Cyber-Resilienz: Wie Systeme Angriffe überstehen.

Hintergrund, Ziele und Ansätze

Hagen Lauer, Professor für IT-Sicherheit
Forschungsgruppe „Trustworthy Systems und Security“

Technische Hochschule Mittelhessen

Prof. Dr. Hagen Lauer

Lehrt und forscht an der TH Mittelhessen (Gießen)

Themen und Gebiete:

- Sicherheit verteilter Systeme
- Cyber-Resilienz
- Trusted Computing
- Computer-Forensik

Zuvor Forschung im Bereich „Cyber-Physical Systems“ und „Smart Grids“ am Fraunhofer-Institut für Sichere Informationstechnologie (SIT)

Promotion an Monash University (Melbourne)

- Thema: Sichere und vertrauenswürdige Cloud-Umgebungen

Technische Hochschule Mittelhessen - Fachbereich Mathematik, Naturwissenschaften und Informatik

THM | CAMPUS GIESSEN | MNI
Mathematik, Naturwissenschaften und Informatik
TECHNISCHE HOCHSCHULE MITTELHESSEN

1971 gegründet und ist heute eine der größten deutschen „Hochschulen für Angewandte Wissenschaften“ (HAW)

- mit verschiedenen Standorten (Gießen, Friedberg, Wetzlar) die größte HAW in Hessen

Mathematik, Naturwissenschaften und Informatik bilden zusammen den größten Fachbereich der THM

Zahlreiche Lehrveranstaltungen, Seminare und Forschungsvorhaben im Bereich „IT-Sicherheit“

Einige Dinge, von denen ich Sie heute überzeugen möchte:

Cyber-Resilienz und Cyber-Sicherheit sind nicht gleich.

Cyber-Resilienz ist auch ein technisches Konzept - kein Wunschziel.

Autonomie und Automation werden in Zukunft wesentlich für die Cyber-Resilienz sein.

Geschichte und Trends in der Informationstechnologie

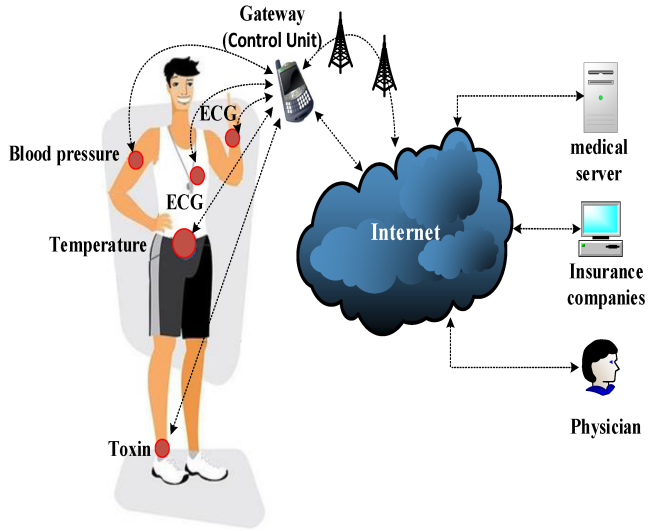
- **Simulation/Berechnung** — 1950 - heute — Forschung, Rechnungswesen, KI, VR, Spiele
- **Vernetzung & Speicher** — 1980 - heute — Email, Messaging, Suchmaschinen, Social Media, Unterhaltung, Arbeit
- **Interaktion** — 2010 - heute — Cyber-Physische Systeme, IoT, IIoT, Smart Grid, Health IoT, autonomes Fahren
- **Integration** — 2040? — Integration von Computern und biologischen Prozessen (e.g., Bewegung, Wahrnehmung, Denken, …)

Trends in der Informationstechnologie

- Anwendungen vermehrt geteilt, verteilt, vernetzt, dynamisch und heterogen
- Angriffe haben heute meist finanzielle Motive (vgl. Ransomware)
- Hohe Anforderungen an Sicherheit und Zuverlässigkeit
- IT-Sicherheit und Datenschutz muss von Beginn an berücksichtigt werden

Smart Grid - Q: Fraunhofer ISE

Autonomes Fahren - Q: IEEE Innovation



Telemedizin - Q: Salehi, Lauer, Rudolph, Grobler

Trends in der Informationstechnologie

Systeme sind heute *komplex*, nicht nur kompliziert.

Ständige Vernetzung mittlerweile notwendig.

Kommunikation und Interaktion sind wichtiger als Isolation.

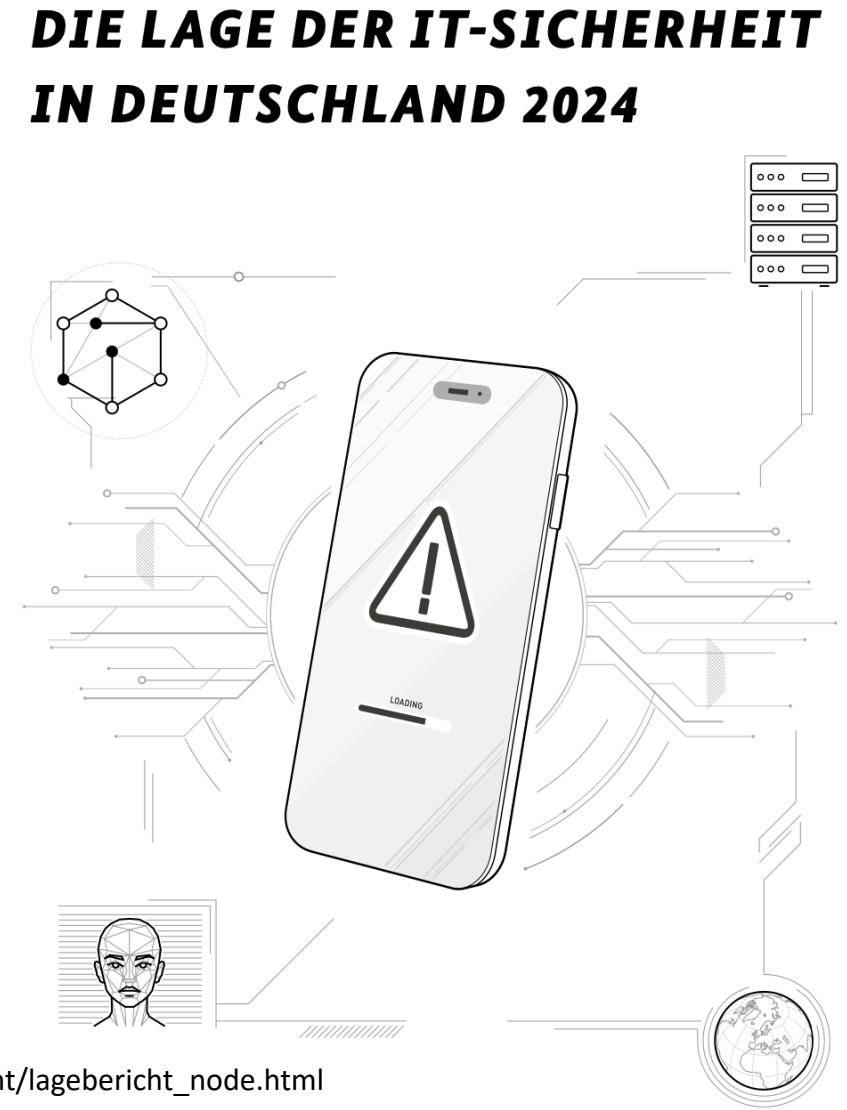
Systeme werden für Zugriff aus dem Internet geöffnet.

Werden in „nicht vertrauenswürdigen“ Umgebungen betrieben.

BSI: Lage der IT-Sicherheit in Deutschland

Übersicht über:

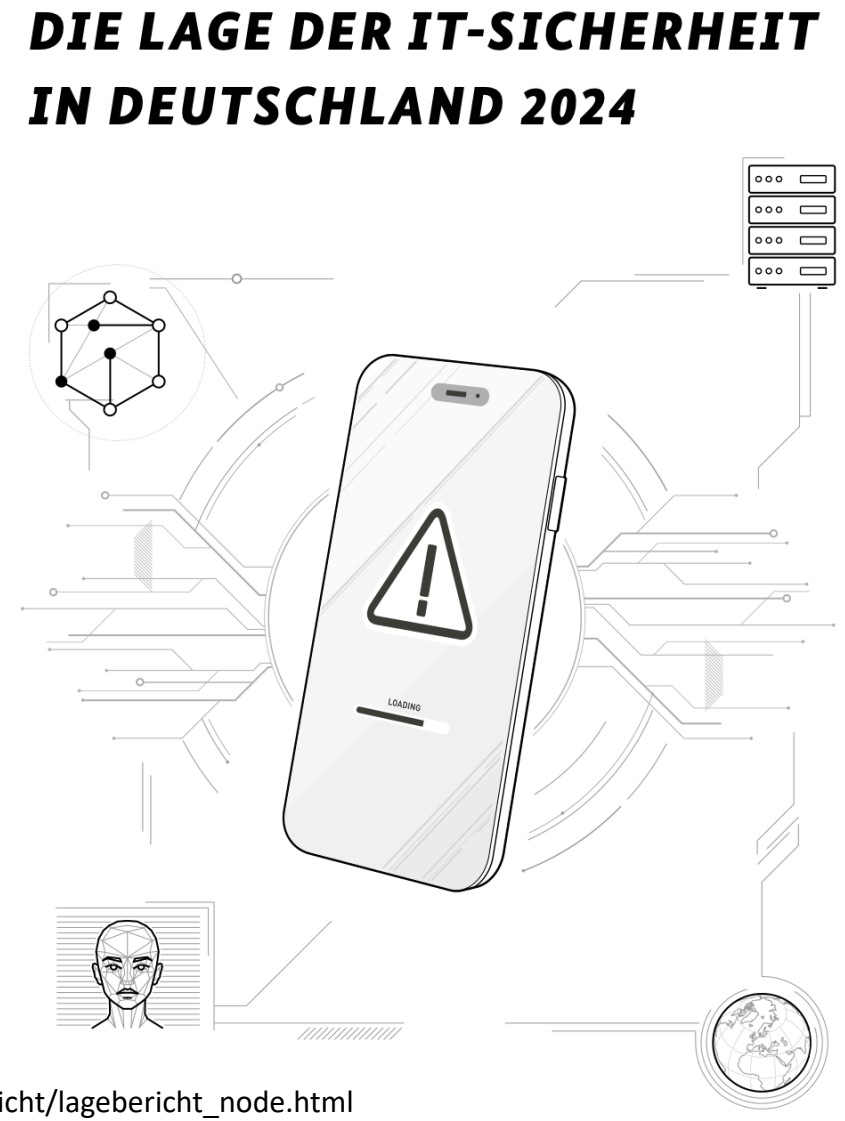
- Bedrohungen
- Angriffsfläche
- Gefährdungen
- Schäden
- „Die entscheidende Dimension Resilienz“



Q: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

BSI: Lage der IT-Sicherheit in Deutschland

- Durch Bedrohungen im Cyber-Raum entstehen immense Schäden in Wirtschaft, Verwaltung und Gesellschaft.
- Aktuelle Lage wird als „angespannt“ bewertet.
- Opfer waren überwiegend kleine und mittlere Unternehmen, insbesondere IT-Dienstleister, und Kommunen.

