SECaaS.IT
IT-Security made SIMPLE

Was müssen von NIS-2 betroffene Unternehmen und Organisationen tun?

Änderungen gem. NIS2UmsUCG-E (Regierungsentwurf)
(Stand 19.11.2024)

Liste der Top Cyberangriffe Deutschland 2024 / 2023

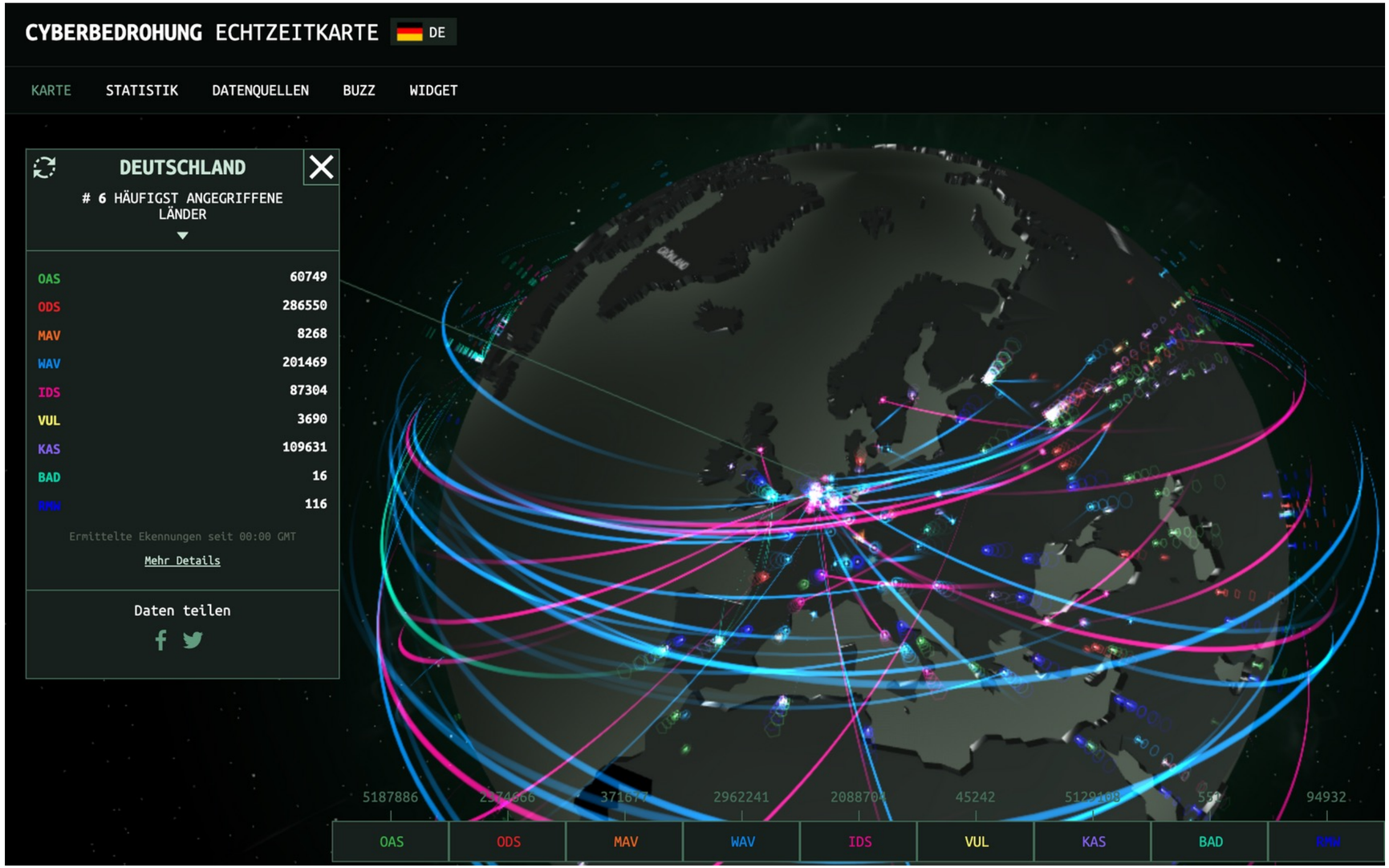
Sie können suchen nach: Bundesland, Ort, Branche, Unternehmen

SEARCH:

