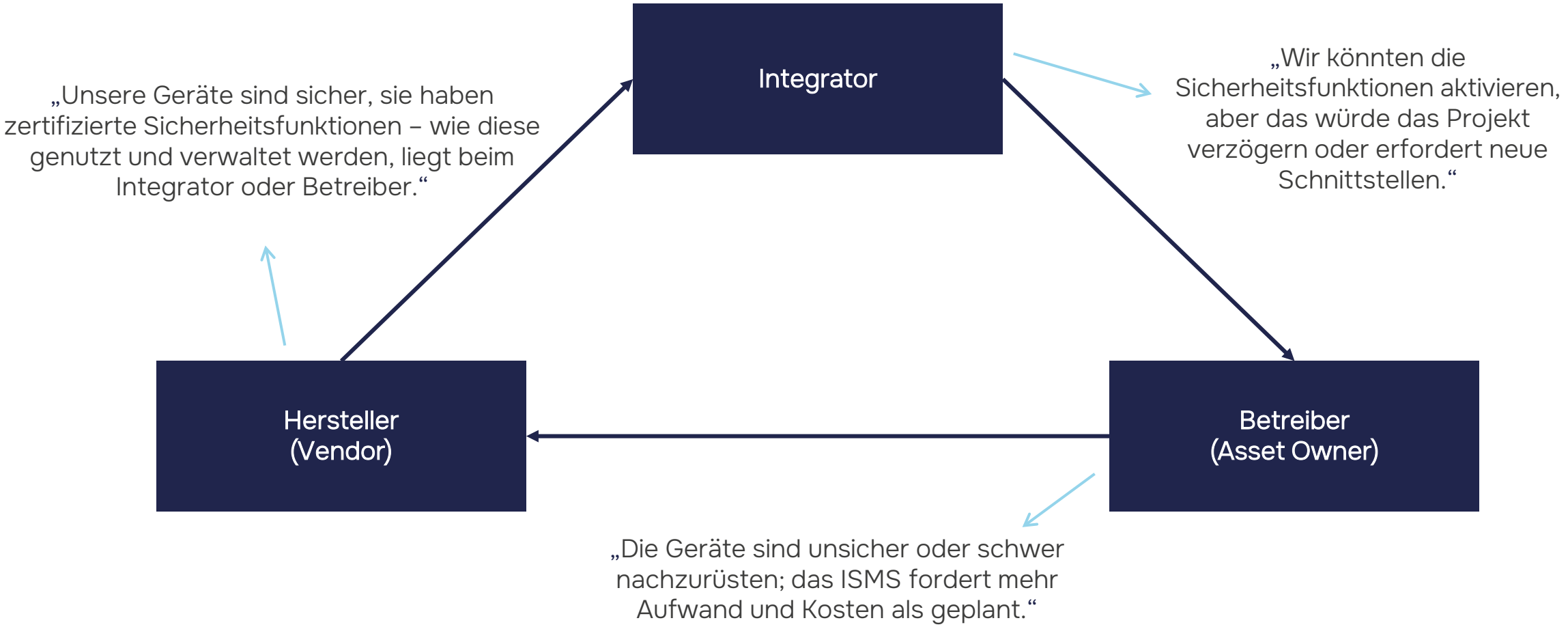
- **Vertraulichkeit**: Die Informationen sind vor Offenlegung geschützt.
- **Integrität**: Die Informationen sind vor versehentlicher oder absichtlicher Änderung oder Veränderung geschützt.
- **Verfügbarkeit**: Die Informationen stehen autorisierten Benutzern bei Bedarf zur Verfügung.



TLP:CLEAR

PHYSEC

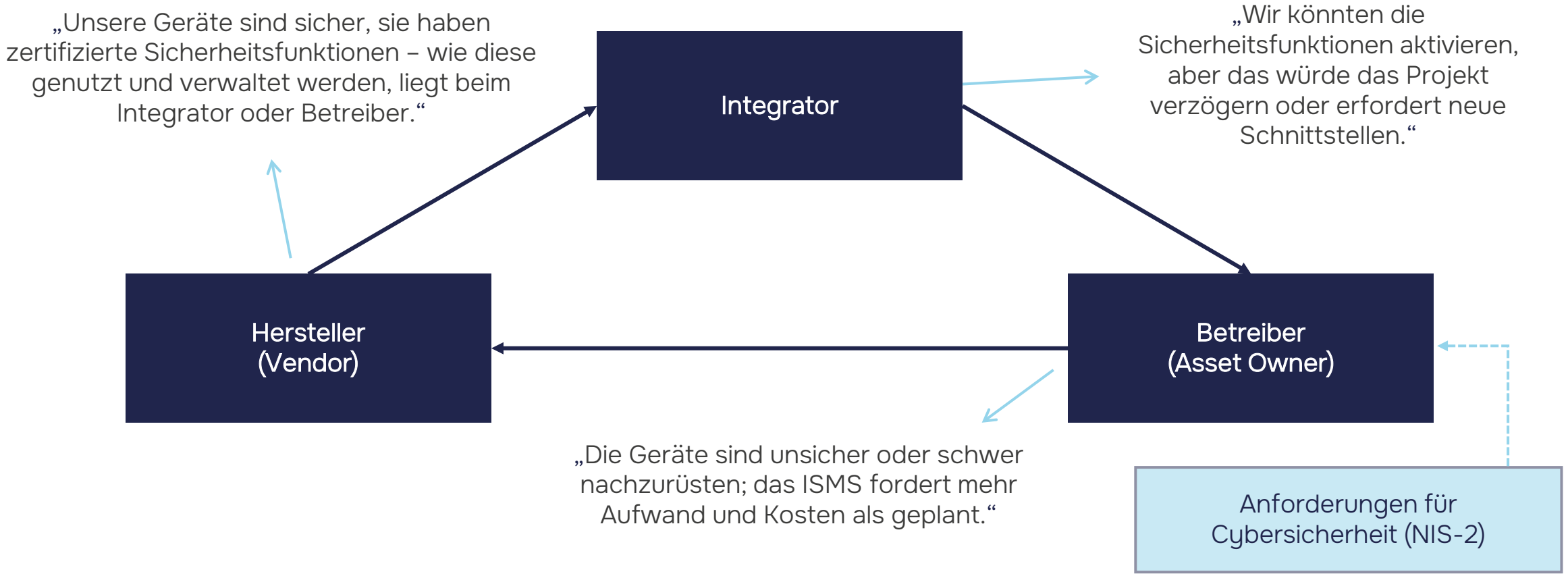
Zirkuläre Verschiebung der Verantwortung



TLP:CLEAR

PHYSEC

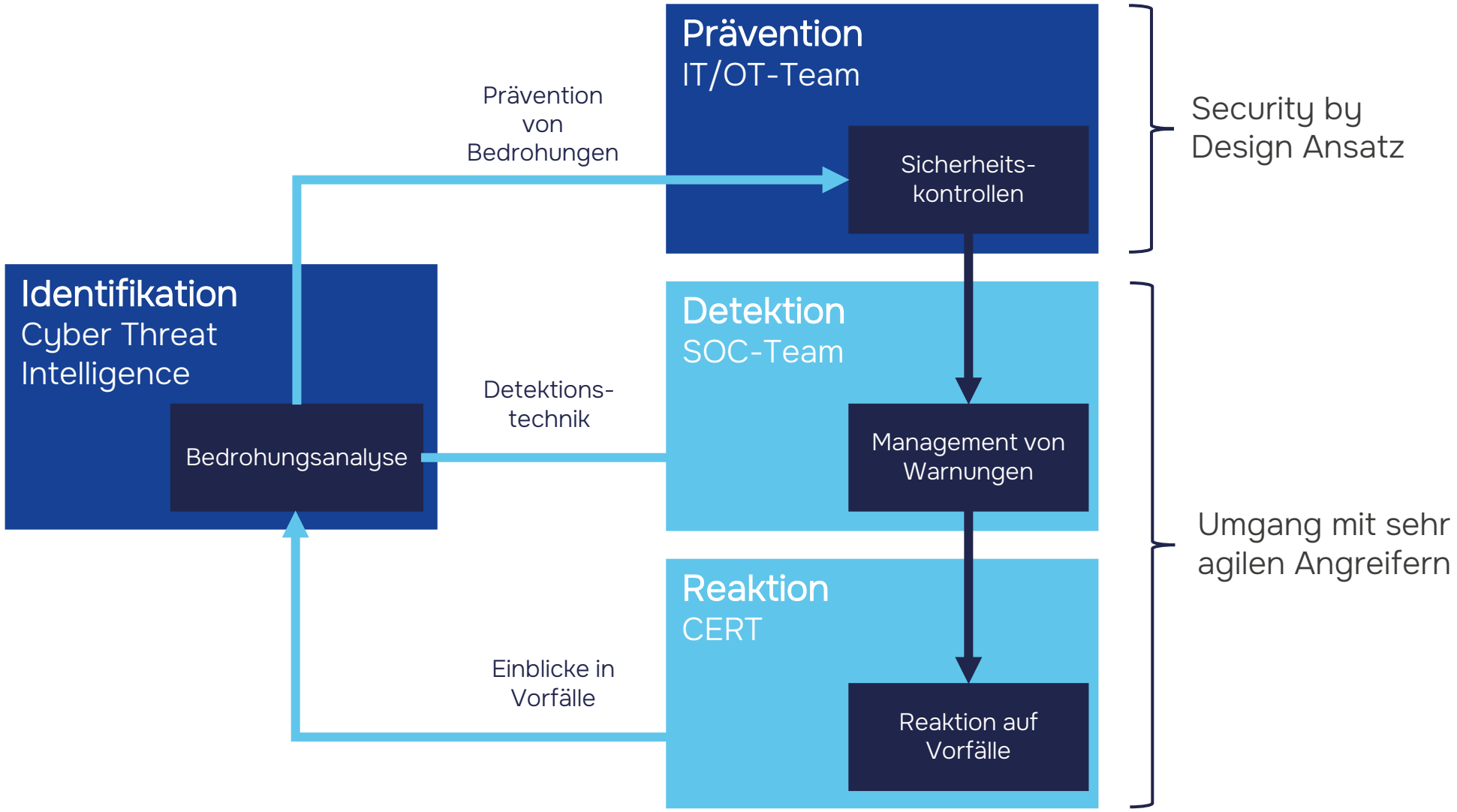
Zirkuläre Verschiebung der Verantwortung



TLP:CLEAR

PHYSEC

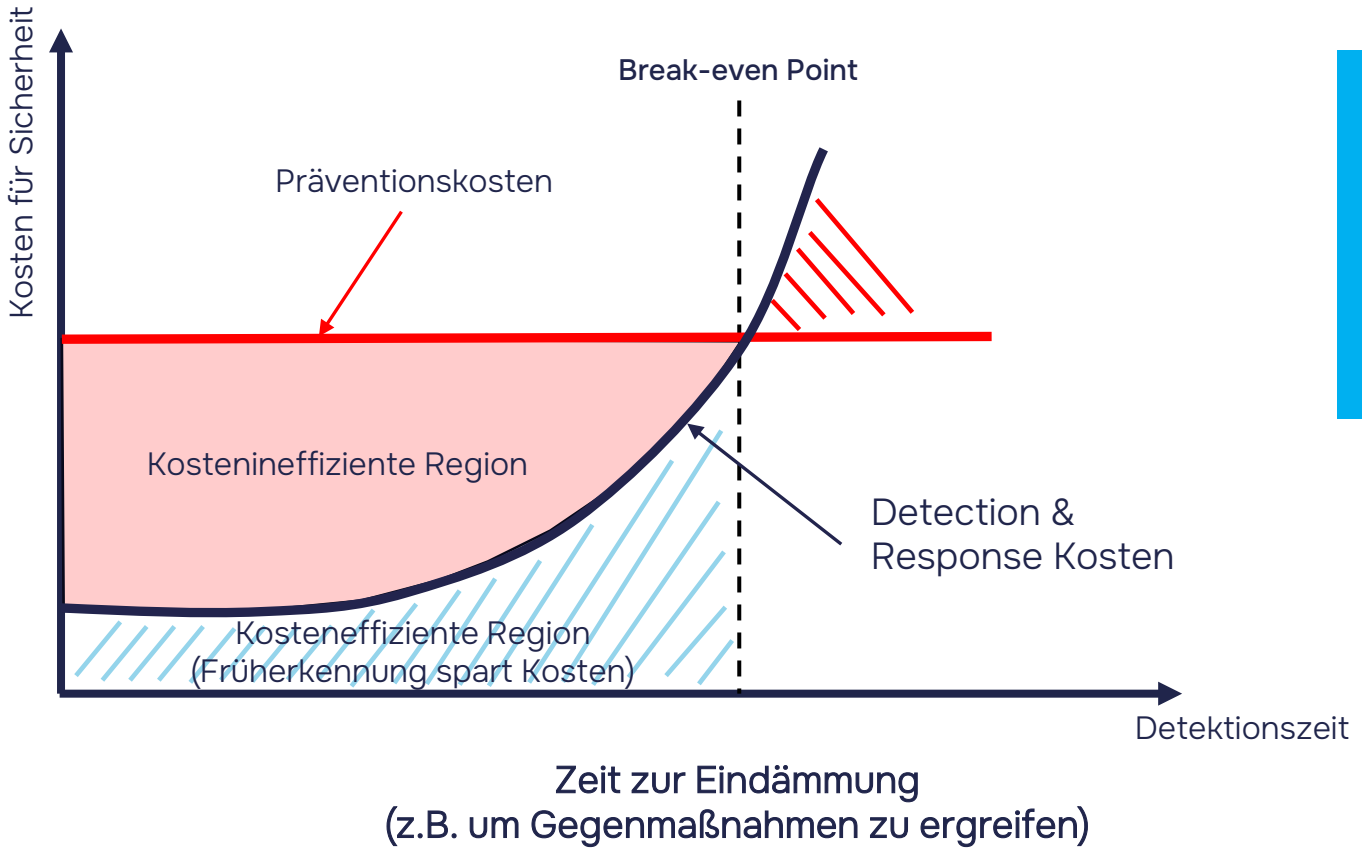
Die vier Blöcke der Informationssicherheit