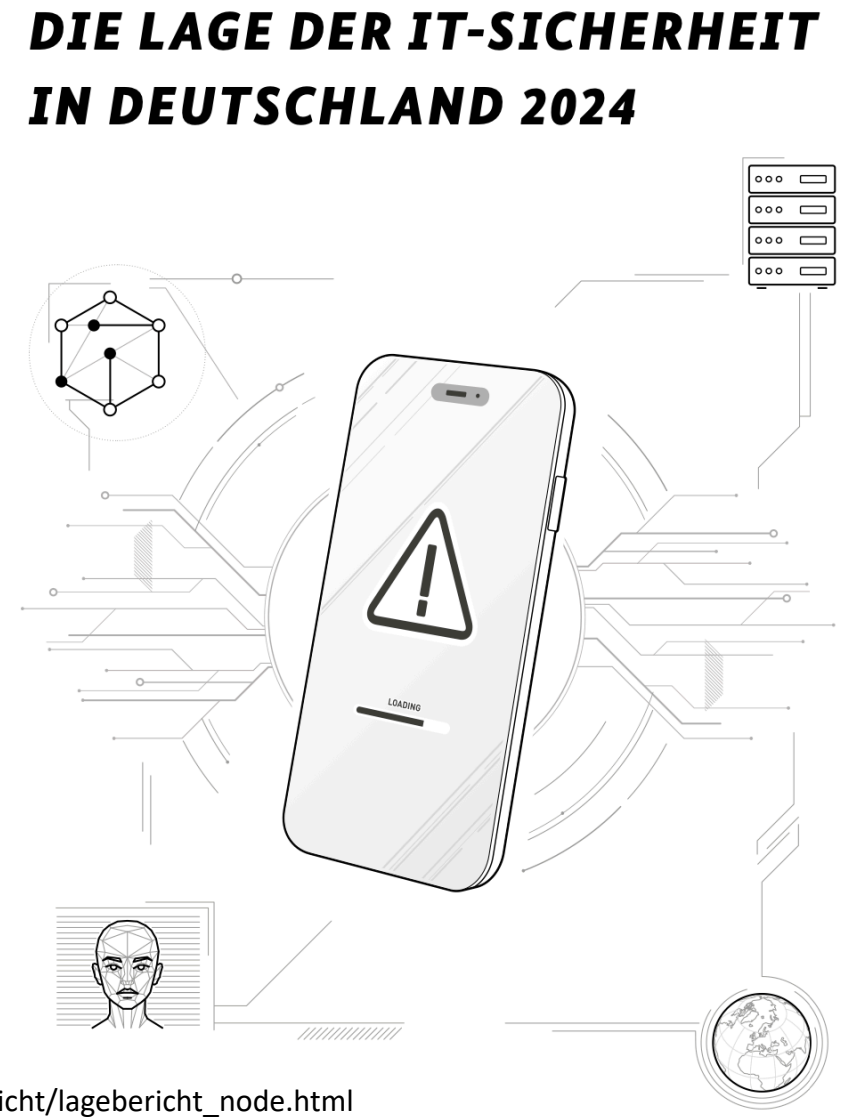


Q: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

BSI: Lage der IT-Sicherheit in Deutschland

Als größte Bedrohungen werden identifiziert:

- Ransomware-Angriffe
- Zero-Day Exploitation für Daten-Lecks
- Distributed Denial of Service (DDoS)



Q: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

Bedrohungen, Schwachstellen und Angriffe

Beispiele

Vom Schutzgut bis zum Angriff

Schutzgut *(Ziel)*

Gefahr *(kein Zusammenhang)*

Bedrohung *(Gefahr mit Bezug zum Ziel)*

+

Schwachstelle *(Mangelnde Schutzmaßnahmen)*

Angriff *(Nutzt Schwachstelle aus)*

Beispiel: Malware

Malware (**mal**icious soft**ware**): Schadcode läuft auf Computer des Opfers

- Sammelbegriff für verschiedene Formen und Funktionen von Schadcode:
  - Dateien löschen
  - Spam Email versenden
  - DoS Attacken ausführen
  - Private Information klauen und mit Leaks drohen
  - User Input aufzeichnen (keylogging, screen capture, webcam capture)
  - Dateien und Festplatten verschlüsseln und Geld für die Herausgabe verlangen (ransomware)
  - Geräte physisch beschädigen / zerstören

Beispiel: Malware

Unter Malware fallen:

- Computer Virus
- Trojanisches Pferd / Trojaner
- Wurm
- Ransomware
- Adware / Spyware
- Rootkits
- ...

Beispiel: Ransomware

- Form von Malware, die „Lösegeld“ oder *Ransom* verlangt,
  - damit Systeme wieder zugreifbar werden,
  - Daten entschlüsselt werden,
  - Daten nicht an die Öffentlichkeit gelangen. (Leaks)

- Aktuelle Ransomwaregruppen:
  - Lockbit
  - Play / PlayCrypt
  - Ransomhub
  - Black Basta
  - 8Base

- Neue Gruppen alleine 2024:
  - DarkVault (Feb 24)
  - ATP73 (Apr 24)
  - Quilong (Apr 24)

WannaCry Ransomware Notice

Beispiel: Ransomware

- Wie *funktioniert* Ransomware:
  - Durch Schwachstellen gelangt Schadcode auf Rechner
  - Verbreitung als Wurm oder Trojaner: Wird initial ungewollt „installiert“ und kommt getarnt als legitimes Programm, Bild, PDF…
  - Ransomware unterwandert das System und verschlüsselt sukzessive Daten
- Systeme und Daten werden dadurch nicht mehr zugreifbar und enormer Schaden durch Ausfälle entsteht
  - Dies sind *nur* unmittelbare oder primäre Schäden

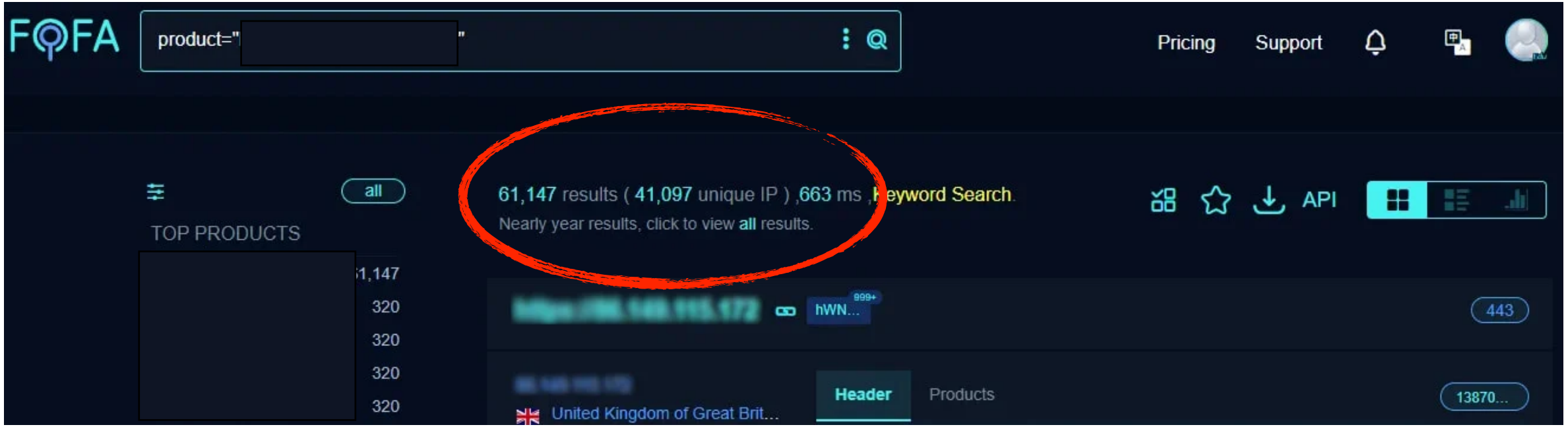
Aktuelles Fallbeispiel 11/24/24: Schwachstellen

- Kritische Schwachstelle in D-Link Produkten
  - Eine 9,2/10
- Schwachstelle erlaubt „os command injection“
- … und das „remote“, d. h. auch über Internetverbindung (Remote Code Execution)
- Angriff wird als „komplex“ und „schwierig“ bewertet
- Der Exploit selbst ist jedoch öffentlich und kann so „verwendet“ werden