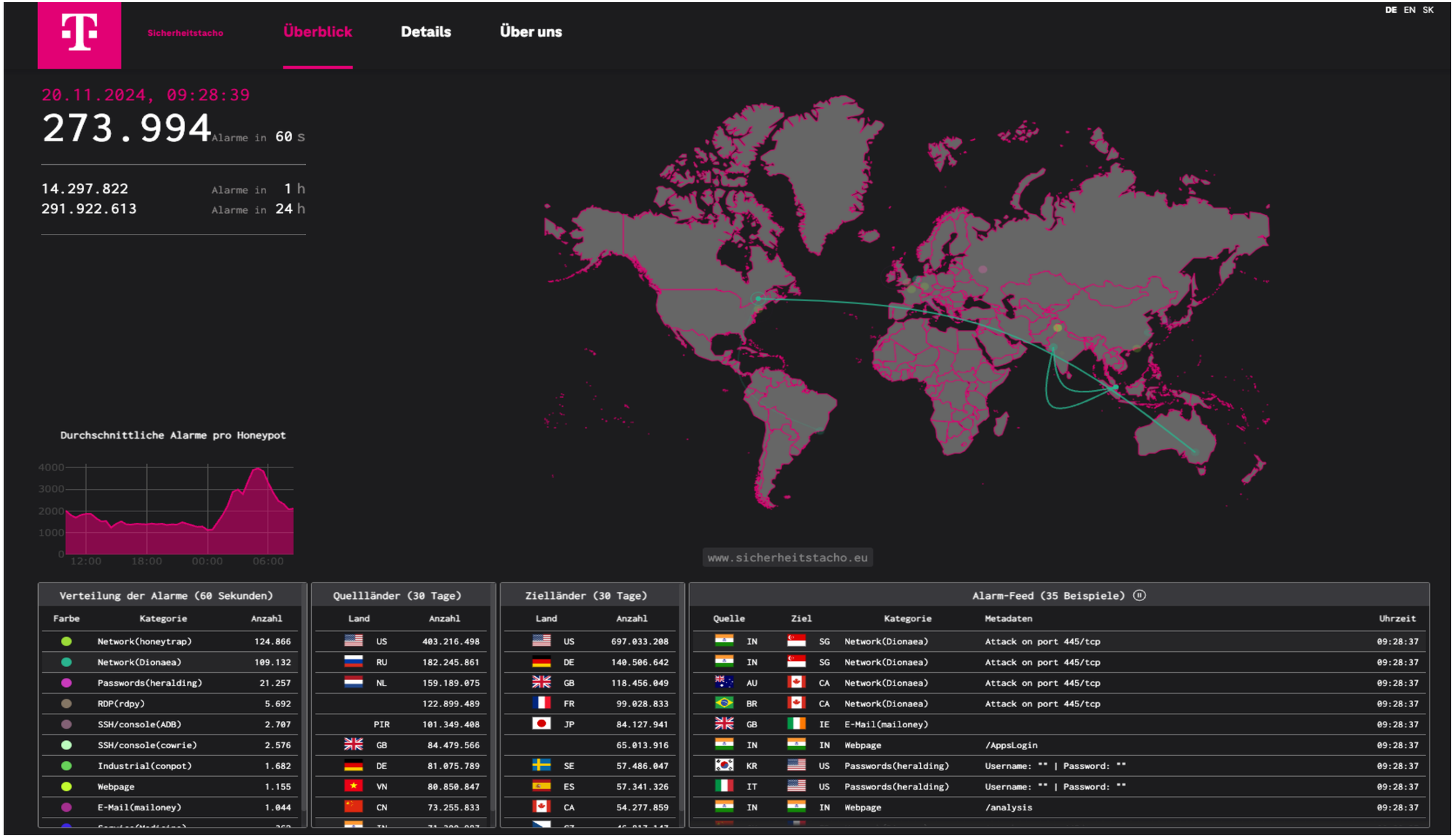
Nr.	Datum	Ort	Land	Unternehmen
1	1. September 2024	Schwabmünchen	BY	Krankenhaus-Betreiber
2	27. August 2024	Werder (Havel)	BB	Politische Partei
3	August 2024 ?	Berlin	BE	Politische Partei
4	August 2024	Langen	HE	Flugsicherungsunternehmen *
5	25. August 2024	Höxter	NW	Hersteller von Antriebsriemen
6	14. Juli 2024	Bitterfeld-Wolfen	ST	Anbieter von Solaranlagen
7	14. Juli 2024	Achern	BW	Entsorgungsunternehmen
8	9. Juli 2024	München	BY	Notarkammer
9	9. Juli 2024	Zweibrücken	RP	Notarkammer
10	6. Juli 2024	Frankfurt/Main	HE	Fachhochschule

* https://www.heise.de/news/Cyberangriff-auf-Deutsche-Flugsicherung-steckt-APT28-dahinter-9853967.html

Quelle: https://konbriefing.com/de-topics/hackerangriff-deutschland.html - Stand 04.03.2024



Quelle: https://cybermap.kaspersky.com/special/ics/de



Quelle: - https://www.sicherheitstacho.eu/start/main#/de/tacho - Stand 20.11.2024

Cyberangriff auf Deutsche Flugsicherung - steckt APT28 dahinter?