TLP:CLEAR

PHYSEC

Kosten-Nutzen-Vergleich: Detection & Response vs. Prävention



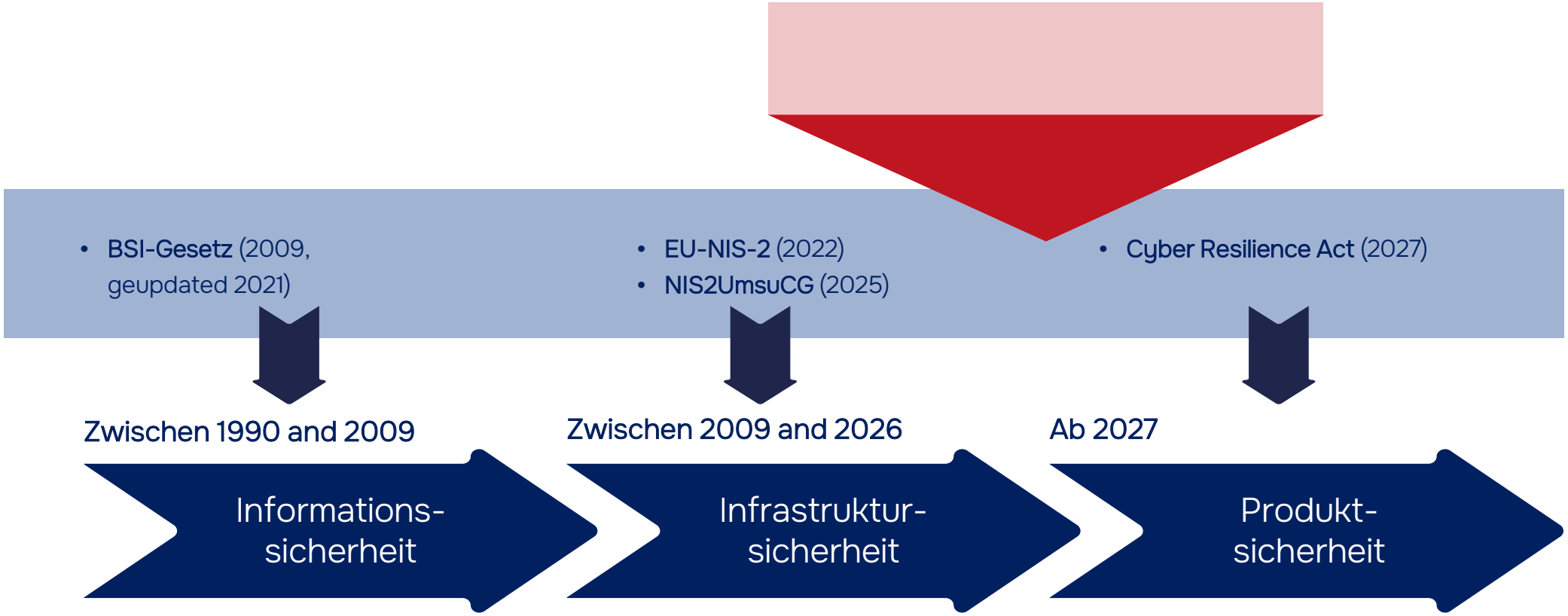
Detection & Response ist nur ökonomischer als Prävention, solange Angriffe frühzeitig erkannt werden (Break-even Point lag früher <200 Tage, heute <11 Tage).“

Quelle: https://www.physec.de/blog/artikel/konvergente-sicherheitssysteme/ https://www.ibm.com/reports/data-breach

TLP:CLEAR

PHYSEC

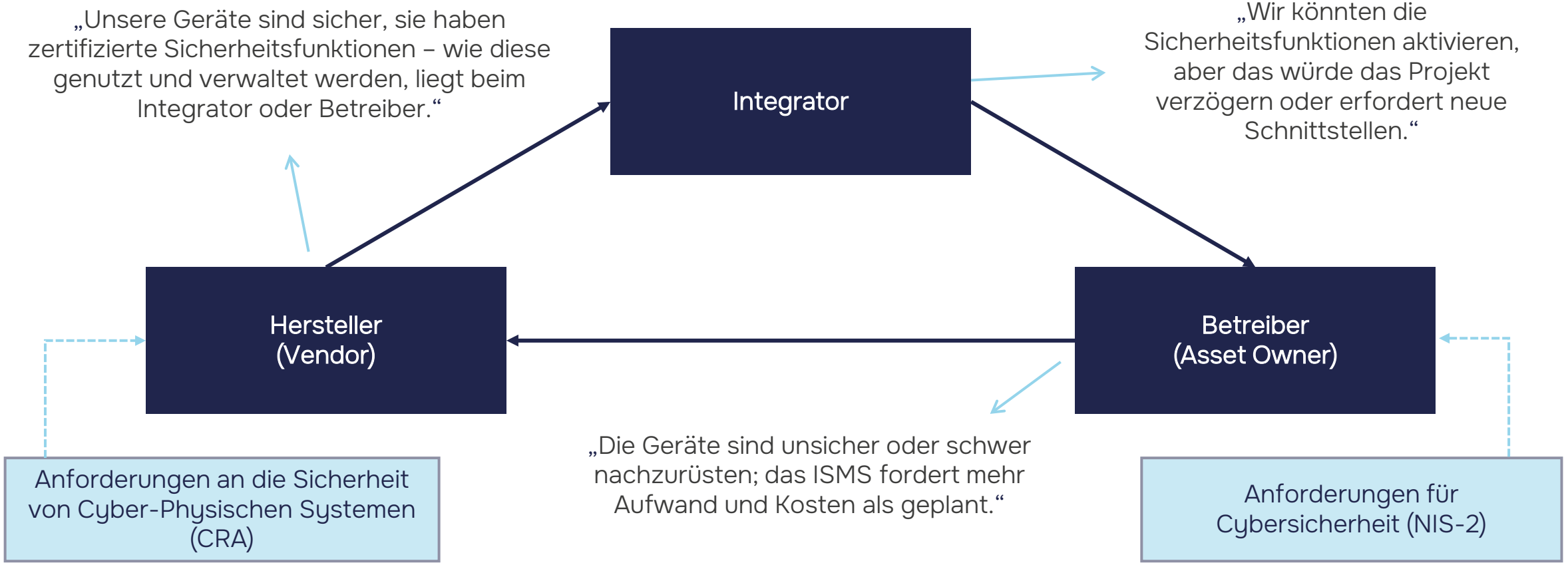
Cybersecurity Regulation History



TLP:CLEAR

PHYSEC

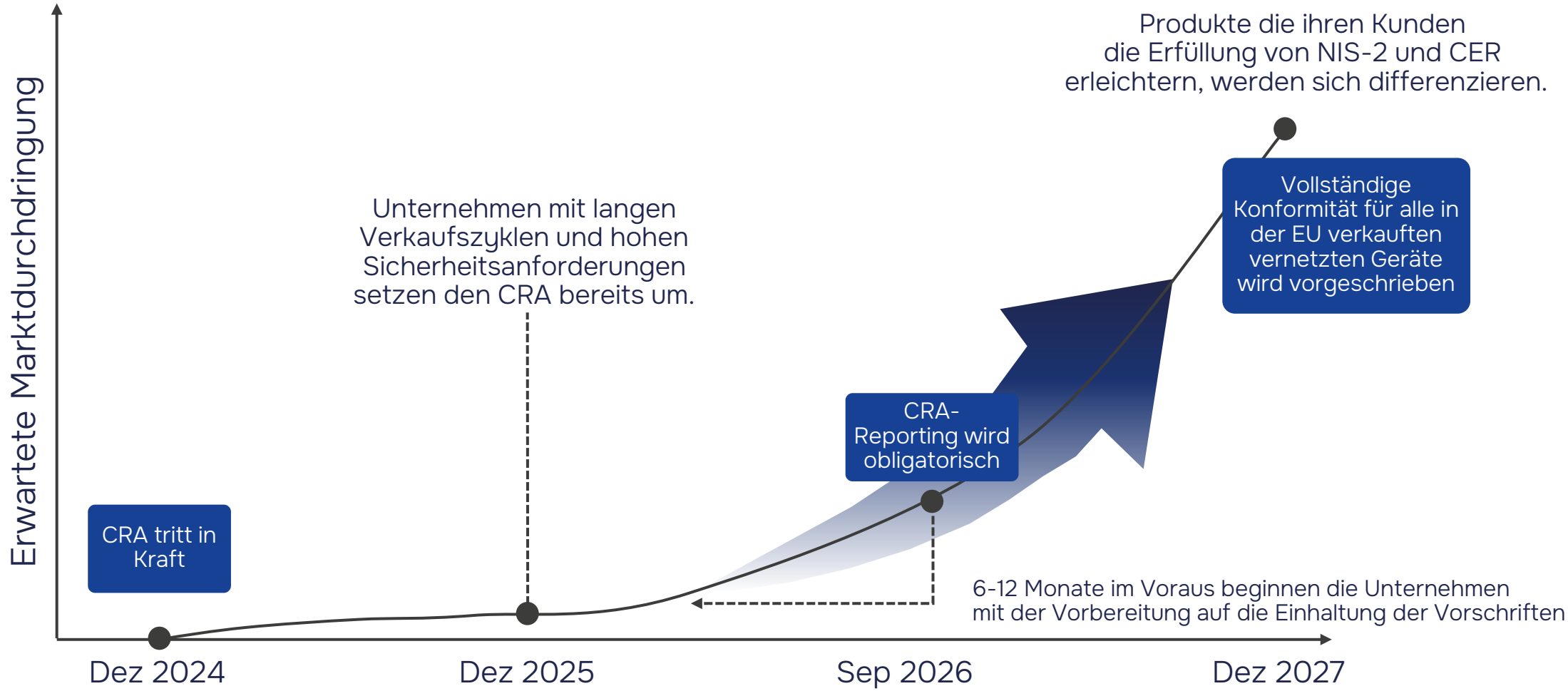
Zirkuläre Verschiebung der Verantwortung



TLP:CLEAR

PHYSEC

Neue CRA-konforme Produkte die ihren Kunden die Erfüllung von NIS-2 und CER erleichtern, werden sich differenzieren.



TLP:CLEAR

PHYSEC

CRA legt verbindliche Sicherheitsanforderungen fest

- Die Einhaltung der CRA-Vorschriften konzentriert sich auf spezifische technische Anforderungen und nicht auf ganzheitliche Sicherheit.
- Isolierte Sicherheit für ein Gerät reicht nicht aus, da es in einem unsicheren Ökosystem (z. B. nicht vertrauenswürdige Gateways oder kompromittierte Netzwerkserver) oder in nicht vertrauenswürdigen Umgebungen betrieben werden kann.

Cybersicherheit muss in der Planungs-, Entwurfs-, Entwicklungs-, Produktions-, Liefer-, & Wartungsphase berücksichtigt werden.

Cybersicherheitsrisiken müssen dokumentiert sein.

Aktiv ausgenutzte Schwachstellen und Zwischenfälle müssen gemeldet werden.

Während der Dauer des Supportzeitraums müssen Schwachstellen wirksam behandelt werden.

Sicherheitsupdates müssen für die voraussichtliche Nutzungsdauer zur Verfügung gestellt werden.

Klare und verständliche Bedienungsanweisungen müssen verfügbar sein.

Vom Cyber Resilience Act geforderte Dokumente

1. **EU-Konformitätserklärung** (öffentlich)

Soll die Konformität formal erklären.

2. Informationen & Anleitungen für den Benutzer *(dem Produkt beigefügt)*

Soll dem Benutzer helfen, das Produkt sicher zu nutzen.