Q: https://www.dlink.com/

Q: https://nvd.nist.gov/vuln/detail/CVE-2024-10914

Aktuelles Fallbeispiel 11/24/24: Schwachstellen

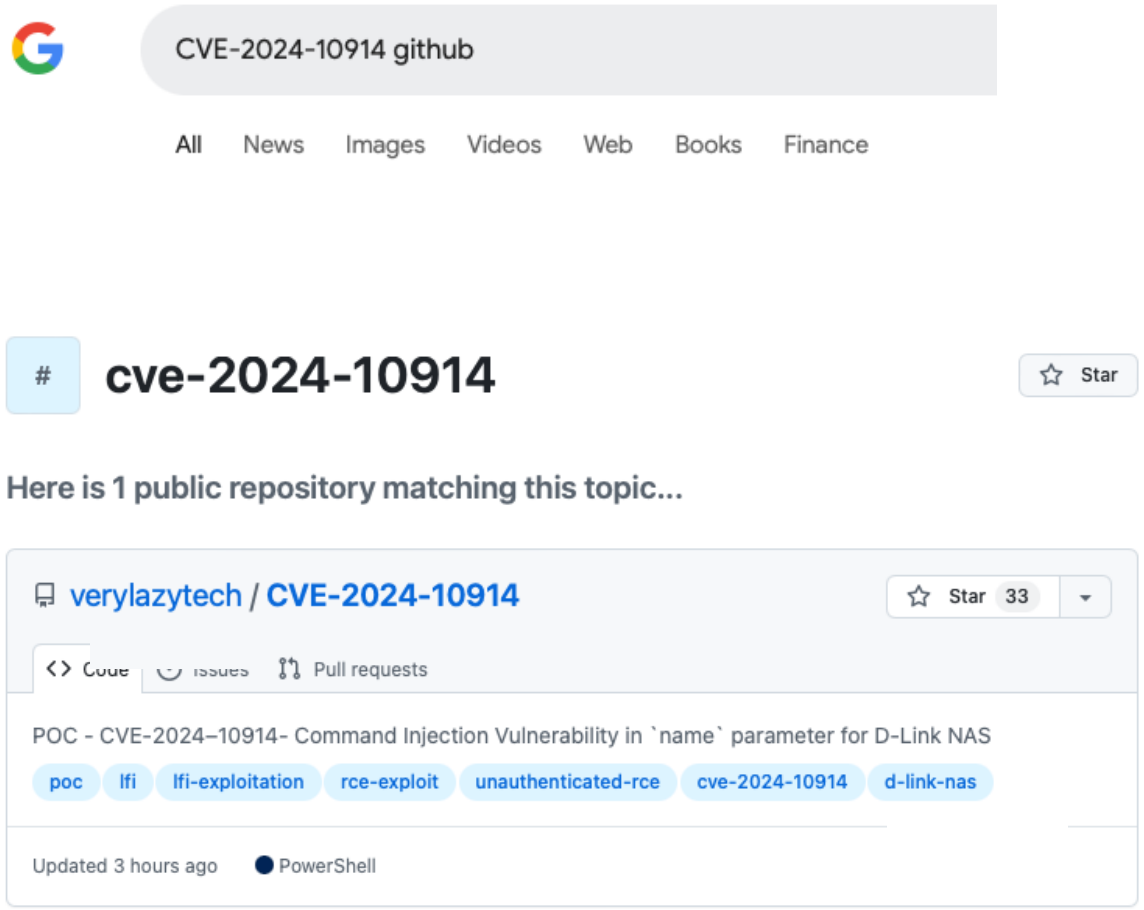


FOFA scan, Quelle: bleepingcomputer.com / Netsecfish

Q: https://www.bleepingcomputer.com/news/security/d-link-wont-fix-critical-flaw-affecting-60-000-older-nas-devices/

Aktuelles Fallbeispiel 11/24/24: Schwachstellen

- D-Link gibt an, dass die betroffenen Produkte nicht mehr unterstützt werden und die Schwachstelle so nicht geschlossen wird.
- Ein Beispielhafter Exploit ist öffentlich.
- Ist der Angriff hier noch „komplex“ und „schwierig“ in der Durchführung?



Q (11/24/24): https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10413

Falsche Annahmen zur Cyber-Sicherheit

Heute sichere Systeme bleiben auch in Zukunft sicher

Perfektionierte Software führt zu sicheren Systemen

Firewalls schirmen unsere Systeme von externen Bedrohungen ab

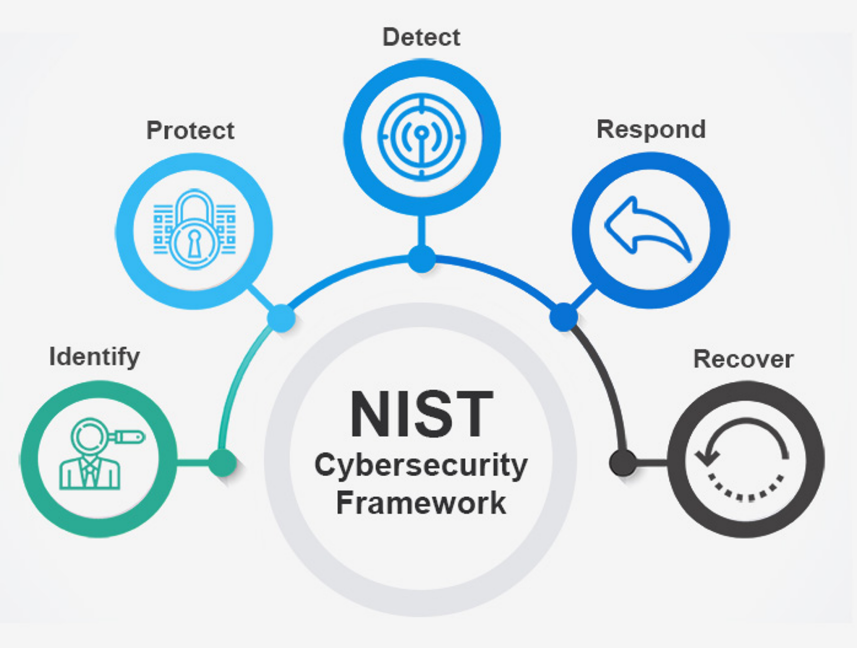
Für sichere Systeme konzentrieren wir uns auf Schutzmaßnahmen wie Verschlüsselung, Zugriffskontrollen, Firewalls, Angriffserkennung (…)

Maßnahmen der IT-Sicherheit

Ein Auszug mit Beispielen

Einige Grundsätze der IT-Sicherheit

- Strukturierung wie folgt:
  - **Identifikation und Planung** von Komponenten, Risiken, Bedrohungen (…)
  - **Schutzmaßnahmen** zur Minimierung von Risiken
  - **Erkennung** von Angriffen und Störungen
  - **Reaktion** auf Angriffe
  - **Wiederherstellung** von Systemen



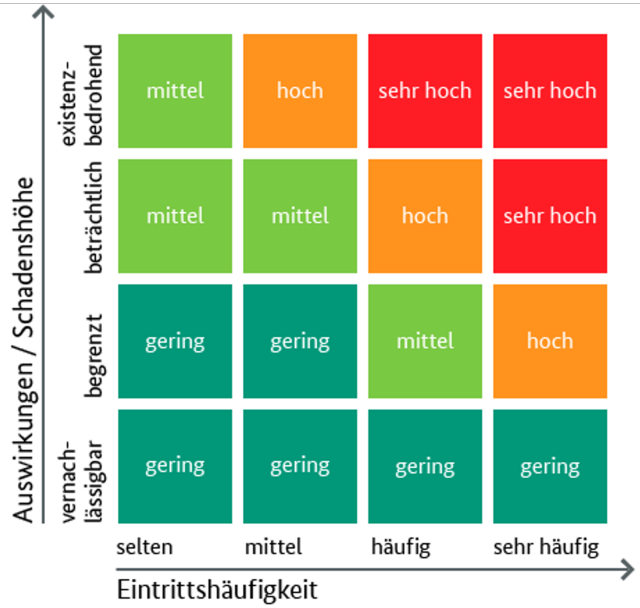
Quelle: NIST Five Functions - Cybersecurity Framework

Risikoanalysen (BSI-Standard 200-3)

Mit ermittelten ***Eintrittshäufigkeiten*** und ***Schadensauswirkungen*** einer Gefährdung kann ***resultierendes Risiko*** bewertet werden.

Zweckmäßiger Ansatz: Eine nicht zu große Anzahl an Kategorien zu verwenden. Drei bis fünf sind üblich, oft werden auch nur zwei Kategorien verwendet.

Der BSI-Standard 200-3 enthält ein Beispiel mit vier Stufen, das an die Gegebenheiten und Erfordernisse angepasst werden kann.



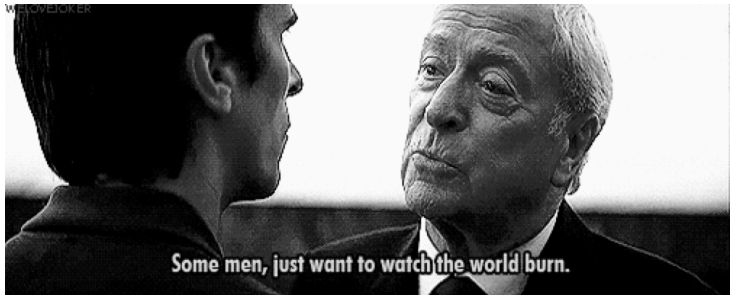
Risikokategorie	Definition
gering	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Maßnahmen bieten einen ausreichenden Schutz.
mittel	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Maßnahmen reichen möglicherweise nicht aus.
hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung. Das Risiko kann mit einer großen Wahrscheinlichkeit nicht akzeptiert werden.
sehr hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung. Das Risiko kann mit einer sehr großen Wahrscheinlichkeit nicht akzeptiert werden.

Bedrohungsanalysen

- **Welche Arten von Angreifern erwarten wir?**
  - System, Person oder Personengruppe, die Angriffe durchführen
  - Beispiel: Hackergruppen, organisierte Kriminalität, Organisationen, Saboteure …
- **Attacker-Model zur Bewertung**
  - Zur Erfassung der verschiedenen Gefährdungslagen, zur Risikoabschätzung z. B. durch Angreifertyp, Fähigkeiten und Motivation.