Wie die DFS bestätigte, drangen Angreifer in die Büro-IT der Behörde ein. Auf den Flugbetrieb habe der Angriff aus der vergangenen Woche keine Auswirkungen.

43

(Bild: FRED CC BY-SA 3.0)

01.09.2024, 17:59 Uhr Lesezeit: 1 Min. | Security

Alert!

Support ausgelaufen: Attacken auf IP-Kamera von Avtech beobachtet

Derzeit attackiert das Corona-Mirai-Botnet die IP-Kamera AVM1203 von Avtech. Die Kamera wird in öffentlichen Einrichtungen und Industrieanlagen verwendet.

13

(Bild: Gerd Altmann, Public Domain (Creative Commons CC0))

30.08.2024, 09:07 Uhr Lesezeit: 2 Min. | Security

Quelle: https://www.heise.de/thema/Cyberwar

Das (bisherige) IT-Sicherheitsgesetz (IT-SiG 2.0)

Das
„Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ - IT-SiG (2.0)

…wurde am 23.04.2021 im Bundestag verabschiedet und am am 27. Mai 2021 im Bundesanzeiger veröffentlicht.

(BGBl Jahrgang 2021 Teil I Nr. 25)

IT-Sicherheitsgesetz 2.0 (IT-SiG)

Das (bisherige) IT-Sicherheitsgesetz (2.0)

IT-Sicherheitsgesetz (IT-SiG)

Artikelgesetz

Begriff wird i.d.R. verwendet, wenn gleichzeitig eine Gruppe von Gesetzen geändert werden.

Das IT-SiG umfasst u.a. Änderungen an:

- **BSI-Gesetz (BSIG)**
- Atomgesetz (AtG)
- Energiewirtschaftsgesetz (§ 11 Abs. 1d, 1e EnWG)
- Telemediengesetz (TMG)
- Telekommunikationsgesetz (§ 109, 113, TKG)
- Bundesbesoldungsgesetz (BBG)
- Bundeskriminalamtgesetz (BKAG)
- Außenwirtschaftsverordnung (§ 55 (1) S. 2, Nr. 2 AWV)
- Zehnten Buches Sozialgesetzbuch (§67 c (3) SGB X)

Grundlagen

Regelungen bzgl. Cybersicherheit in der EU

Quelle:https://www.digitalbusiness-cloud.de/nis2-schutz-der-kritischen-infrastruktur-vor-cyberangriffen/
https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-FAQ/FAQ-zu-NIS-2_node.html

Das ändert sich

NIS2 Directive ((EU) 2022/2555) => NIS2UmsuCG:

- **Fokus:** Cybersecurity und Informationstechnik
- **Betroffen:** KRITIS-Betreiber + besonders wichtige Einrichtungen
- + wichtige Einrichtungen
- **Schutzobjekt:** Große Teile der Wirtschaft
- **Aufsicht:** (BSI) + EU

EU-Richtlinie über die Resilienz kritischer Einrichtungen (EU RCE Directive (EU 2022/2557)

=> KRITIS Dachgesetz

- **Fokus:** Physische Sicherheit und Resilienz
- **Betroffen:** Kritische Anlagen (KRITIS-Betreiber)
- **Schutzobjekt:** Große Teile der Wirtschaft
- **Aufsicht:**(BBK) Bevölkerungsschutz und Katastrophenhilfe

Quelle: https://www.openkritis.de/r/OpenKRITIS_NIS2_KRITIS-Dachgesetz_Betreiber.pdf

IT-SiG 2.0 => BSIG (neu BSIG 3.0)

Das BSIG regelt die Aufgaben und Befugnisse des Bundesamts für Sicherheit in der Informationstechnik (BSI), das als zentrale Behörde für die IT-Sicherheit fungiert. Zu den wichtigsten Zielen gehören:

1. Schutz kritischer Infrastrukturen (KRITIS): Das BSIG stellt sicher, dass Betreiber kritischer Infrastrukturen Maßnahmen zum Schutz ihrer IT-Systeme ergreifen.