- Verwendungszweck & wesentliche Funktionen
- Sicherheitseigenschaften & Sicherheitsumfeld
- Vorhersehbare missbräuchliche Verwendung, die zu Sicherheitsrisiken führt
- Notwendige Maßnahmen für sichere Nutzung

3. **Technische Dokumentation** *(i.d.R. nicht öffentlich)*

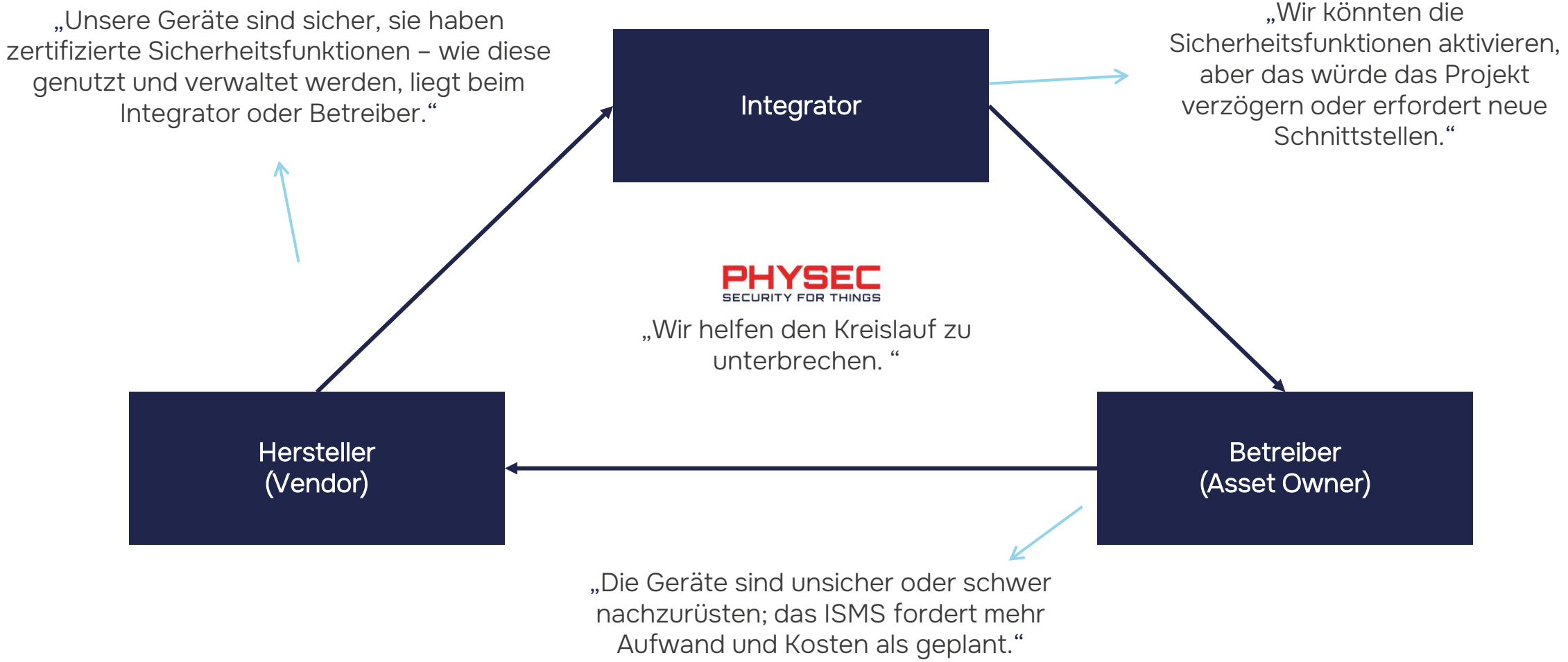
Soll die Konformität nachweisen.

- Beschreibung & Verwendungszweck
- Entwurfsinformationen
- Dokumentation des Schwachstellen-Managementprozesses
- Bewertung der Cybersicherheitsrisiken
- Liste der angewandten harmonisierten Normen
- Testberichte aus Konformitätsbewertungsverfahren
- Dokumentation zur Bestimmung des Unterstützungszeitraums
- Software Bill of Materials (SBOM)

TLP:CLEAR

PHYSEC

Zirkuläre Verschiebung der Verantwortung

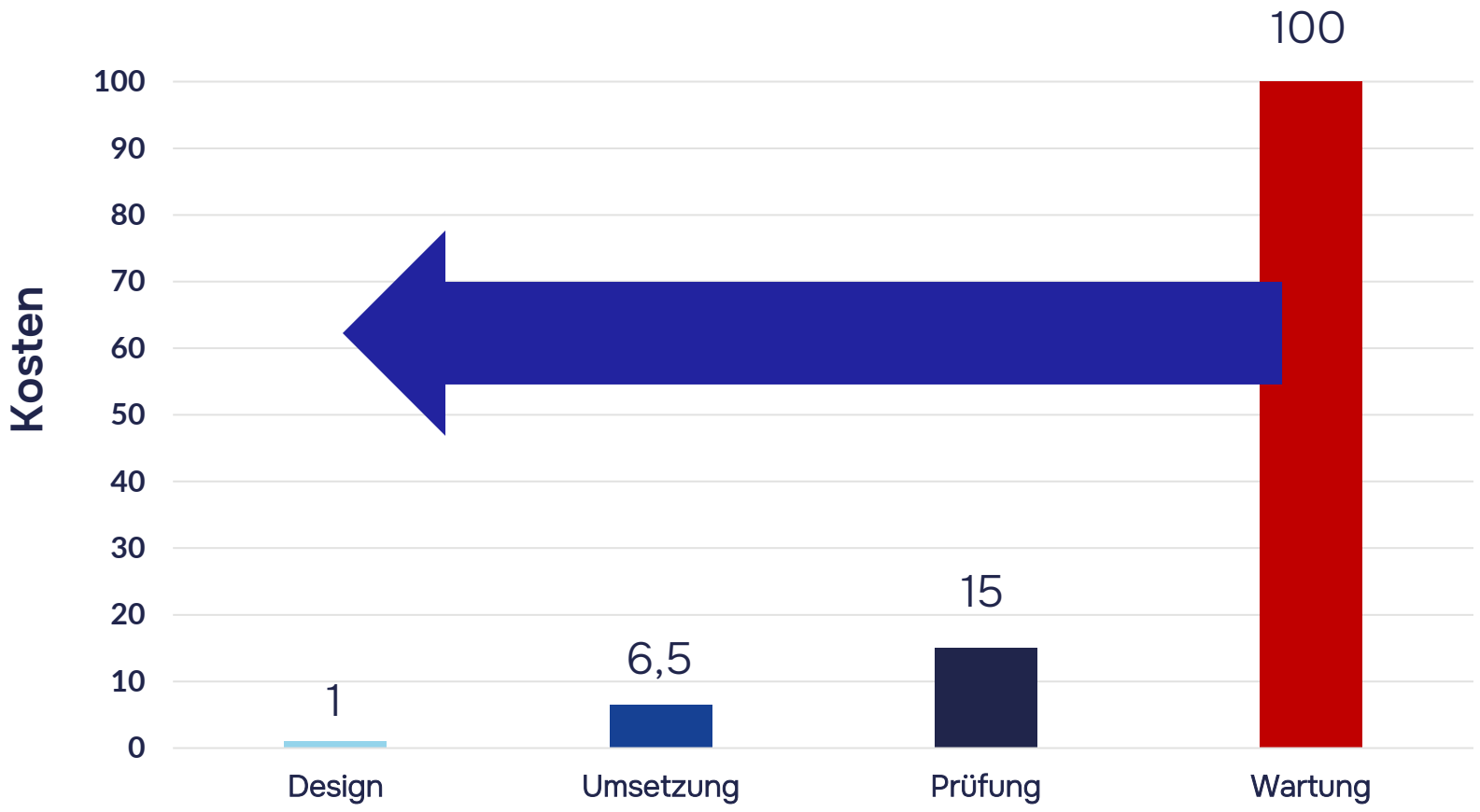


TLP:CLEAR

PHYSEC

Relative Kosten für das Beheben von Defekten

Durch verpflichtendem „Security by Design“ werden die Systemkosten sinken



Quelle: IBM System Science Institute, Relative Cost of Fixing Defects, 1983.

TLP:CLEAR

PHYSEC

Close Access Operations

Bundesamt für Verfassungsschutz

Bundesamt für Verfassungsschutz
75 Jahre
IM AUFTRAG DER DEMOKRATIE

Hinweis geben

VERFASSUNGSSCHUTZ

Startseite › Themen › Spionage- und Proliferationsabwehr › Gefährdungen durch russische Spionage, Sabotage und Desinfo

Gefährdungen durch russische Spionage, Sabotage und Desinformation

Bild: picture alliance/dpa | Patrick Pleul DOWNLOAD (MP3, 25 MB)

Newsjunkies

Nach Tesla-Brandanschlag: Wie gefährdet ist die kritische Infrastruktur?

Wie anfällig sind Stromnetze, Bahntrassen und Datenkabel für Sabotage und Auswirkungen von Extremereignissen? Wie steht es um die Sicherheit der kritischen Infrastruktur in Deutschland? Seit dem Brandanschlag auf die Stromversorgung von Tesla vor rund zwei Wochen ist der Druck unter anderem auf die Politik gestiegen, die Gesetze zu verschärfen. Auch das Bundeskriminalamt und das Bundesamt für Sicherheit in der Informationstechnik

Wie gut sind Häfen und Schleusen in SH vor Sabotage geschützt?

Stand: 11.10.2022 19:08 Uhr

Seit der Sabotage wichtiger Bahn-Kabel ist klar, wie anfällig die Infrastruktur für Anschläge sein kann. Doch nicht nur die Bahn kann es treffen. Experten warnen, dass auch die maritime Struktur zum Ziel werden könnte.

WIRTSCHAFT | DEUTSCHLAND

Warum braucht Deutschland eine neue Hafenstrategie?

Dirk Kaufmann
06.04.2024

Häfen gehören zur "kritischen Infrastruktur", sie müssen deshalb besonders geschützt werden - real und auch digital. Dazu entwickelt die Bundesregierung eine Hafenstrategie, die das Konzept von 2015 ersetzen soll.

Kritische Infrastruktur: Der größte deutsche Hafen in Hamburg

tagesschau

tagesschau24 live

Brandsätze in Luftfracht

Russischer Geheimdienst soll hinter Sabotage stecken

Stand: 23.04.2025 06:00 Uhr

WDR

Wetter | Verk

Nachrichten | Sport | Wissen | Verbraucher | Kultur | Unterha

…ler Bahn-Sabotage: Wie gut ist die kritisc… …ktur geschützt?

…10.2022, 17:05 Uhr

…undbar ist die kritische Infrastruktur bei uns? Seit den Lecks …ines Nord Stream 1 und 2 wird darüber diskutiert. Und die S… …i der Deutschen Bahn wirft nun neue Fragen auf.

…ittlerweile: Es gab zwei Tatorte bei der Sabotage gegen die E… …ige Kabel durchtrennt wurden - einen in Berlin und einen in… …g unklar ist dagegen, wer dahinter steckt.

Geheimdienste

"Der Ukrainekrieg ist hier längst angekommen"

21. Mai 2024, 13:07 Uhr | Lesezeit: 3 Min. | 31 Kommentare

Leitungen aller Art (hier als Beispiel eine Erdgasempfangsstation der Ferngasleitung Eugal in Lumin) sind ins Visier von Saboteuren geraten.
Stefan Sauer/DPA

Bauarbeiter finden ein Sprengstoffdepot nahe einer Nato-Pipeline in Rheinland-Pfalz - wer es angelegt hat, ist unklar. Aber deutsche und europäische Sicherheitsbehörden warnen schon länger davor, dass Russland auch vor Sabotage nicht zurückschrecke.

Christian Schaller

Spionage und Sabotage vor Europas Küsten – Kritische Infrastruktur im …adenkreuz

…ölkerrechtliche Spielräume für …bwehrmaßnahmen

…P-Studie 2024/S 08, 28.02.2024, 26 Seiten
…:10.18449/2024508

PROZESS IN STUTTGART

„Wegwerfagenten" vor Gericht – was steckt hinter dem Phänomen?

von Miriam Hollstein und Viktar Vasileuski 17. März 2026 • 06:10 Uhr • 5 Min.

TOP SECRET//COMINT//REL TO USA, FVEY

COTTONMOUTH-I

ANT Product Data

08/05/08

COTTONMOUTH - 1

…REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant … provide a wireless bridge into a target network as well as the ability to load exploit … onto target PCs.

…REL) CM-I will provide air-gap bridging, software persistence capability, "in-field" re-… mability, and covert communications with a host software implant over the USB. The … will enable command and data infiltration and exfiltration. CM-I will also communicate … ta Network Technologies (DNT) software (STRAITBIZARRE) through a covert … implemented on the USB, using this communication channel to pass commands and … ween hardware and software implants. CM-I will be a GENIE-compliant implant … CHIMNEYPOOL.

…REL) CM-I consists digital components (TRINITY), USB 1.1 FS hub, switches, and … RMONKEY (HM) RF Transceiver within the USB Series-A cable connector. … SIN is the version permanently connected to a USB keyboard. Another version can … e with an unmodified USB connector at the other end. CM-I has the ability to … icate to other CM devices over the RF link using an over-the-air protocol called … LATION.

Availability – January 2009 Unit Cost: 50 units: $1.015K

TOP SECRET//COMINT//REL TO USA, FVEY

Kritische Infrastrukturen

Energie
Elektrizität, Gas, Mineralöl, Fernwärme

Wasser
Öffentliche Wasserversorgung, öffentliche Abwasserbeseitigung

Ernährung
Ernährungswirtschaft, Lebensmittelhandel

Gesundheit
Medizinische Versorgung, Arzneimittel und Impfstoffe, Labore

IT und Telekommunikation
Rechenzentren, Infrastrukturen, Internet, Kommunikation

Medien und Kultur
Fernsehanstalten, Zeitungen, Radio

Transport und Verkehr
Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik

Finanz- und Versicherungswesen
Kreditinstitute, Börsen, Versicherungen, Finanzdienstleister

TLP:CLEAR

PHYSEC

The Problem: Trust Ends at the Edge of the Casing

Physical attacks on power grid rose by 71% last year, compared to 2021

By Nicole Sganga

February 22, 2023 / 1:49 PM EST / CBS News

CBS NEWS

PROZESS IN STUTTGART

„Wegwerfagenten“ vor Gericht – was steckt hinter dem Phänomen?