Profit

Politik



Fun

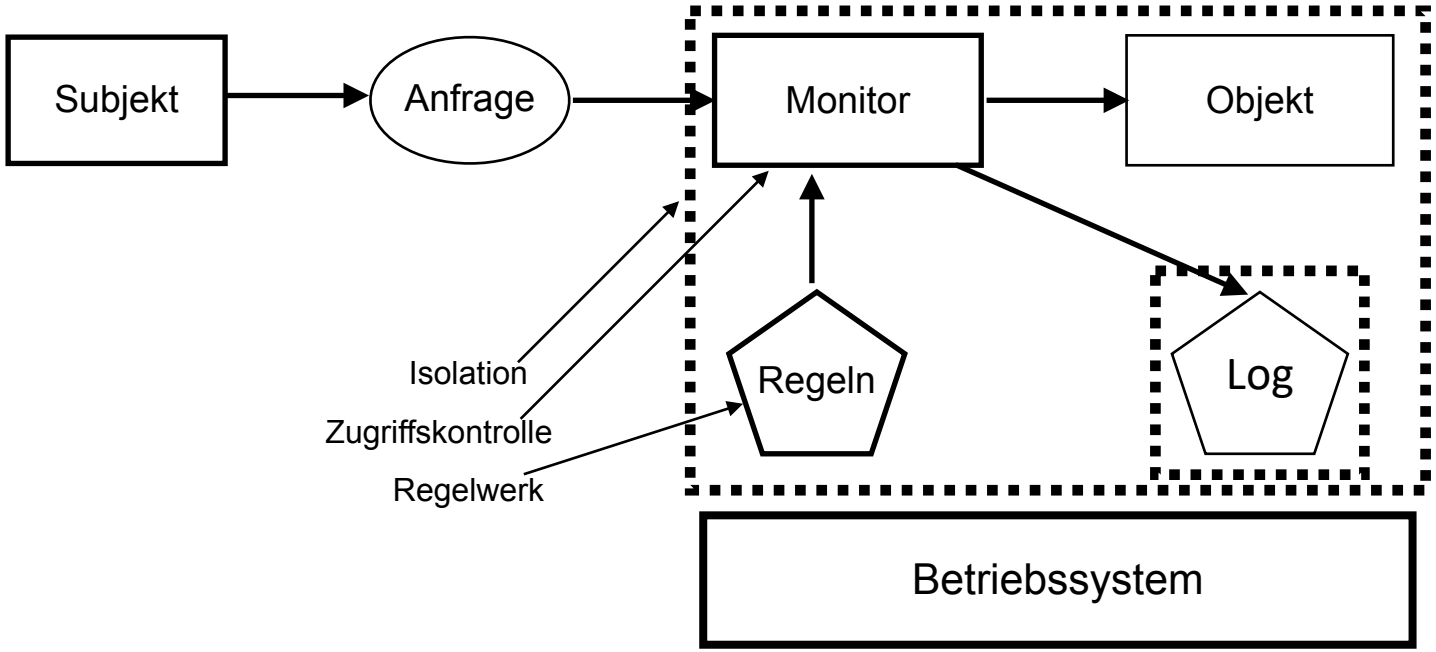
Security By Design

- Idee: Sicherheit von Beginn an, als fester Teil des Systementwurfes
- Aufgabe: Schreibe eine Spezifikation, oder:
  - „*Wie man ein System versteht bevor (oder nachdem) man es gebaut hat.*“—B. Lampson
  - Problematisch: Kein generelles Modell oder Axiome für IT-Sicherheit
  - Problematisch ist Unterscheidung: **Präzise** vs. **ungenaue** Systeme
    - **Präzise**: Banken, SCADA, IIoT, Flugsteuerung …
    - **Ungenau**: Google Suche, News, Social Media
- Welche Sorte System liegt überhaupt vor?
- Welche Bedrohungen liegen vor?
- Was soll im System erlaubt sein und was nicht?

Schutzmaßnahmen: Zugriffskontrolle

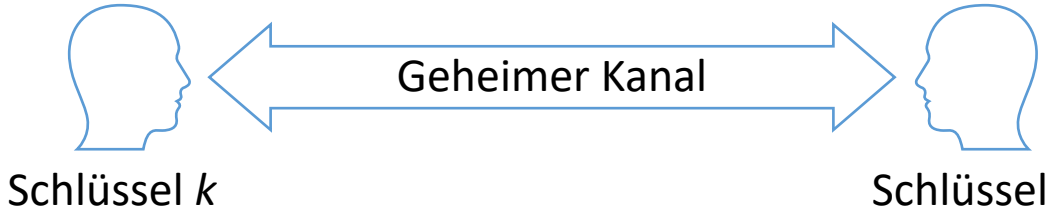
- „Regelt den Umgang zwischen Subjekten und Objekten.“
  - Subjekte können dabei User sein.
  - Objekte können Daten oder Funktionen sein.

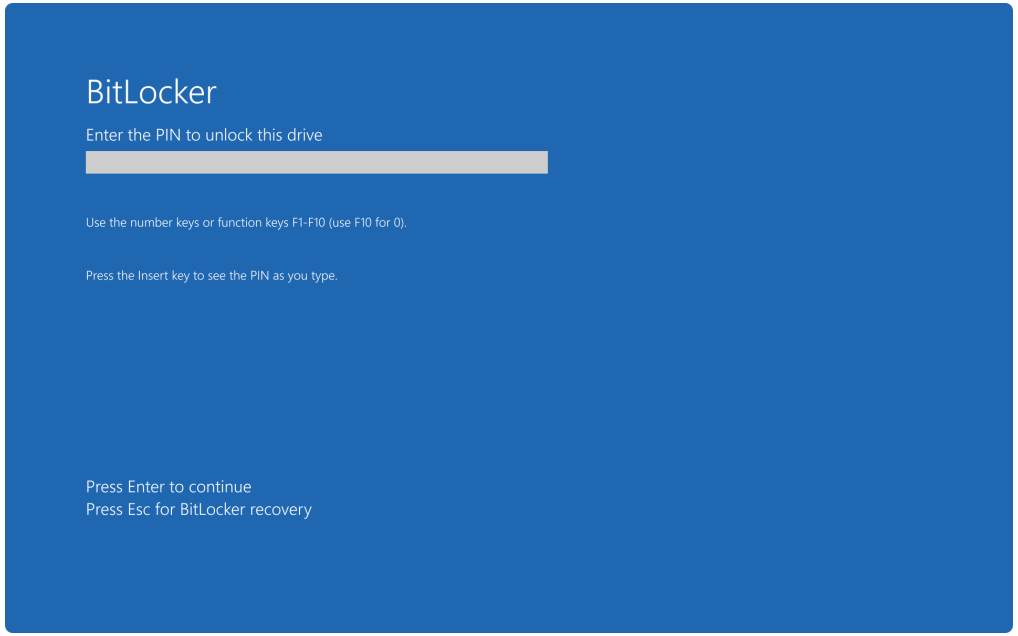
- Blockiert werden soll: User „Malware“ möchte Datei „User-Datenbank“ lesen
-
- Blockiert werden soll: User möchte „Malware.exe“ installieren.



Schutzmaßnahmen: Kryptografie

- Dient u.a. der Geheimhaltung von Daten,
  - wenn diese über öffentliche Kanäle ausgetauscht werden sollen (e.g. Internet, Mail, etc.)
  - Schützt Daten auf der Festplatte vor Zugriffen ohne Kenntnis eines Schlüssels
- Beispiele:
  - Bowser und Internetsicherheit (HTTPS)
  - Festplattenverschlüsselung (Bitlocker)
  - Virtual Private Networks (VPN)



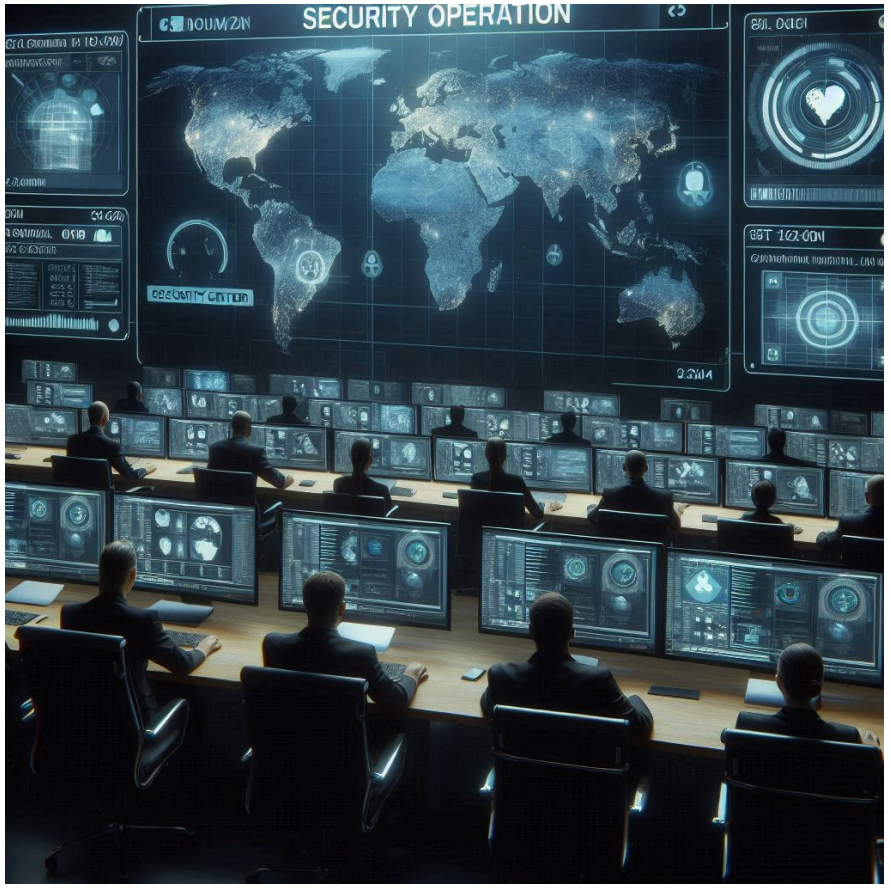


Überwachung und Erkennung: Monitoring trotz Schutzmaßnahmen

- Systeme zur Angriffserkennung und Behandlung
  - Security Information & Event Management
  - Intrusion Detection Systeme
  - Intrusion Prevention Systeme

- Merksatz „Vertrauen ist gut, Kontrolle ist besser.“
  - Taucht in unzähligen Sprachen so oder ähnlich auf…
  - Weisheit daraus: Vorbereitung, Schutz und Vertrauen scheitern und ersetzen kein Monitoring des Produktes
- Schutzmaßnahmen funktionieren oft nicht (mehr):
  - Zeit im Sinne der Angreifenden
    - Legacy Systeme, keine Patches, veraltete Krypto…
    - Warum gelingen Gefängnisausbrüche?
      - Design und Bau: 3 Jahre
      - Insassen: 15+ Jahre
    - Wie hoch war das Security-Budget? -> *Sicherheit ist Ökonomie*.

Monitoring und Response ist in jedem Fall unerlässlich.

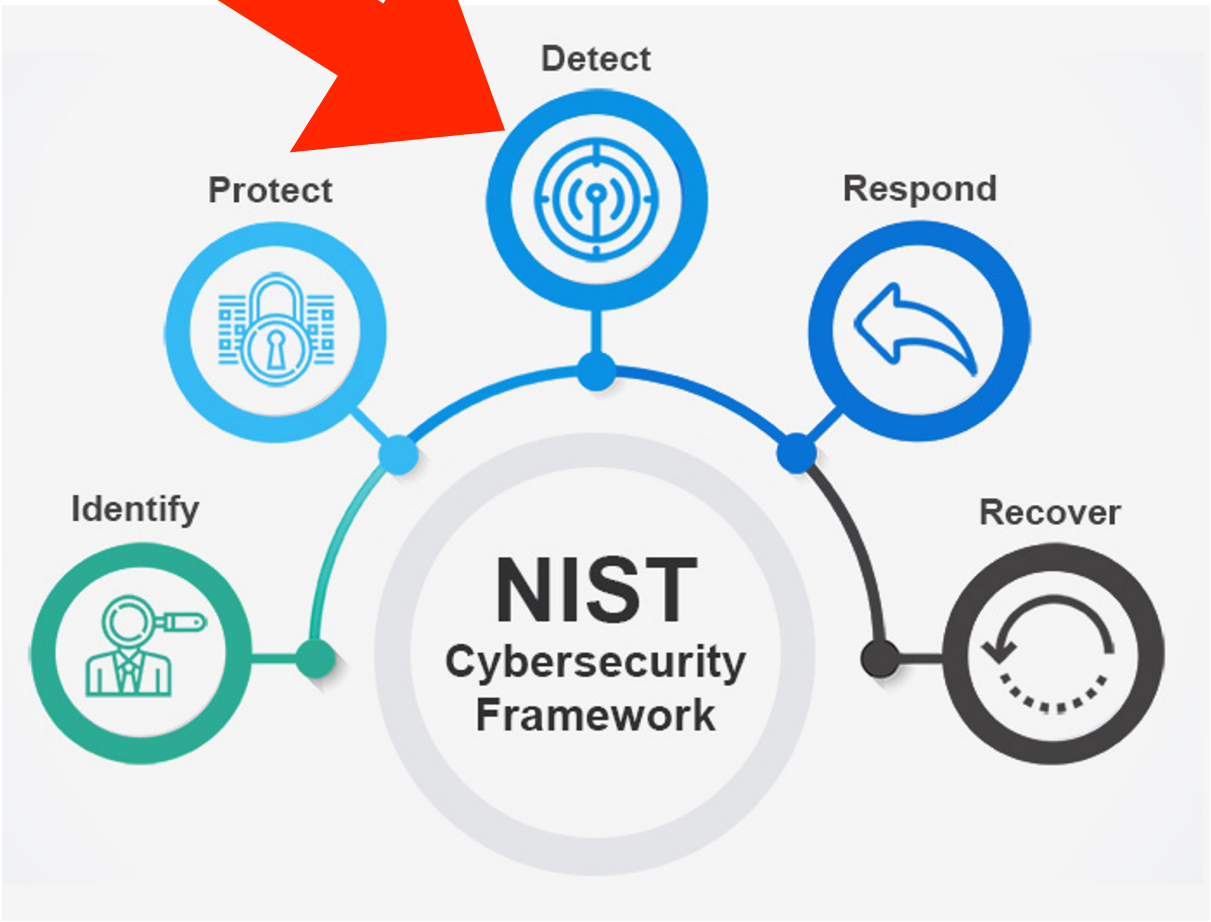


Security Operations Centre (AI Illustration)

Überwachung und Erkennung: Monitoring trotz Schutzmaßnahmen

- **Angriffserkennung**
  - Die Erkennung von Angriffen beruht auf Messungen des Systemverhaltens und Systemzuständen, die Indizien für mögliche Angriffe sind.
    - Boot-Logs, System-Logs, Network-Traffic, User-Login-Times, CPU-Activity, externe Faktoren…
  - Gewöhnlich werden dazu Regel-basierte Verfahren eingesetzt, die Zugriff auf Datenbanken für Angriffe haben:
    - Malware Definition Strings („Virusscanner“)
    - Email Headers und Sender-Listen (Spam-Filtering)
    - Packet- und Content-checking (Deep Inspection)
- **Anomalieerkennung**
  - Weniger spezifische CVEs, Listen, etc. stattdessen Indicators of Compromise (IoCs) und „gelerntes Normalverhalten“
    - **Vorteil**: Wesentlich bessere Erkennungsraten, Möglichkeit auch *Effekte* von 0-Days zu erkennen
    - KI-Basierte Erkennung ist erhöht Vorteil zwischen Kosten (Defense) und Kosten (Offense) deutlich
    - **Problem**: Anomalie ist nicht immer Angriff und nicht jeder Angriff resultiert in Anomalien

Wir sind hier.



Quelle: NIST Five Functions - Cybersecurity Framework

Warum Cyber-Resilienz?

„Neue“ Annahmen für *praktische* Cyber-Sicherheit

- Die Bedrohungslage entwickelt sich weiter, Angriffe passieren ständig, manche werden gelingen
- Systeme arbeiten in potenziell „feindlichen“ Umgebungen
- Die Verfügbarkeit der Systeme muss bestehen bleiben, die Wiederherstellung schnell passieren
- Systeme sollen auch während Angriffen und Störungen Auftrag erfüllen
- Widerstandsfähigkeit und rasche Wiederherstellung sind kritisch für die Verfügbarkeit von Systemen

Cyber-Resilienz nach Cyber Resilience Act?

- EU Cyber Resilience Act (EU-Gesetz über Cyberresilienz)
  - „Von Babymonitoren bis hin zu Smartwatches, Produkte und Software, die eine digitale Komponente enthalten, sind in unserem täglichen Leben allgegenwärtig.“

- Cyber Resilience Act garantiert:
  - harmonisierte Vorschriften für das Inverkehrbringen von Produkten oder Software mit einer digitalen Komponente;
  - einen Rahmen von **Cybersicherheitsanforderungen** für die **Planung**, **Gestaltung**, **Entwicklung** und Wartung solcher Produkte mit Verpflichtungen, die in jeder Phase der Wertschöpfungskette zu erfüllen sind;
  - eine Verpflichtung zur Sorgfaltspflicht für den gesamten Lebenszyklus solcher Produkte.

Quelle: https://digital-strategy.ec.europa.eu/de/policies/cyber-resilience-act

Cyber-Resilienz und Cybersicherheit

Sichtweise auf EU Cyber Resilience Act:

Cybersicherheitsniveau generell steigern und dadurch natürlich Angriffe erschweren.

Das Cyber-Risiko sinkt dadurch.

Cyber-Resilienz bedeutet jedoch nicht schützen und abwehren, bis es nicht mehr geht. Was geschieht während und nach dem Angriff?

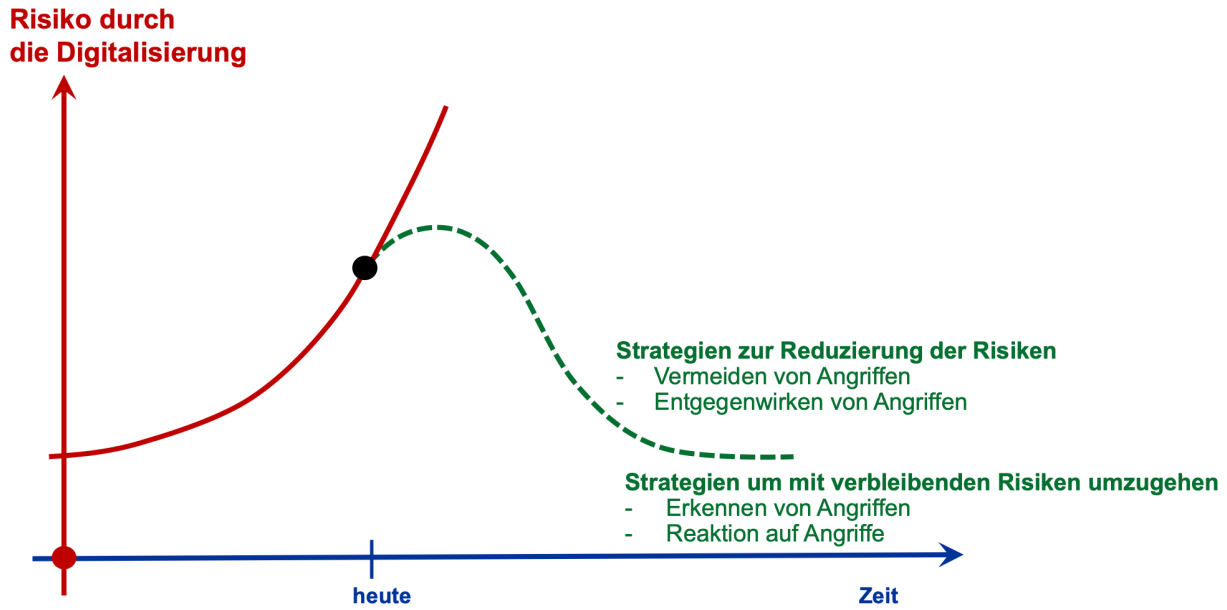
Echte Cyber-Resilienz bedeutet auch, dass ein System auch dann noch *funktioniert*, wenn es angegriffen ist.

Cyber-Sicherheit: Risiken behandeln.

Bedeutet Risiken behandeln (Vermeidung, Reduktion, Transfer oder Akzeptanz).

Bei erfolgreichem Angriff werden so Schäden minimiert.

Eintrittswahrscheinlichkeit, *Schaden* und resultierendes *Risiko* —> Risikoakzeptanz?