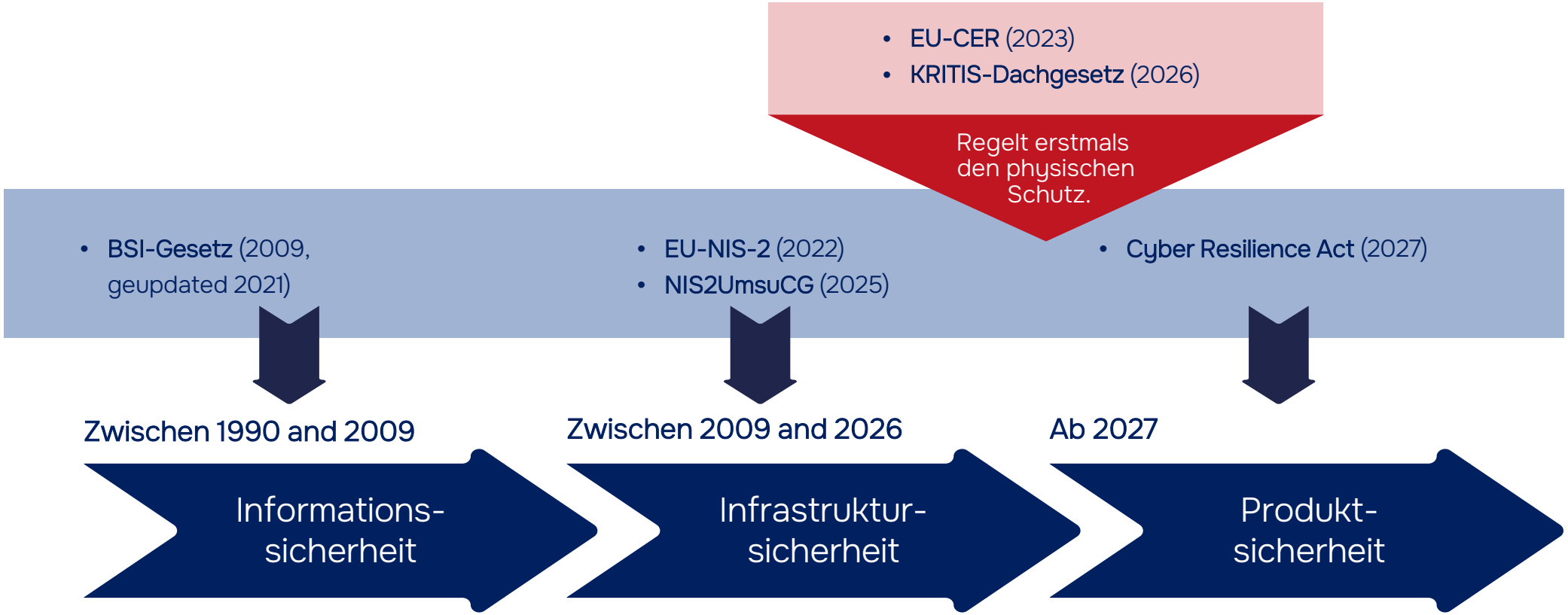
von **Miriam Hollstein** und **Viktar Vasileuski** 17. März 2026 • 06:10 Uhr • 5 Min.

Systems appear “trusted“ while already compromised.

TLP:CLEAR

PHYSEC

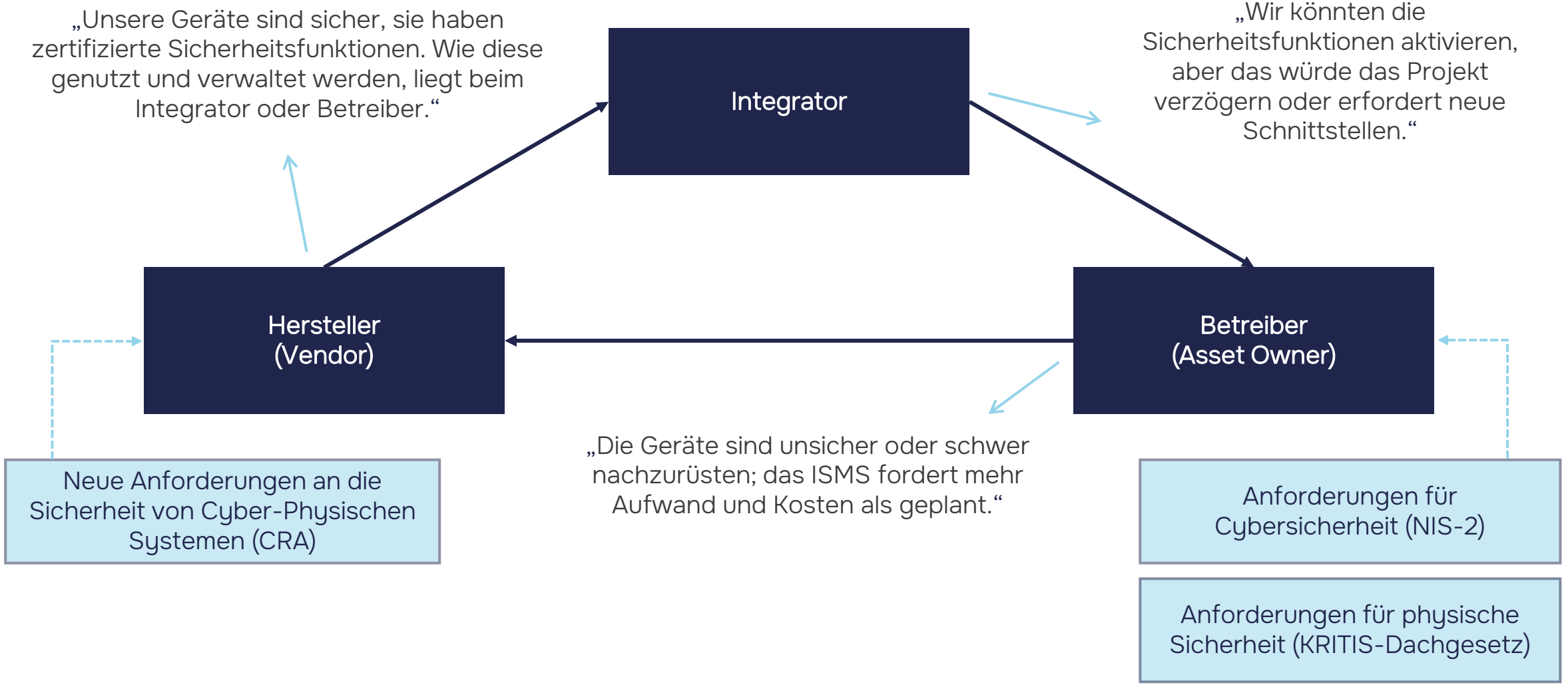
Cybersecurity is Expanding into the Physical World



TLP:CLEAR

PHYSEC

Zirkuläre Verschiebung der Verantwortung



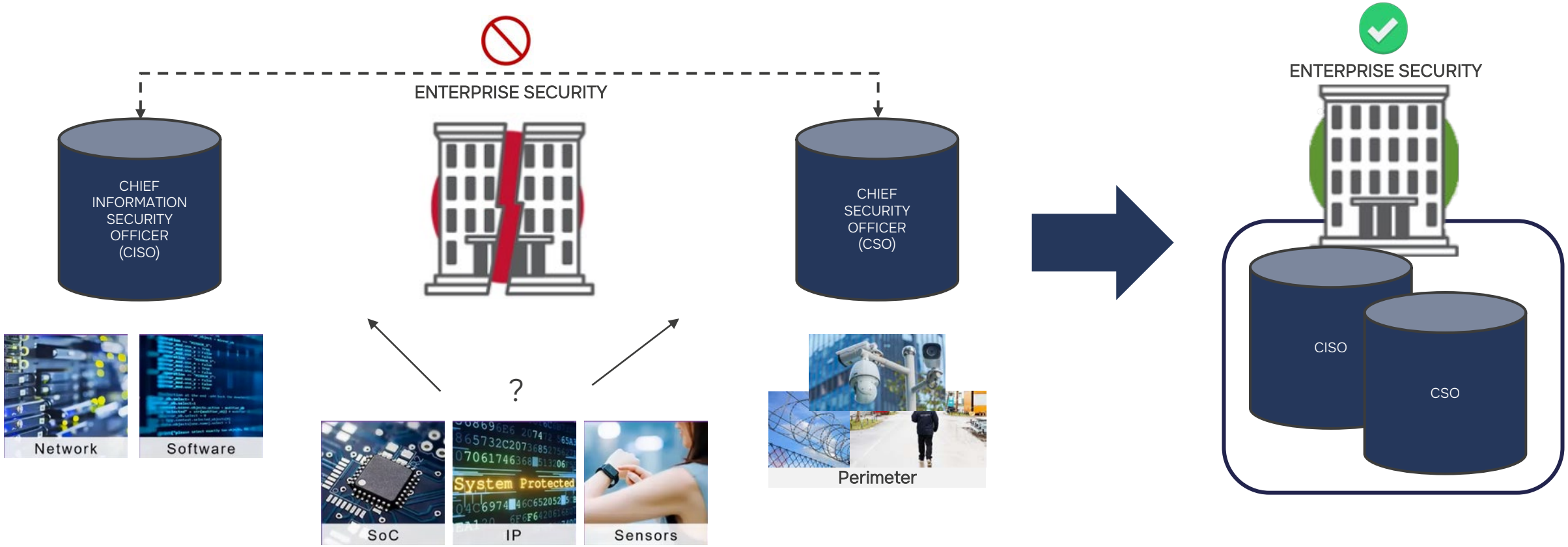
TLP:CLEAR

PHYSEC

§13 KRITIS-Dachgesetz: Maßnahmen

Maßnahmen		
• Überwachung kritischer Assets • Erkennung physischer Manipulation • Auditierbare Ereignis- und Zustandsdaten • Starker Beitrag zum Resilienzplan	• Objektschutz und Perimeter • Manuelle Sichtprüfung • Zugangskontrollkonzepte • Alarm- und Reaktionsabläufe • Krisenmanagement und Notfallvorsorge • Betriebsaufrechterhaltung	• Lieferketten-Resilienz • Personal- und Dienstleistermanagement • Schulungen und Übungen • Risiko- und Governance-Prozesse

Cyber & Physical Security wachsen zusammen



TLP:CLEAR

PHYSEC

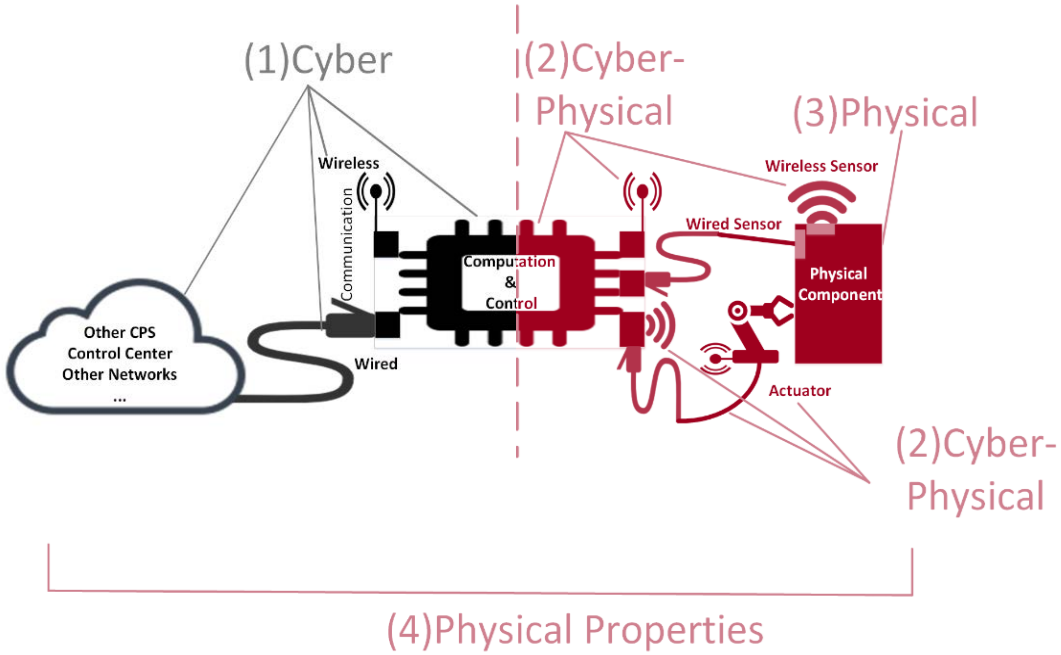
Kritische Infrastruktur

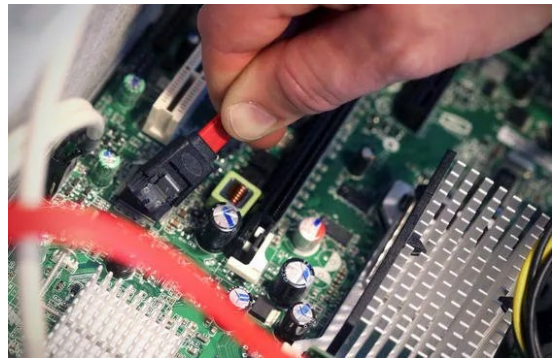
TLP:CLEAR

PHYSEC
https://hauff-technik-gridcom.de/

Cyber-Physical System Security

Cyberangriffe,
z. B. Inbounding-Angriffe, Phishing-E-Mails, Seitenkanalangriffe, Oracle-Angriffe, Implementierungsangriffe, Zero-Day-Exploits.





Physische Angriffe,
z. B. durch unbefugte Benutzer, Social Engineering, unehrliche Mitarbeiter, Fehler von Mitarbeitern, Hardware-Trojaner.