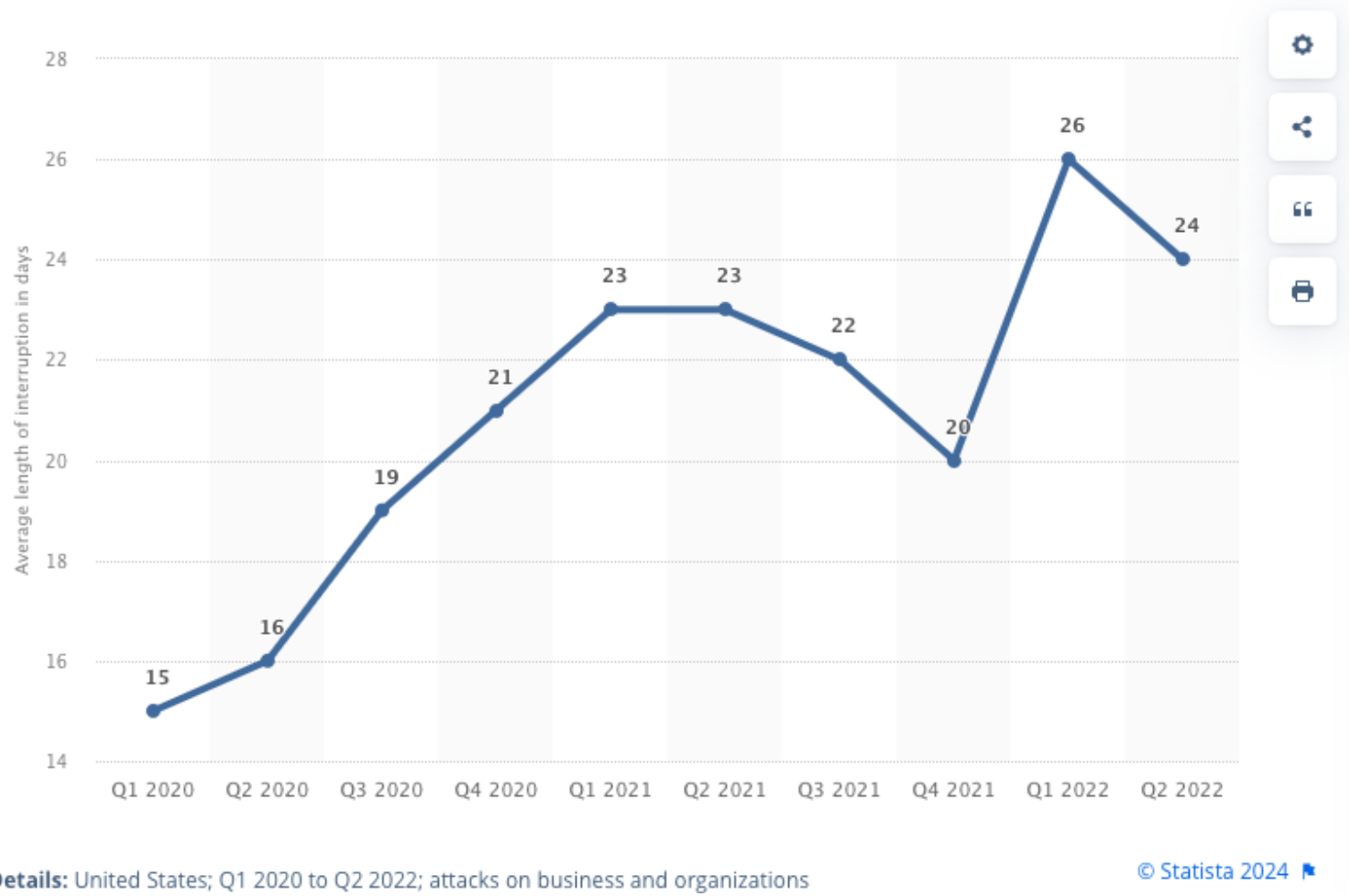


Prof. Dr. Norbert Pohlmann - Sichtweisen IT-Security

Was ist mit dem System bzw. Dienst, was passiert beim „Kunden“?

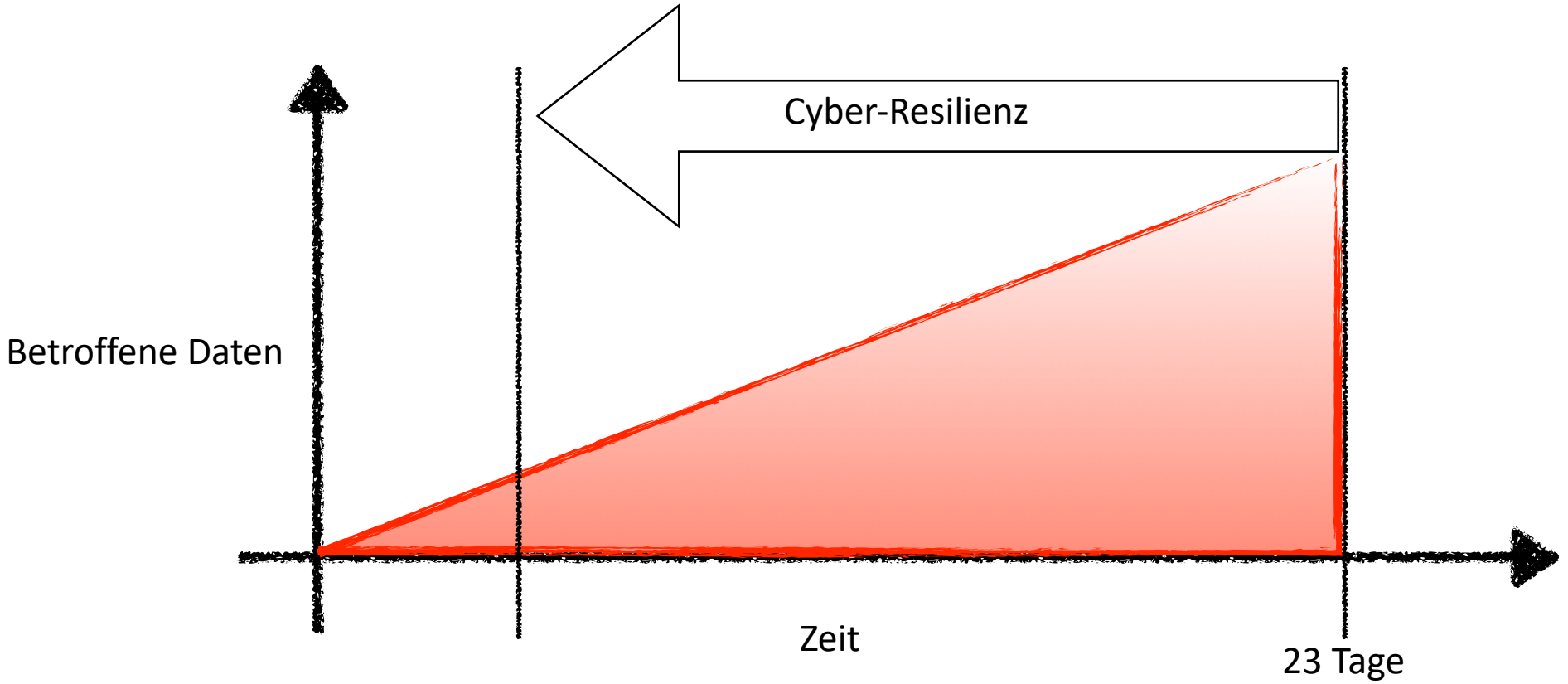
Perspektive Cyber-Resilienz: Schnelle „Erholung“ von Angriffen

- Bei Ransomware-Angriffen im Durchschnitt 23 Tage.



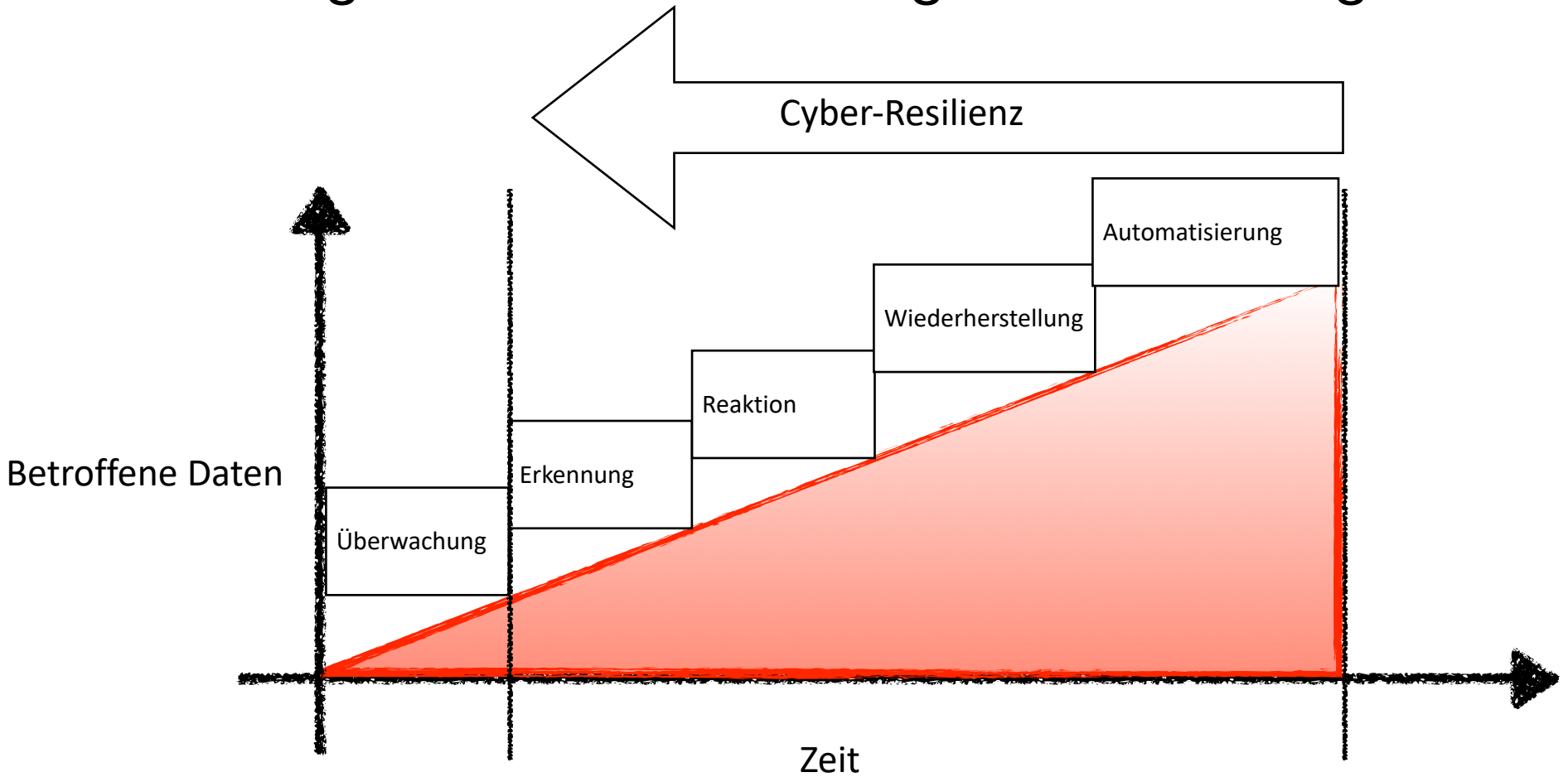
Cyber-Resilienz: Schnelle „Erholung“ von Angriffen

- Zielsetzung: Schnelle Erkennung und Behebung von Angriffen



Cyber-Resilienz: Schnelle „Erholung“ von Angriffen

- Zielsetzung: Schnelle Erkennung und Behebung von Angriffen



Perspektive Cyber-Resilienz: Handlungsfähig bleiben.

Erhöht die Verfügbarkeit und Widerstandsfähigkeit des gesamten Systems.

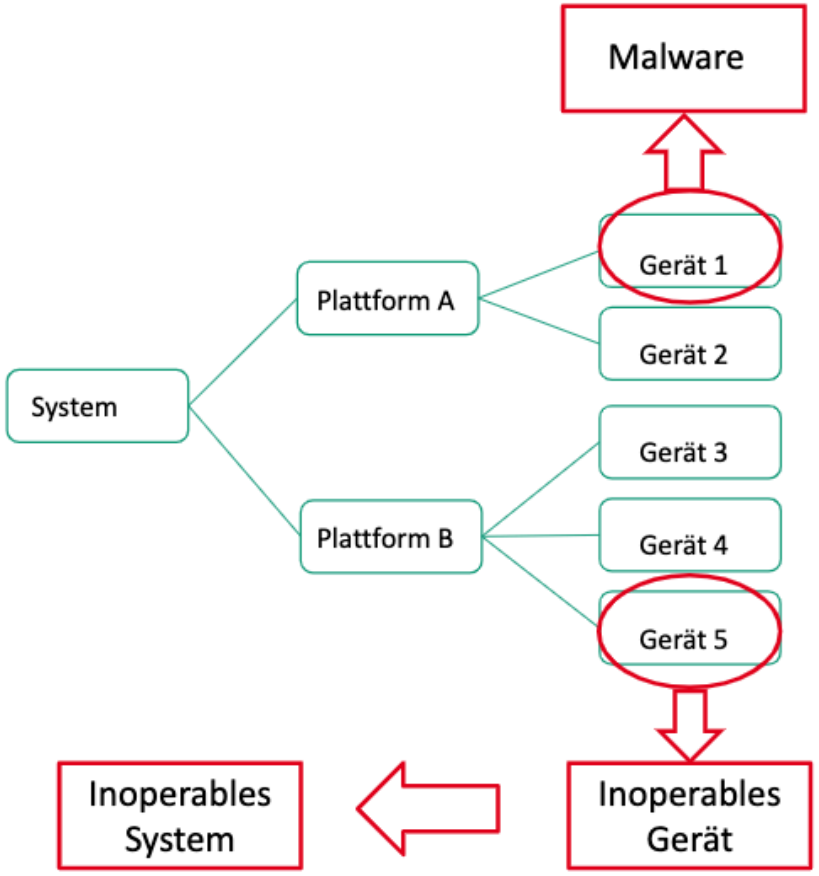
Die Systeme müssen wieder vertrauenswürdig sein und „ihre Aufgaben erfüllen“.

Systeme tolerieren Angriffe und funktionieren auch unter ungünstigen Bedingungen (und kehren zum Normalzustand zurück).

Cyber-Resilienz bezieht sich auf die Fähigkeit, trotz Cyber-Angriffen kontinuierlich die beabsichtigten Missions- oder Geschäftsziele zu erreichen.

Warum ist Handlungsfähigkeit für Cyber-Resilienz so wichtig?

- Fail-Safes, Notlaufmodi, Wiederherstellung
  - Systeme bestehen aus Plattformen
  - Plattformen wiederum aus Geräten
  - Einzelne Geräte sind wichtig für die **Verfügbarkeit** und **Integrität** des Systems
    - Angriffe auf Geräte bedrohen das System!
  - Ausfall von Geräten kann zum Versagen des Systems führen
    - Angriffe können so permanente, physische Schäden verursachen
- Denken Sie hierbei gerne an einen beliebigen KRITIS-Bereich.



Cyber-Resilienz mit Fail-Safes und Wiederherstellung

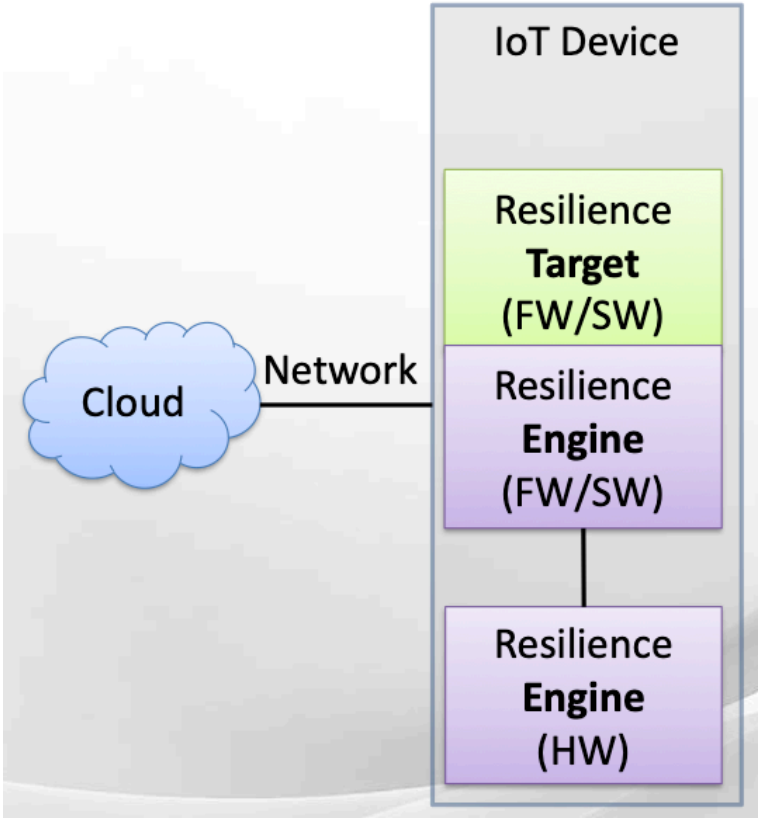
- Fail-Safes sind existenziell für die Betriebssicherheit
  - Redundanz, manual Overwrite, Wiederherstellungsoption
  - Balanciert Security mit Safety

- **Idee**: Wenn Angriffe oder Ausfälle erkannt sind, dann fällt das System in einen „Notlaufmodus“ zurück
  - Notlaufmodi sind minimalistisch, besonders abgesichert, und zur Überbrückung gedacht
  - Systeme können dabei von innen und aussen isoliert werden (Ausschluss aus vertrauenswürdigen Systemen)
  - Fehlerisolation und Schadenbegrenzung

Cyber-Resilienz mit Fail-Safes und Wiederherstellung

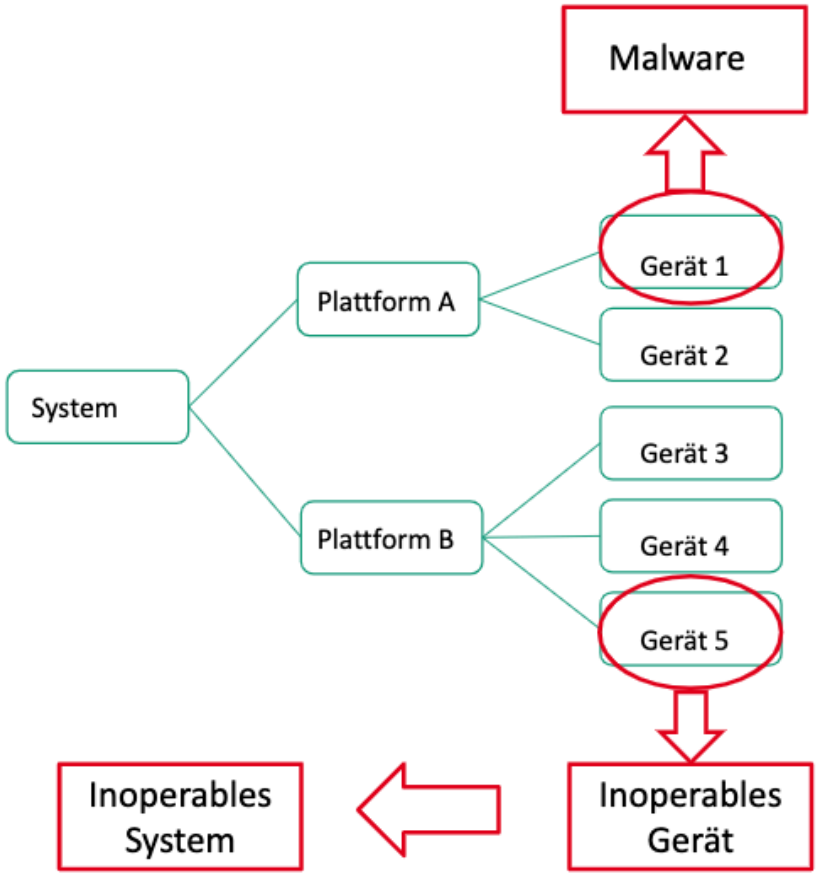
- Wiederherstellung: Aber wie? Das System ist vielleicht nicht erreichbar oder gehorcht nicht mehr.
  - Bsp: „*Totmannschalter*“
    - Fällt das Ziel aus oder ist es kompromittiert, so kann es diesen Zustand nicht beibehalten oder eine Wiederherstellung wird ausgelöst

- **Vorteil**: Reale Chance, Angreifer permanent zu übertrumpfen! Wieso? Ökonomie der Sicherheit.

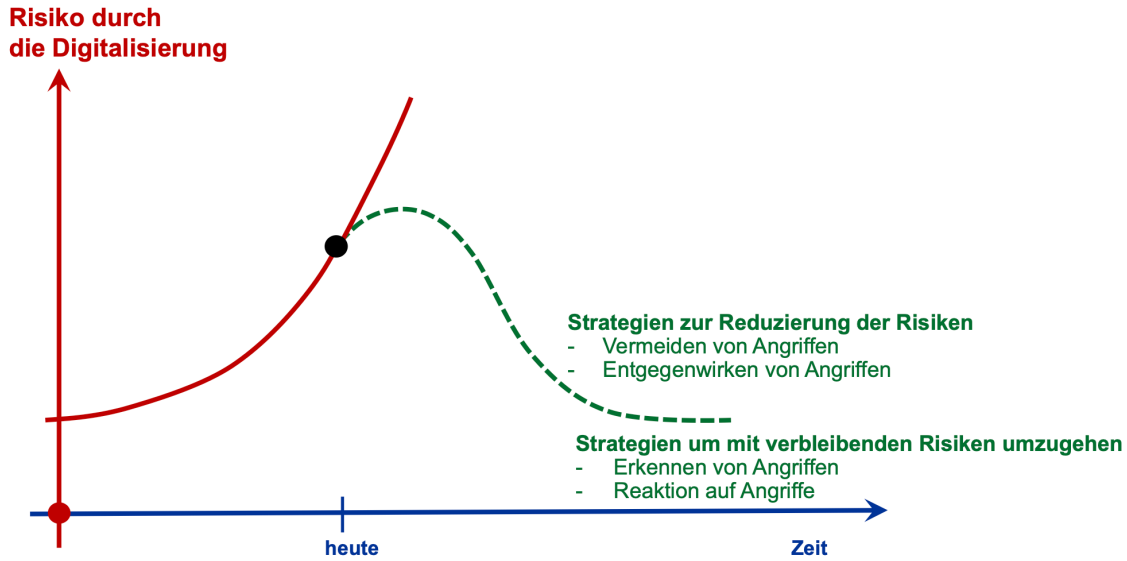


Trusted Computing Group - CyRes

Cyber-Resilienz ist nicht (nur) Cyber-Security.