TLP:CLEAR

PHYSEC

Perimeter Physical Security

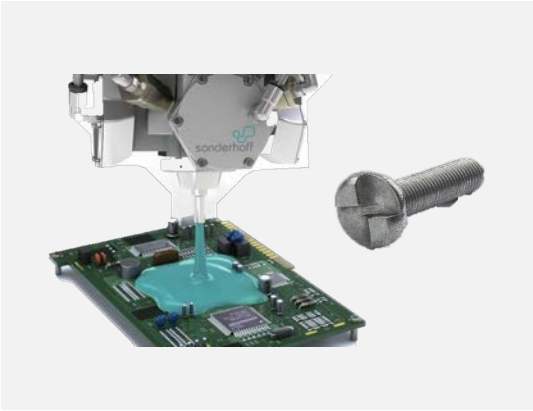
- **Deter (Abschrecken):** Potenzielle Eindringlinge oder Angreifer davon abhalten, überhaupt einen Versuch zu starten, die Sicherheit zu verletzen.
- **Detect (Erkennen):** Feststellen, dass ein Eindringen, Angriff oder eine Sicherheitsverletzung stattgefunden hat, um rechtzeitig reagieren zu können.
- **Delay (Verzögern):** Die Zeitspanne verlängern, die ein Eindringling oder Angreifer benötigt, um in kritische Bereiche oder zu wichtigen Assets einer Organisation vorzudringen.
- **Deny (Verweigern):** Den physischen Zugang zu bestimmten Orten oder Assets blockieren.

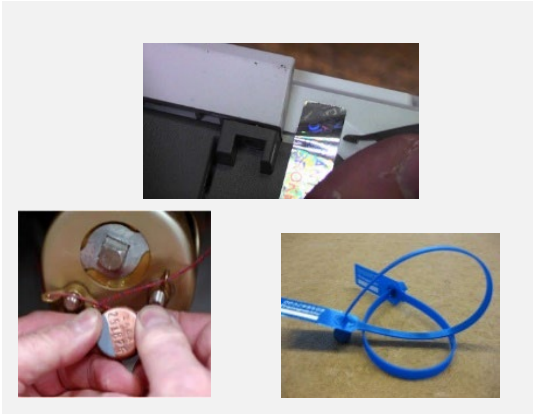
TLP:CLEAR

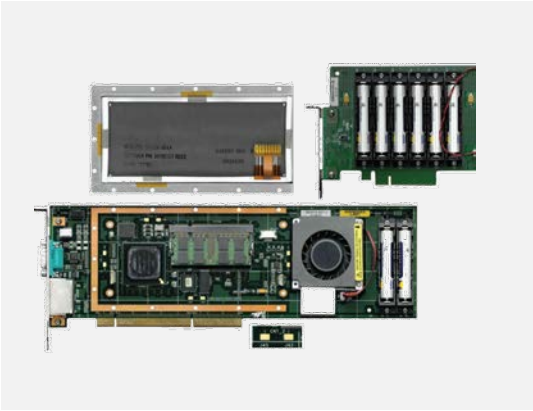
PHYSEC

Cyber-Physical Security von elektronischen Geräten

- **Tamper Resistance (Manipulationsresistenz):** Manipulation wird erschwert.
- **Tamper Evidence (Manipulationsnachweis):** Manipulationsversuche müssen erkennbar sein.
- **Tamper Detection (Manipulationserkennung):** Der Nutzer wird über Manipulationsangriffe informiert.
- **Tamper Responsiveness (Manipulationsreaktion):** Gegenmaßnahmen werden ausgelöst, sobald eine Manipulation erfolgt.







TLP:CLEAR

PHYSEC

Solution Gap for Hardware Security for IIoT

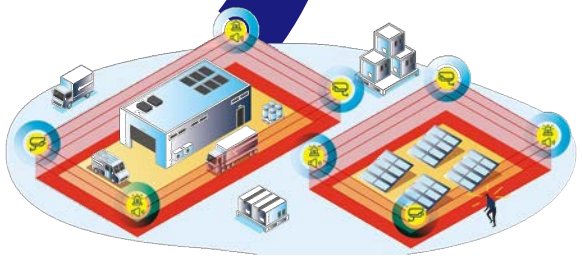
Too costly to scale.

Military Field Assets

Tamper Proofed Products

Edge, IIoT & OT

Physical trust remains unresolved



IT

Trusted Execution Environment

Das Dilemma: Sicherheit gegen Nation-State-Angreifer

Dilemma

Informationsasymmetrie entscheidet das Spiel

Verteidiger
muss mit Unwissenheit schützen.

Angreifer
braucht nur einen erfolgreichen Weg

Verteidiger	Nation-State-Angreifer
• Kennt die relevantesten Angriffstechniken oft nicht • Erfolg ist schwer nachweisbar • Angriffe liegen oft außerhalb des betrachteten Modells • Kunden erwarten Sicherheit, können das Niveau aber kaum bewerten.	• Zero-Day-Exploits & unbekannte Schwachstellen • Hardware-Manipulation & physische Angriffe • Supply-Chain-Angriffe & Insider-Zugänge • Spezialisierte Werkzeuge (EM, Side-Channel, Firmware, etc.)

Der Angreifer kennt mehr. Daher kann er sich durchsetzen.

TLP:CLEAR

PHYSEC

Physische Manipulationsangriffe

Vertraulichkeit, Integrität und Verfügbarkeit durch physischen Zugriff kompromittieren

ANGRIFFS-KATEGORIE	ÖFFNEN & ZUGRIFF	KOMPONENTEN-MANIPULATION	SIGNAL- & INTERFACE-MANIPULATION	FIRMWARE- & SPEICHERMANIPULATION	STROMVERSORGUNGS-MANIPULATION	INVASIVE PHYSISCHE TECHNIKEN	SUPPLY CHAIN & LOGISTIK-MANIPULATION
							
ZIEL / TYPISCHE ABSICHT	Erlangung von Zugriff auf das innere System durch Öffnen, Demontage oder Entfernen von Gehäuseteilen.	Verändern, Entfernen oder Ersetzen von elektronischen Komponenten.	Manipulation von elektrischen Signalen, Bussen oder Schnittstellen.	Auslesen, Verändern oder Ersetzen von Firmware und Speicherinhalten.	Manipulation der Stromversorgung zur Beeinflussung oder Übernahme des Systems.	Zerstörungsarme, invasive Techniken zur Datengewinnung oder Manipulation.	Manipulation während Herstellung, Transport, Lagerung oder Wartung.
BEISPIELE	• Gehäuse öffnen • Schrauben entfernen • Siegel brechen • Abdeckungen entfernen	• IC austauschen • Widerstände/Filter ändern • Sensoren manipulieren • Zusatzhardware einlöten	• Abgreifen von Signalen • Bus-Manipulation (z. B. I²C, SPI, JTAG) • Debug-Ports aktivieren	• SPI-Flash auslesen • Firmware modifizieren • Bootloader ersetzen • Speicherinhalte verändern	• Spannungsinjektion (Glitching) • Unter-/Überspannung • EM- oder Power-Glitching • Stromverbrauchsanalysen	• Mikrobohren / FIB • Chip-Decapping • Leiterbahnanzapfen • Laser-Manipulation	• Hardware-Trojaner einbauen • Manipulation in der Lieferkette • Austausch von Komponenten • Wartungszugriff missbrauchen
MÖGLICHE AUSWIRKUNGEN	Zugriff auf Komponenten, Schnittstellen und Speicher; Vorbereitung weiterer Angriffe.	Veränderung von Funktionen, Aushebeln von Sicherheitsmechanismen, Hintertüren schaffen.	Datenabfluss, Umgehung von Kontrollen, Code-Auslese oder -Einschleusung.	Persistenten Backdoor-Einschleusung, IP-Diebstahl, Manipulation des Systemverhaltens.	Umgehung von Sicherheitsprüfungen, Schlüsselextraktion, instabiles oder manipuliertes Verhalten.	Direkter Zugriff auf Chips, Schlüssel, Speicher oder Geheimhaltungsmechanismen.	Kompromittierung vor Inbetriebnahme, verdeckte Hintertüren, langfristige Risiken.
TYPISCHE GEGENMASSNAHMEN	• Manipulationssichere Gehäuse • Siegel, Plomben, Lacke • Öffnungserkennung	• Verguss / Conformal Coating • Komponentenauthentifizierung • Layout- & Schaltungsüberwachung	• Schnittstellenabsicherung • Deaktivieren/Absichern von Debug-Ports • Bus-Monitoring & Anomalieerkennung	• Secure Boot & Signaturen • Speicher-Verschlüsselung • Integritätsprüfung zur Laufzeit	• Spannungsüberwachung • Glitch-Detektion • Stabile & gefilterte Stromversorgung	• Active Shielding / Mesh • Tamper-Evident Design • Detektion von physischen Eindringversuchen	• Lieferketten-Sicherheit • Vertrauenswürdige Fertigung • Integritätsprüfung bei Inbetriebnahme

TLP:CLEAR

PHYSEC

Das nicht erfüllbare Paradoxon

Warum Hochsicherheit gegen unbekannte Angriffe nicht vollständig beweisbar ist

1. Unbekannte Angriffe

Die gefährlichsten Methoden bleiben oft jahrelang geheim – Verteidiger kennen sie nicht.

2. Schwer messbarer Erfolg

Ein Produkt kann selten beweisen, dass es einen geheimen Angriff verhindert hat.

3. Angriff außerhalb des Modells

Nation-States kombinieren Cyber- und physische Angriffe – klassische Modelle greifen zu kurz.

4. Erwartungen vs. Bewertungen

Kunden erwarten Schutz gegen Geheimdienste, können das Niveau aber kaum bewerten.

5. Paradoxon der Offenheit

Sicherheit braucht Transparenz – relevante Informationen sind aber oft klassifiziert.

Dieses Dilemma ist nicht auflösbar.

Informationen bleiben asymmetrisch.

TLP:CLEAR

PHYSEC

Vertrauen durch messbare Integrität

Statt den Angriff zu kennen, erkennen wir, ob das System noch im vertrauenswürdigen Zustand ist.

System in vertrauenswürdigem Zustand

PHYSEC SEAL misst, überwacht und prüft Integrität

Abweichung erkannt – auch bei unbekannten Angriffen

Vorteile

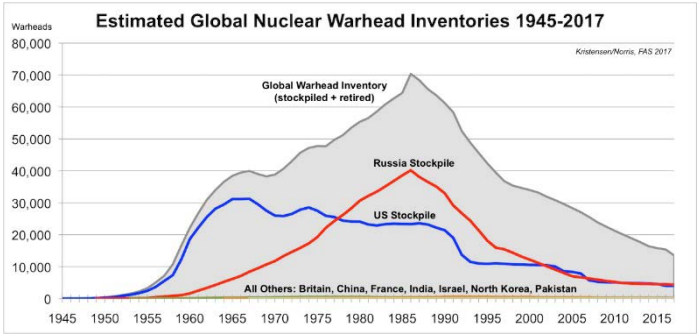
- Unabhängig vom Wissen über konkrete Angriffstechniken
- Erkennt Manipulationen und Veränderungen
- Schafft eine zusätzliche Vertrauensebene für kritische Systeme
- Ideal gegen Nation-State-Angreifer, bei denen das Unbekannte das Entscheidende ist

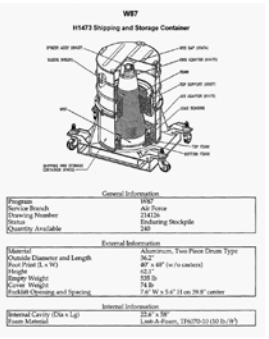
Sicherheit gegen Nation-States bedeutet:
Nicht alles wissen, aber Integrität nachweisbar machen.

TLP:CLEAR

PHYSEC

Spitzenforschung am Excellenzcluster der RUB





Wie können wir physikalische Aussagen aus der Ferne nachweisen, ohne auf klassische manipulationssichere Hardware und kryptografische Schlüssel zurückzugreifen?

RUHR UNIVERSITÄT BOCHUM RUB

PRINCETON UNIVERSITY

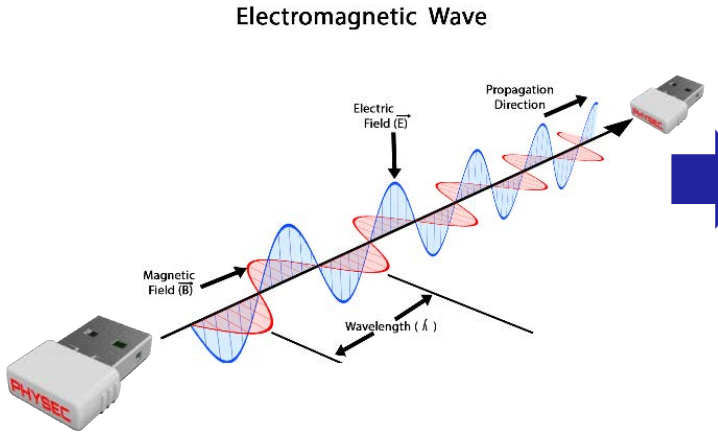
HARVARD UNIVERSITY

PHYSEC SECURITY FOR THINGS

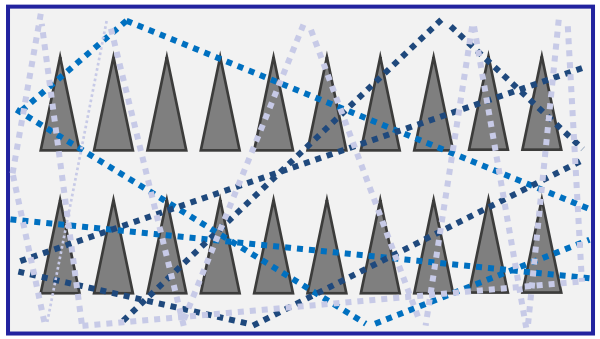
TLP:CLEAR

Spitzenforschung am Excellenzcluster der RUB

Wie können wir physikalische Aussagen aus der Ferne nachweisen, ohne auf klassische manipulationssichere Hardware und kryptografische Schlüssel zurückzugreifen?