Cyber-Resilienz erhält Funktion der System.



Prof. Dr. Norbert Pohlmann - Sichtweisen IT-Security

Cyber-Sicherheit reduziert Risiken.

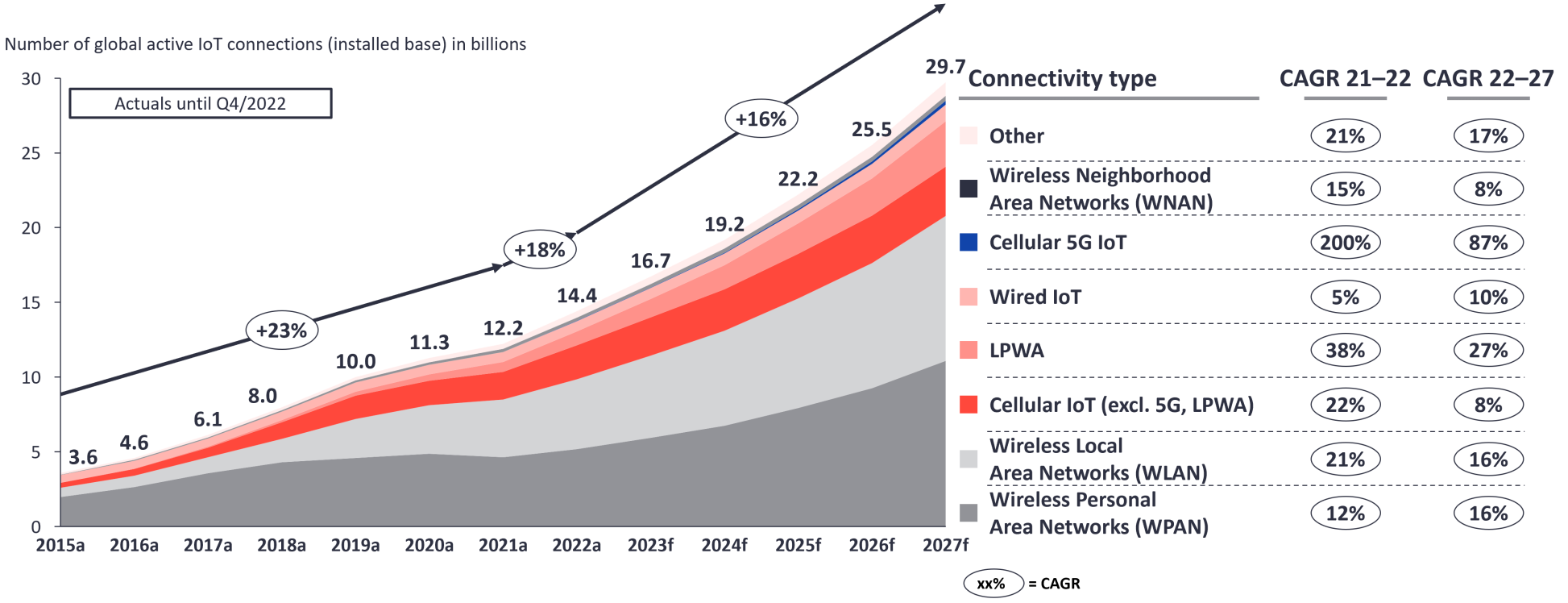
Warum Autonomie? Viele komplexe und verteilte Systeme.

IOT ANALYTICS

May 2023

Your Global IoT Market Research Partner

Global IoT market forecast (in billions of connected IoT devices)



Connectivity type	CAGR 21–22	CAGR 22–27
Other	21%	17%
Wireless Neighborhood Area Networks (WNAN)	15%	8%
Cellular 5G IoT	200%	87%
Wired IoT	5%	10%
LPWA	38%	27%
Cellular IoT (excl. 5G, LPWA)	22%	8%
Wireless Local Area Networks (WLAN)	21%	16%
Wireless Personal Area Networks (WPAN)	12%	16%

Note: IoT connections do not include any computers, laptops, fixed phones, cellphones, or consumers tablets. Counted are active nodes/devices or gateways that concentrate the end-sensors, not every sensor/actuator. Simple one-directional communications technology not considered (e.g., RFID, NFC). Wired includes ethernet and fieldbuses (e.g., connected industrial PLCs or I/O modules); Cellular includes 2G, 3G, 4G, 5G; LPWA includes unlicensed and licensed low-power networks; WPAN includes Bluetooth, Zigbee, Z-Wave or similar; WLAN includes Wi-Fi and related protocols; WNAN includes non-short-range mesh, such as Wi-SUN; Other includes satellite and unclassified proprietary networks with any range.
Source: IoT Analytics Research 2023. We welcome republishing of images but ask for source citation with a link to the original post and company website.

Ausblick: Autonome und intelligente Cyber-Resilienz?

Geräte und Angriffe selbst werden zunehmend „intelligent“ und „autonom“.

Menschliche Akteure werden weder der Menge noch der Dringlichkeit gerecht.

-> Umsetzung der Resilienz-Funktionen.

Zentrales Management von verteilten Systemen ist mindestens widersprüchlich.

Archer TV-Series (2009)

Ausblick: Autonomous Intelligent Cyber-Resilience Agent

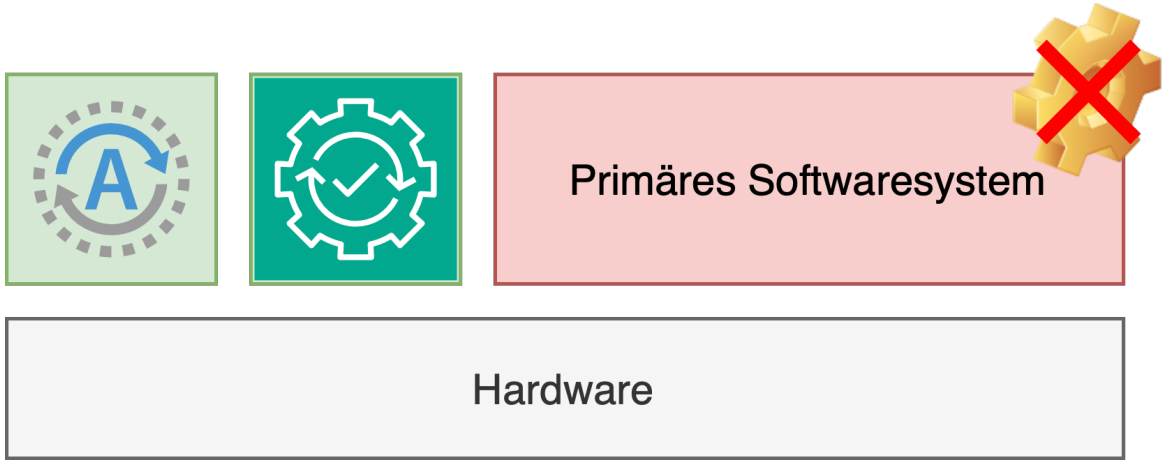
Kennt „primäre Aufgabe“, Auftrag oder Mission

Übernimmt Schutz des Systems

Angriffserkennung und Reaktion alleinstehend, im Verbund oder zentralisiert möglich

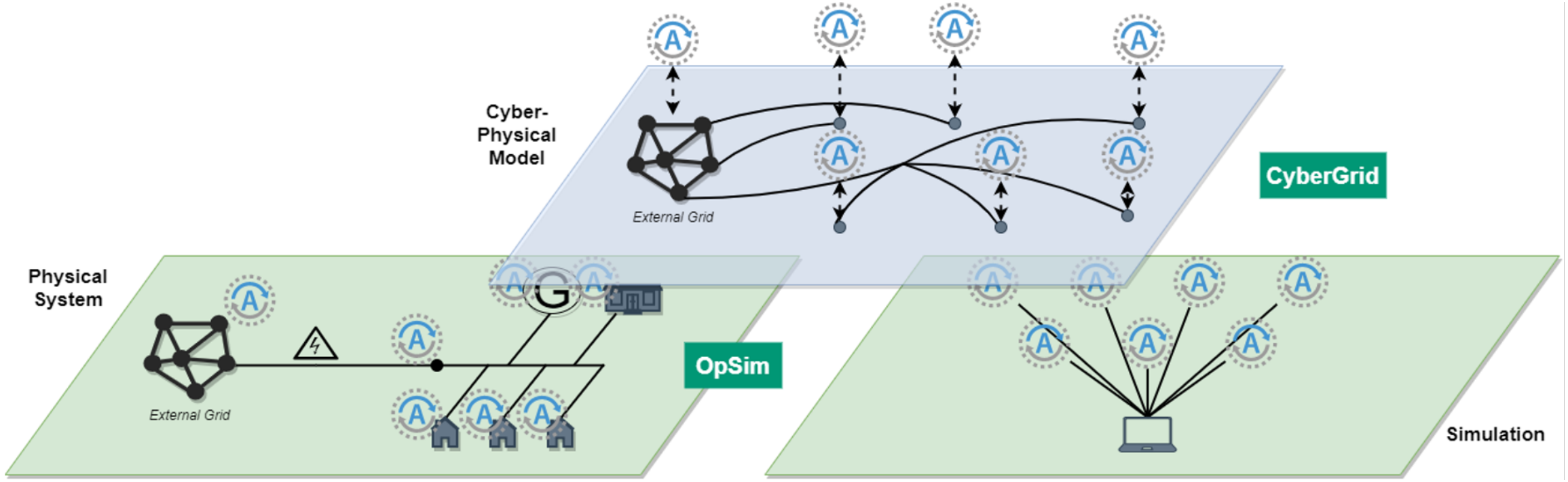
Reaktion auf erkannte Angriffe immer im Bezug auf primäre Aufgabe

Notlaufmodus und Wiederherstellungsoption für das Gerät



Beispielhafte Architektur

Beispielhafte Anwendung: Intelligentes Energienetz



Quelle: H. Lauer; C. Krauß: CyberGrid: Design, Implementation and Evaluation of Security Protocols in Energy Systems

Vielen Dank für Ihre Aufmerksamkeit.

https://www.thm.de/mni/hagen-lauer

Kontakt:
Prof. Dr. Hagen Lauer

hagen.lauer@mni.thm.de