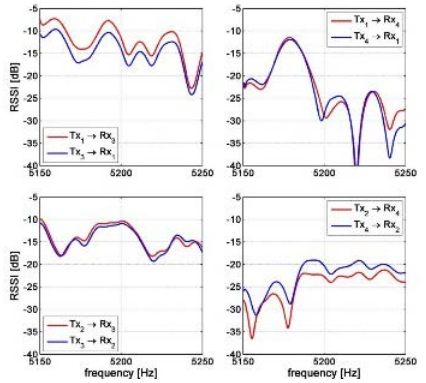


Challenges C_i



Physical Unclonable Function

$R_i = PUF(C_i)$

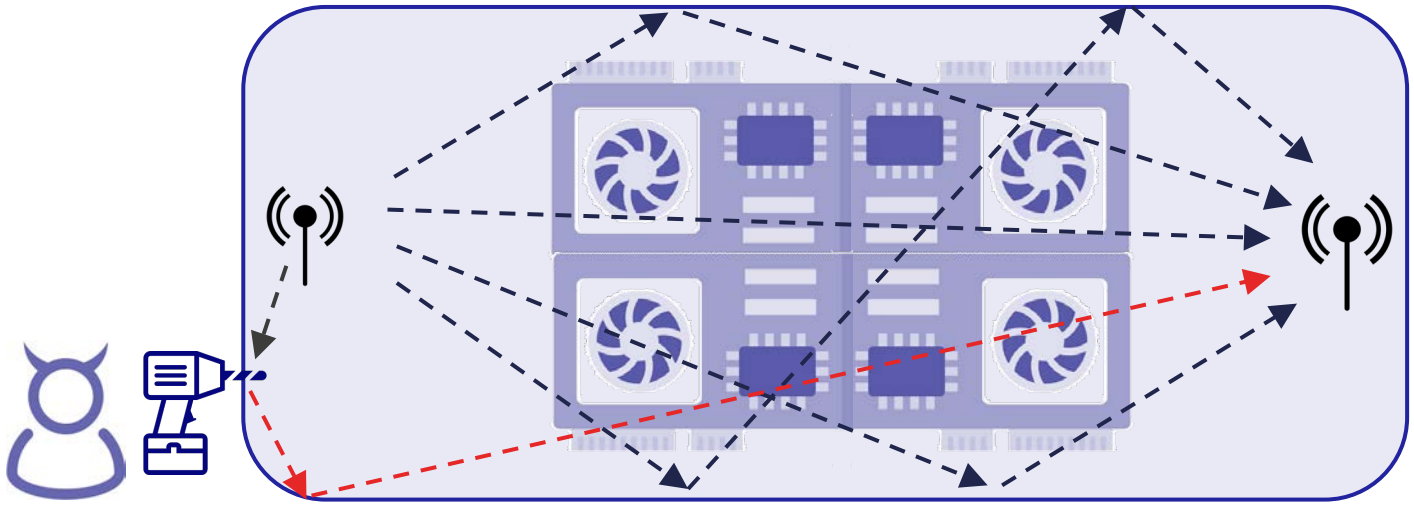


Responses R_i (≈Fingerprint)

TLP:CLEAR

PHYSEC

Anti-Tamper-Radio (ATR)



Signalanalyse

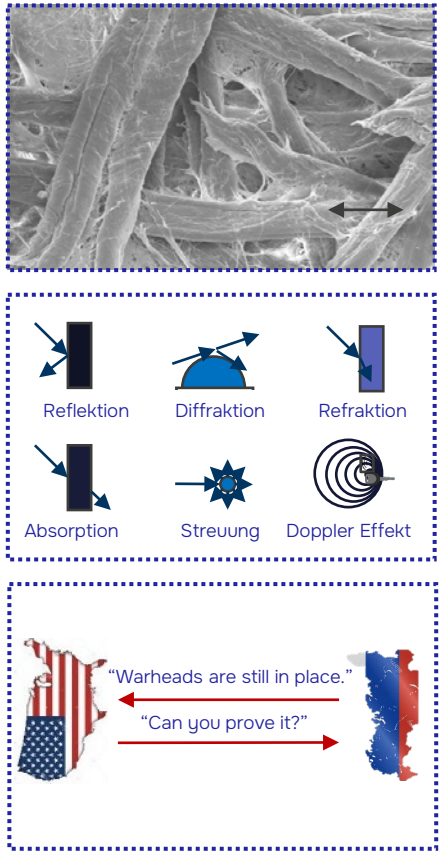
Prüfung der physischen Integrität

- Erkennung auf Systemebene
- Hohe Flexibilität
- Nachrüstbar
- Neu initialisierbar

Radiowellen reagieren empfindlich auf Umgebungsschwankungen!

Der Kerngedanke

Physikalische Systeme durch die Messung ihres einzigartigen elektromagnetischen Fingerabdrucks maschinenlesbar machen.



Die physikalisch ungeordnete Oberfläche des Objekts

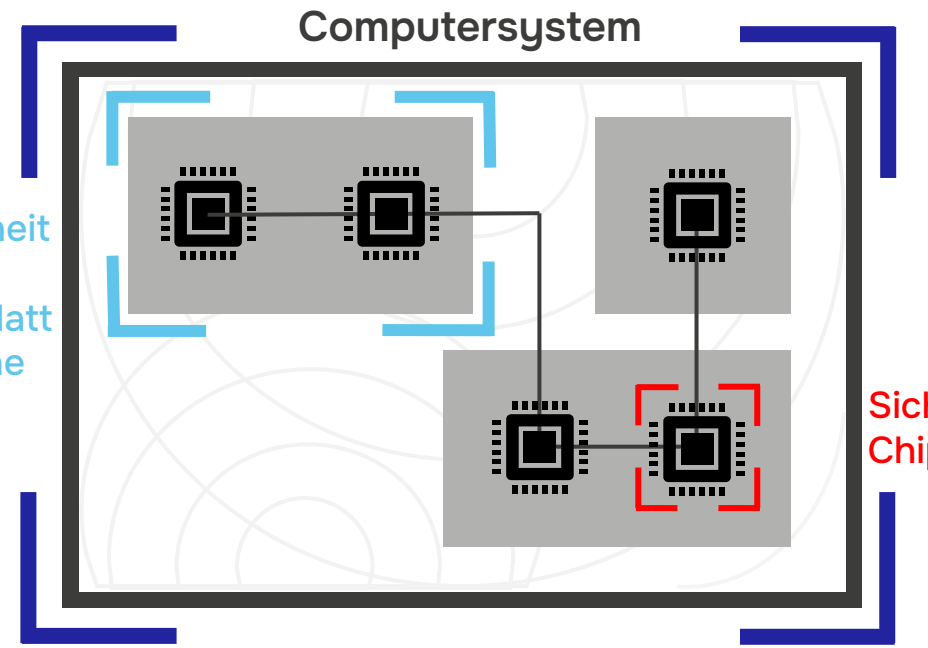
+

Auswirkungen der Ausbreitung von Funkwellen

+

Kryptografisches Challenge-Response-Protokoll

Sicherheit auf Leiterplatt enebene



Sicherheit auf Chip-Ebene

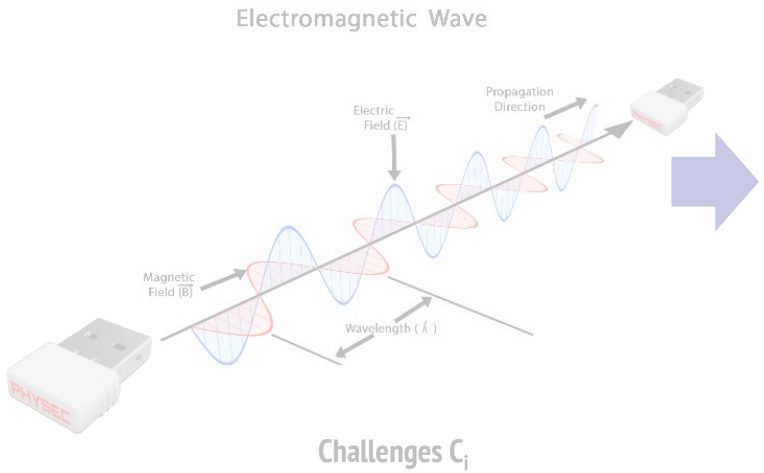
Sicherheit auf Systemebene

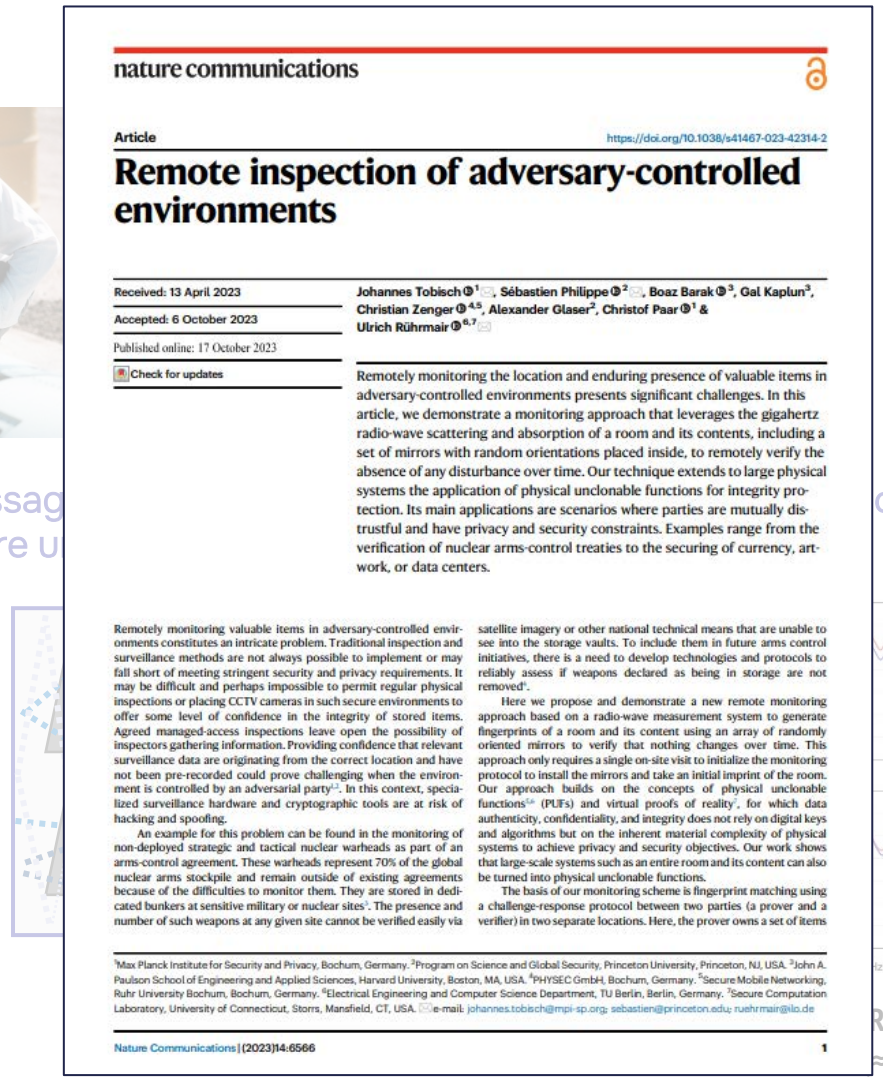
TLP:CLEAR

PHYSEC

Spitzenforschung am Excellenzcluster der RUB

Wie können wir physikalische Aussag … che
manipulationssichere Hardware u …





nature communications

Article

https://doi.org/10.1038/s41467-023-42314-2

Remote inspection of adversary-controlled environments

Received: 13 April 2023

Accepted: 6 October 2023

Published online: 17 October 2023

Check for updates

Johannes Tobisch[1], Sébastien Philippe[2], Boaz Barak[3], Gal Kaplun[3], Christian Zenger[4,5], Alexander Glaser[2], Christof Paar[1] & Ulrich Rührmair[6,7]

Remotely monitoring the location and enduring presence of valuable items in adversary-controlled environments presents significant challenges. In this article, we demonstrate a monitoring approach that leverages the gigahertz radio-wave scattering and absorption of a room and its contents, including a set of mirrors with random orientations placed inside, to remotely verify the absence of any disturbance over time. Our technique extends to large physical systems the application of physical unclonable functions for integrity protection. Its main applications are scenarios where parties are mutually distrustful and have privacy and security constraints. Examples range from the verification of nuclear arms-control treaties to the securing of currency, artwork, or data centers.

Remotely monitoring valuable items in adversary-controlled environments constitutes an intricate problem. Traditional inspection and surveillance methods are not always possible to implement or may fall short of meeting stringent security and privacy requirements. It may be difficult and perhaps impossible to permit regular physical inspections or placing CCTV cameras in such secure environments to offer some level of confidence in the integrity of stored items. Agreed managed-access inspections leave open the possibility of inspectors gathering information. Providing confidence that relevant surveillance data are originating from the correct location and have not been pre-recorded could prove challenging when the environment is controlled by an adversarial party[1,2]. In this context, specialized surveillance hardware and cryptographic tools are at risk of hacking and spoofing.

An example for this problem can be found in the monitoring of non-deployed strategic and tactical nuclear warheads as part of an arms-control agreement. These warheads represent 70% of the global nuclear arms stockpile and remain outside of existing agreements because of the difficulties to monitor them. They are stored in dedicated bunkers at sensitive military or nuclear sites[3]. The presence and number of such weapons at any given site cannot be verified easily via satellite imagery or other national technical means that are unable to see into the storage vaults. To include them in future arms control initiatives, there is a need to develop technologies and protocols to reliably assess if weapons declared as being in storage are not removed[4].

Here we propose and demonstrate a new remote monitoring approach based on a radio-wave measurement system to generate fingerprints of a room and its content using an array of randomly oriented mirrors to verify that nothing changes over time. This approach only requires a single on-site visit to initialize the monitoring protocol to install the mirrors and take an initial imprint of the room. Our approach builds on the concepts of physical unclonable functions[5,6] (PUFs) and virtual proofs of reality[7], for which data authenticity, confidentiality, and integrity does not rely on digital keys and algorithms but on the inherent material complexity of physical systems to achieve privacy and security objectives. Our work shows that large-scale systems such as an entire room and its content can also be turned into physical unclonable functions.

The basis of our monitoring scheme is fingerprint matching using a challenge-response protocol between two parties (a prover and a verifier) in two separate locations. Here, the prover owns a set of items

[1]Max Planck Institute for Security and Privacy, Bochum, Germany. [2]Program on Science and Global Security, Princeton University, Princeton, NJ, USA. [3]John A. Paulson School of Engineering and Applied Sciences, Harvard University, Boston, MA, USA. [4]PHYSEC GmbH, Bochum, Germany. [5]Secure Mobile Networking, Ruhr University Bochum, Bochum, Germany. [6]Electrical Engineering and Computer Science Department, TU Berlin, Berlin, Germany. [7]Secure Computation Laboratory, University of Connecticut, Storrs, Mansfield, CT, USA. e-mail: johannes.tobisch@mpi-sp.org; sebastien@princeton.edu; ruehrmair@ilo.de

Responses R_i
≈Fingerprint)

RUHR UNIVERSITÄT BOCHUM RUB

PRINCETON UNIVERSITY

HARVARD UNIVERSITY

PHYSEC SECURITY FOR THINGS

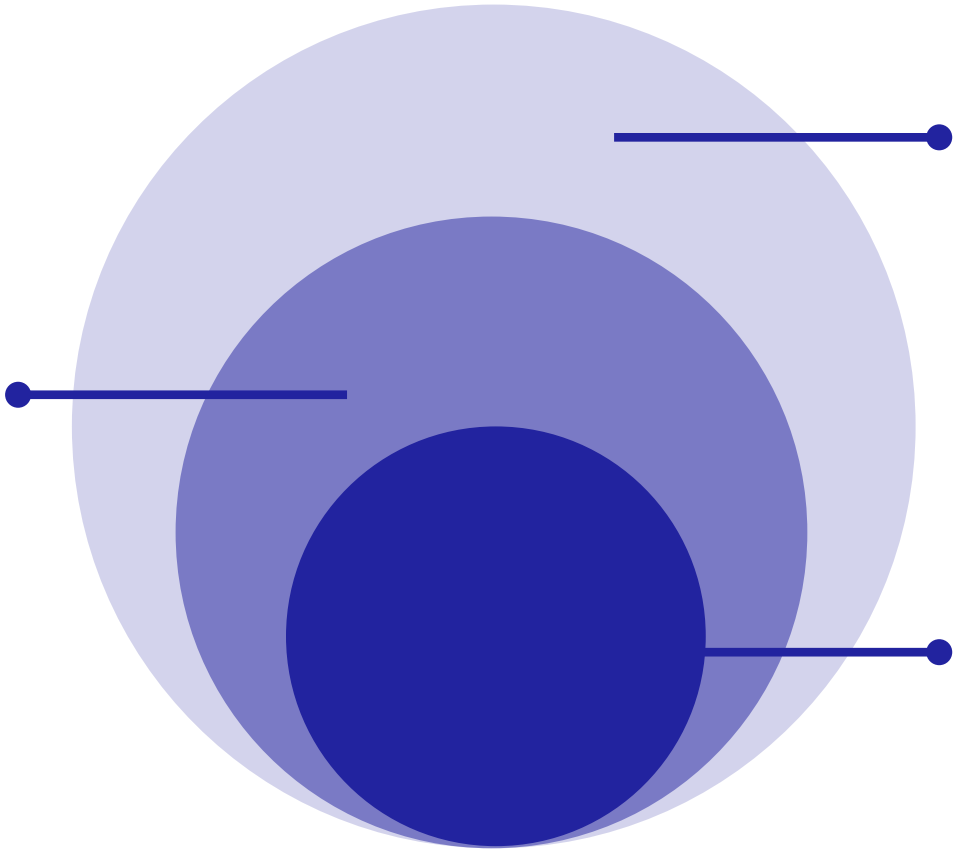
TLP:CLEAR

PHYSEC

Eine neue Sicherheitsebene

Physische Integrität
Gerätehardware und Manipulationsstatus überprüfen

Vertrauen in Software
sicherstellen, dass nur vertrauenswürdige Software ausgeführt wird



Identitätsvertrauen
Benutzeridentität und Anmeldedaten überprüfen

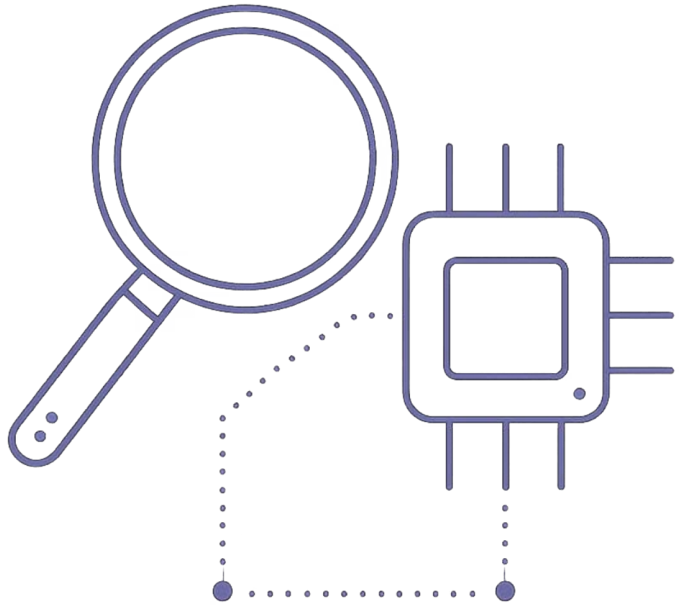
Wir erweitern Zero Trust über die Software hinaus – in die physische Welt.

TLP:CLEAR

PHYSEC

Wo PHYSEC SEAL® den Unterschied macht

PHYSEC SEAL® führt eine Überprüfung der physischen Unversehrtheit über den gesamten Lebenszyklus ein



01 Nach dem Transport: Vor der Inbetriebnahme überprüfen

02 Nach der Lagerung: Vor der Inbetriebnahme überprüfen

03 Nach der Wartung: Systemintegrität überprüfen

04 Während des Betriebs: Erkennung versteckter Manipulationen

Vorher

Vertrauen durch Prozesssicherheit und Compliance

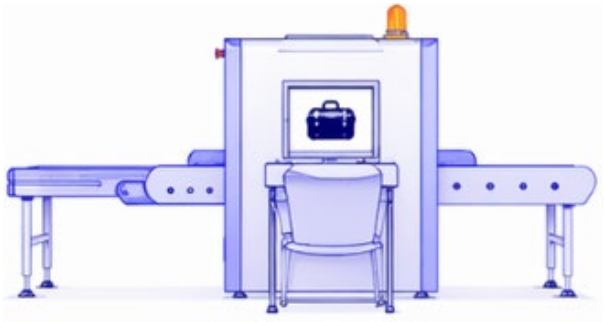
Mit PHYSEC SEAL®

Vertrauen, das auf der messbaren physikalischen Realität beruht

Snapshot-basierte Integritätsprüfung

Verifiziert die Integrität Ihrer Geräte von innen heraus unmittelbar

Herkömmliche Sicherheitskontrolle (z.B. Flughafenscanner)

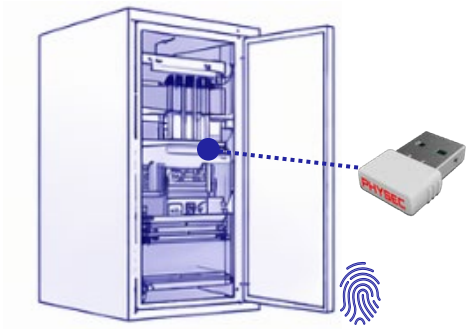


Scannt Objekte von außen nach innen

10 bis 100 mal günstiger

Erkennt Mikro-veränderungen bis zu 125 μm^3

PHYSEC SEAL®



Scannt Objekte von innen nach außen

Erstellt einen digitalen Fingerabdruck des Geräts

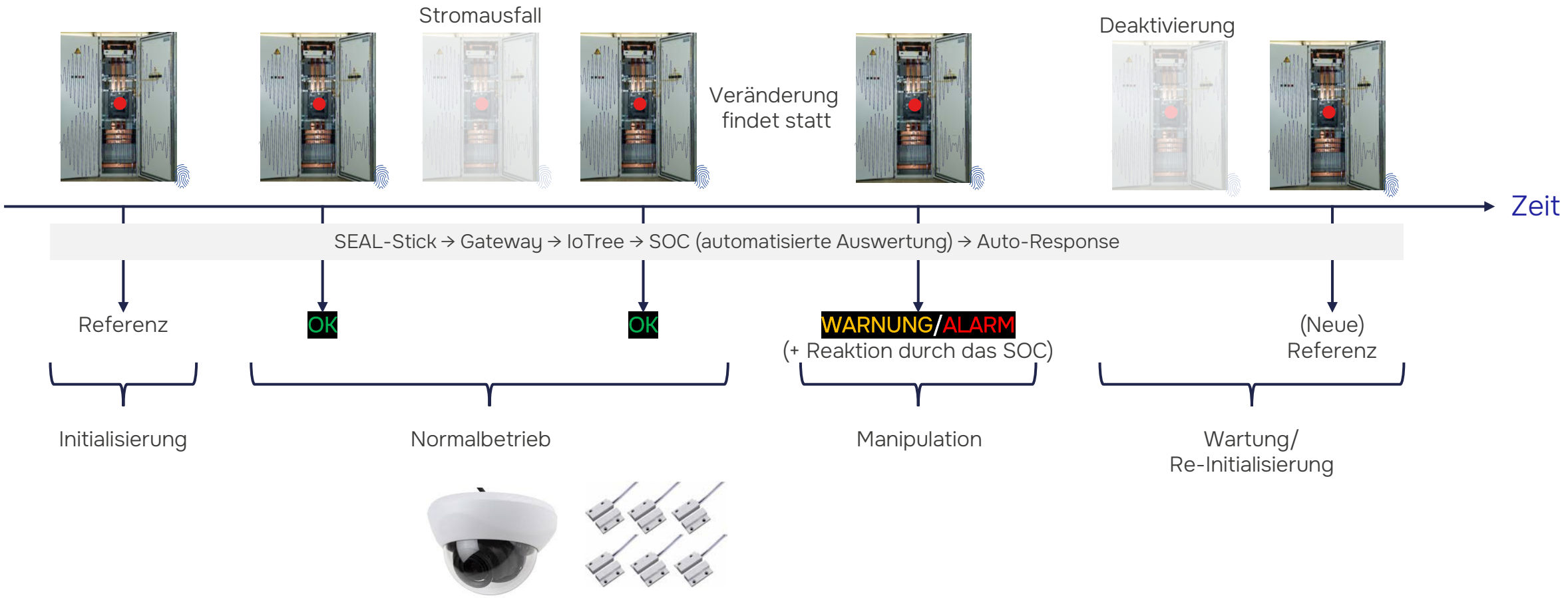
Erkennt selbst kleinste interne Veränderungen

SEAL scannt von innen nach außen und erkennt, was andere nicht erkennen können – und das zu einem Bruchteil der Kosten.

TLP:CLEAR

PHYSEC

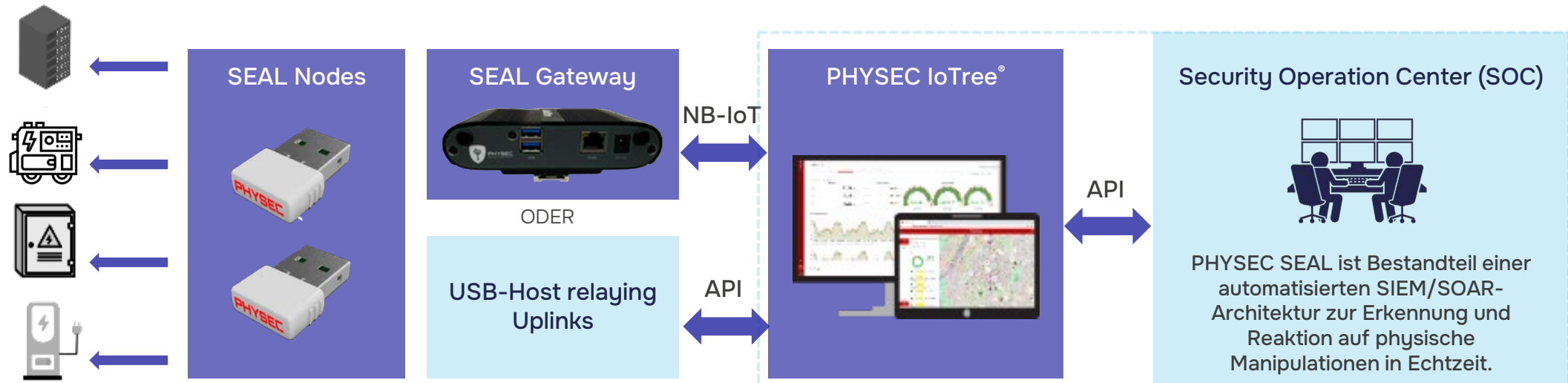
Gezielte Erkennung statt Dauerüberwachung durch Snapshot-basierte Integritätsprüfung



TLP:CLEAR

PHYSEC

Automatisierte Sicherheitsarchitektur mit PHYSEC SEAL: Von der Manipulationserkennung bis zur Reaktion im SOC



PHYSEC SEAL® ist eine Monitoring-as-a-Service-Lösung, die für KRITIS geeignet ist. Wir bieten ein mit Partnern abgestimmtes Full-Service-Paket an.

TLP:CLEAR

PHYSEC

Was PHYSEC SEAL® für Betreiber kritischer Systeme ermöglicht

- kontinuierlicher Integritätsnachweis von Geräten
- frühzeitige Erkennung physischer Manipulation
- zusätzliche Sicherheitsebene für OT und IoT
- Unterstützung regulatorischer Anforderungen (z. B. IEC 62443, CRA, KRITIS-Dachgesetz)
- Integration in bestehende Systeme möglich
- Beispiele für Einsatzbereiche:
  - Energieinfrastruktur
  - industrielle Anlagen
  - Rechenzentren
  - kritische IoT-Systeme

Kerntechnologie des Sensors ist eine miniaturisierte Radaranlage die EMV, CE und FCC konform die physischen Strukturen vermisst.

TLP:CLEAR

PHYSEC

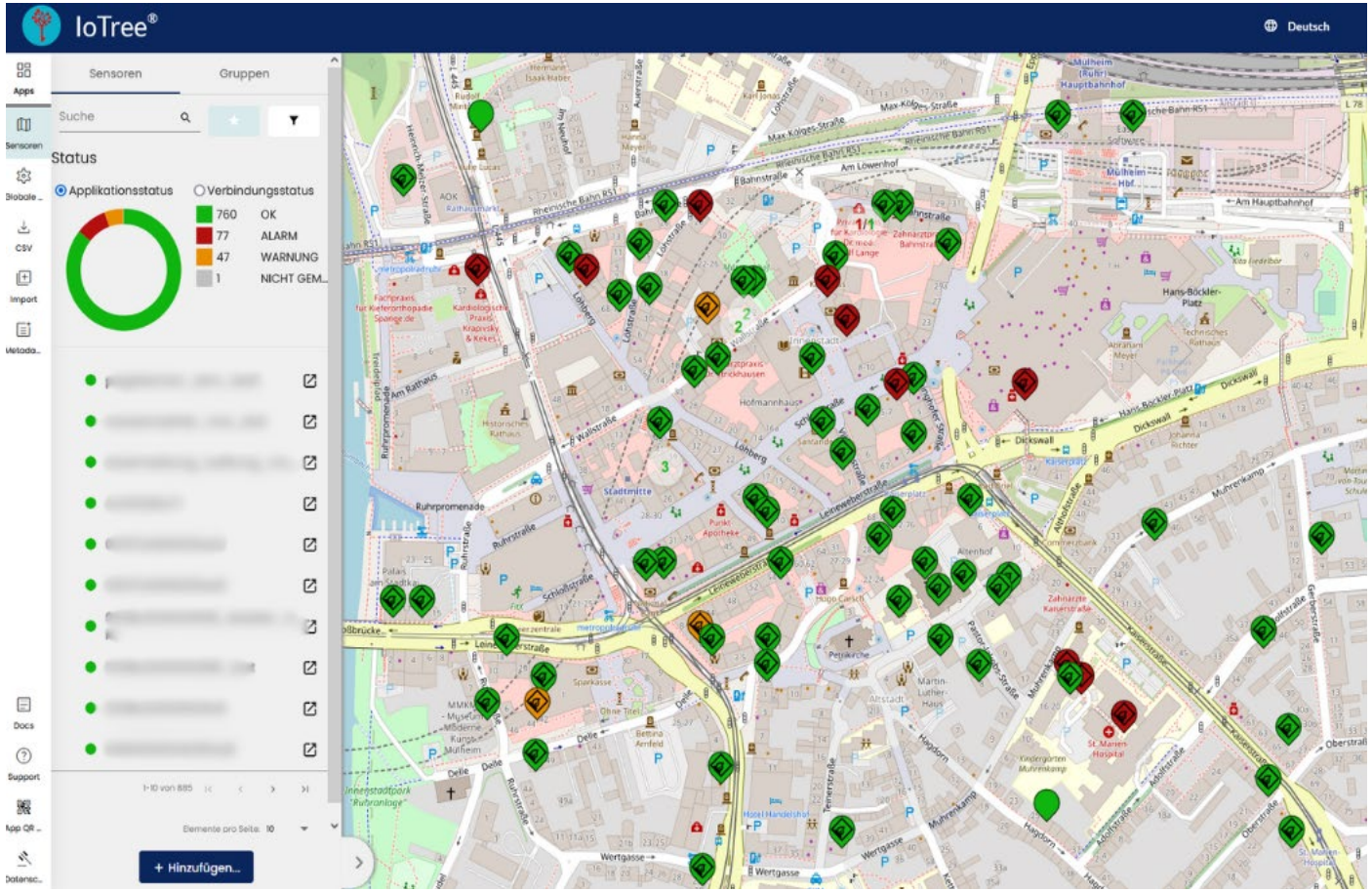
§13 KRITIS-Dachgesetz: Wo PHYSEC SEAL® echten Mehrwert schafft

Direkt unterstützt	Teilweise ersetzbar / unterstützt	Zusätzlich erforderlich
• Überwachung kritischer Assets • Erkennung physischer Manipulation • Auditierbare Ereignis- und Zustandsdaten • Starker Beitrag zum Resilienzplan	• Objektschutz und Perimeter • Manuelle Sichtprüfung • Zugangskontrollkonzepte • Alarm- und Reaktionsabläufe • Krisenmanagement und Notfallvorsorge • Betriebsaufrechterhaltung	• Lieferketten-Resilienz • Personal- und Dienstleistermanagement • Schulungen und Übungen • Risiko- und Governance-Prozesse

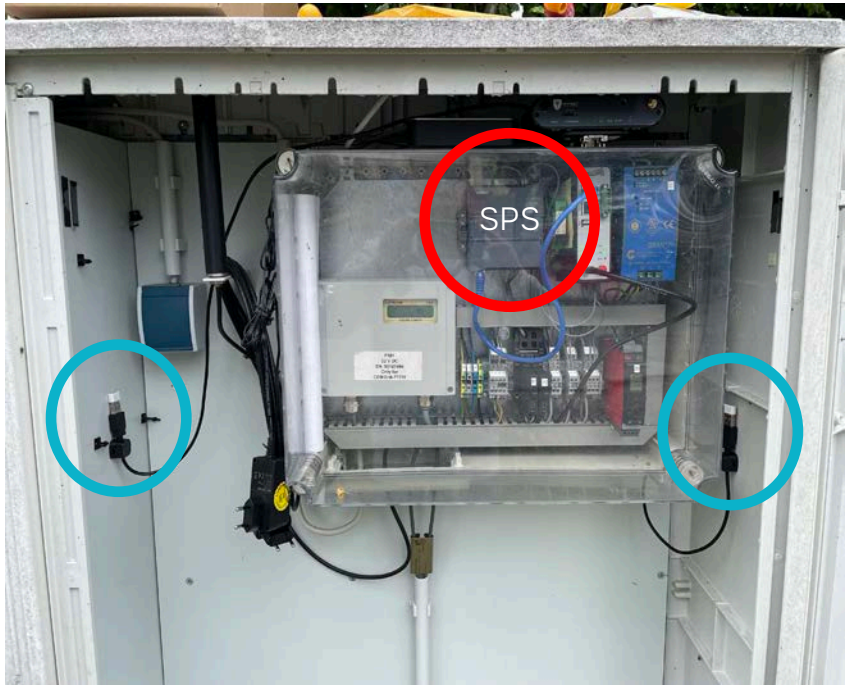
SEAL ist kein Ersatz für ein vollständiges KRITIS-Resilienzmanagement – aber ein hochwirksamer Baustein dort, wo physische Integrität sichtbar und nachweisbar werden muss.

Impressionen

Plattform zum Schutz cyber-physischer Systeme schützt unternehmenskritische Ressourcen außerhalb der IT-Umgebungen von Unternehmen.



Der Screenshot bietet eine realistische Darstellung der Benutzeroberfläche und enthält keine vertraulichen oder personenbezogenen Daten.



Das Bild zeigt eine zugelassene Testinstallation; bei Standardinstallationen werden die Knoten jedoch in der Regel innerhalb des Gehäuses installiert.

TLP:CLEAR

PHYSEC

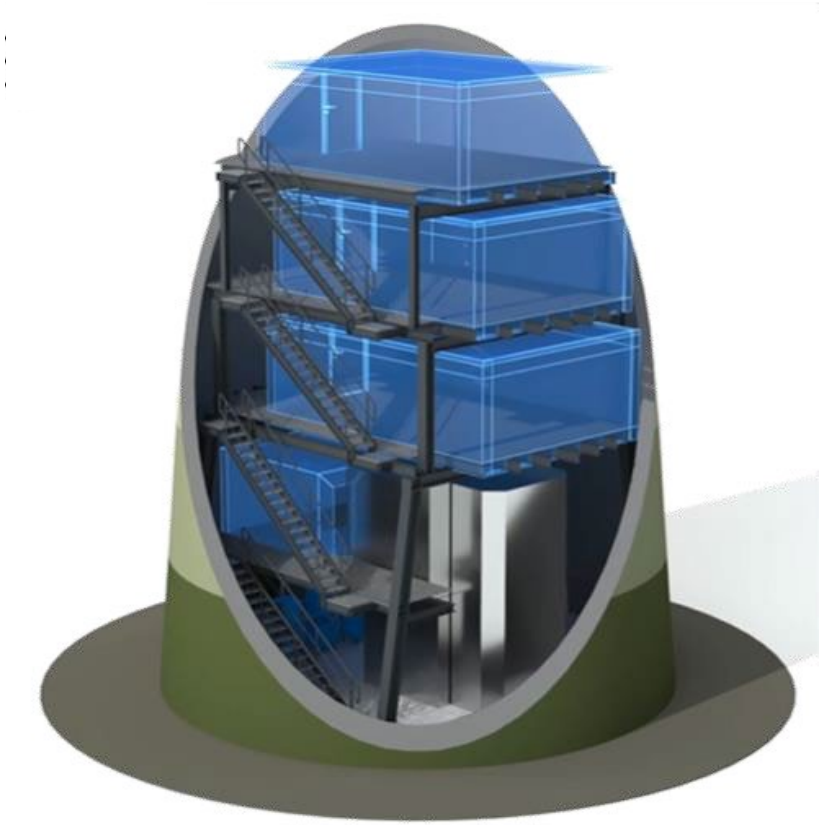
Impressionen E-Ladestation

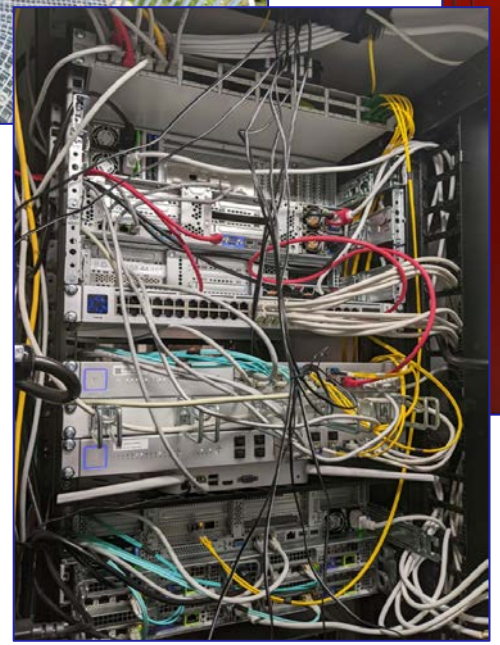
TLP:CLEAR

PHYSEC

Impressionen Gasdruckregeln und Abrechnung

Impressionen Edge-Datacenter





TLP:CLEAR

PHYSEC

Impressionen Verlegefähige BTuLBs

TLP:CLEAR

PHYSEC

PHYSEC in Zahlen

40+
Mitarbeitende

9+
Jahre am Markt

Information Security Management System
RSM Certification GmbH
RSM
CERTIFIED
Certificate No.
RSMCERT.2024.12
ISO/IEC 27001

100+
Sensortypen von mehr als 30 Herstellern

80+
Kunden und +60 Partner

PHYSEC
SECURITY FOR THINGS

200.000+
Angeschlossene Geräte

5+
Patentfamilien

TLP:CLEAR

PHYSEC

Vielen Dank für Ihre Aufmerksamkeit!

Fragen? Gerne jetzt...

...oder später:

christian.zenger@physec.de

“This young German innovators [PHYSEC] show an impressive combination of entrepreneurial and scientific-technical skills and are developing a technology with the potential to impact the world.”
— Mahvash Siddiqui, MIT Technology Review

MIT Technology Review

Gefördert durch:

SPRIN-D
BUNDESAGENTUR FÜR SPRUNGINNOVATIONEN

Ausgezeichnet mit dem:

Deutscher IT-Sicherheitspreis

PHYSEC GmbH
Suttner-Nobel-Allee 7
44803 Bochum

+49 234 544 28224
info@physec.de
www.physec.de

TLP:CLEAR