2. Sicherheitsstandards: Das BSI entwickelt und fördert Sicherheitsstandards für IT-Systeme, um die Informationssicherheit in Unternehmen und Behörden zu verbessern.

3. Prävention und Beratung: Das BSI informiert und berät sowohl öffentliche Stellen als auch die Privatwirtschaft über Risiken im Bereich der IT-Sicherheit.

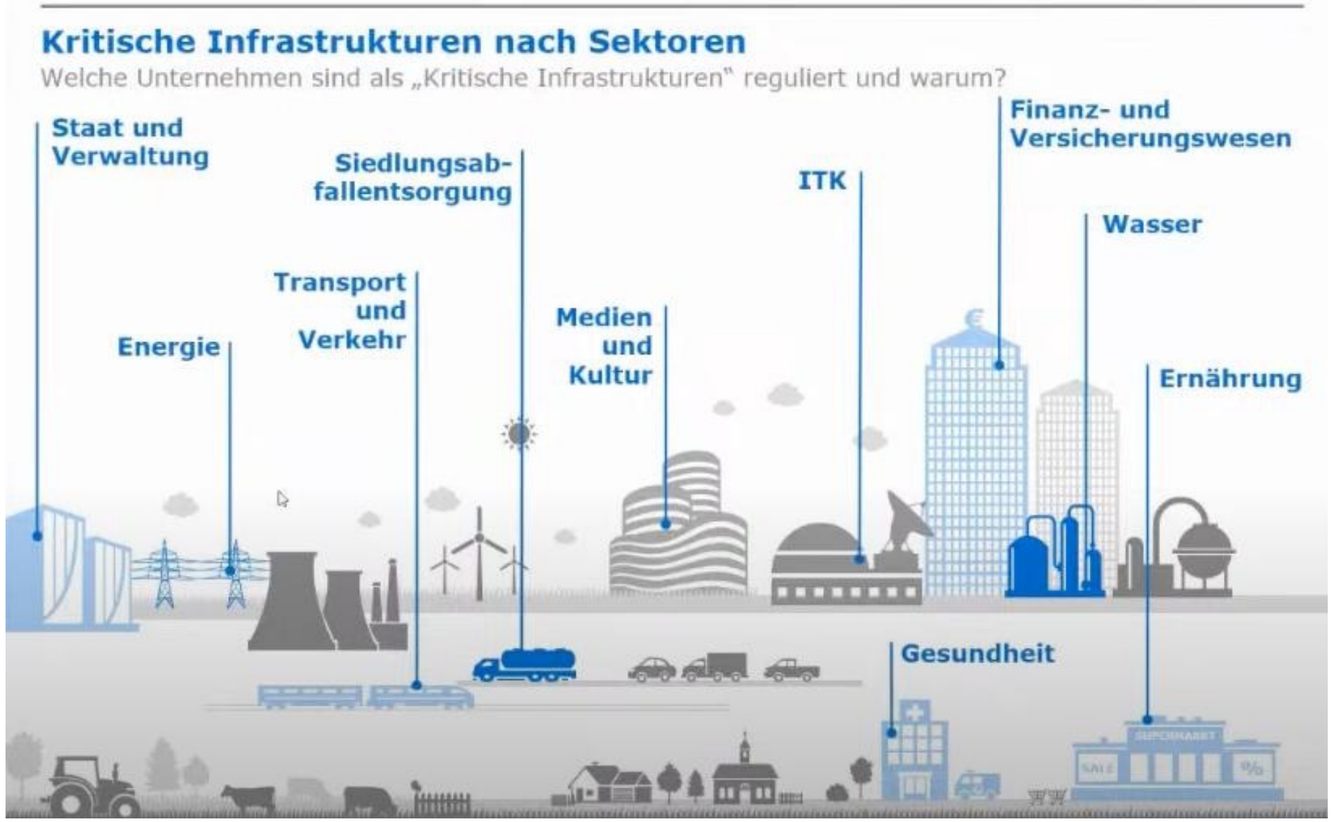
4. Überwachung und Meldungen: Das Gesetz verpflichtet Betreiber kritischer Infrastrukturen, Sicherheitsvorfälle an das BSI zu melden.

Grundlagen

Die Kritische Infrastrukturen (KRITIS - ITSiG)

- **Definition:**
- **Kritische Infrastrukturen** (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen.

- Deren Ausfall oder Beeinträchtigung bewirkt nachhaltig Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen.

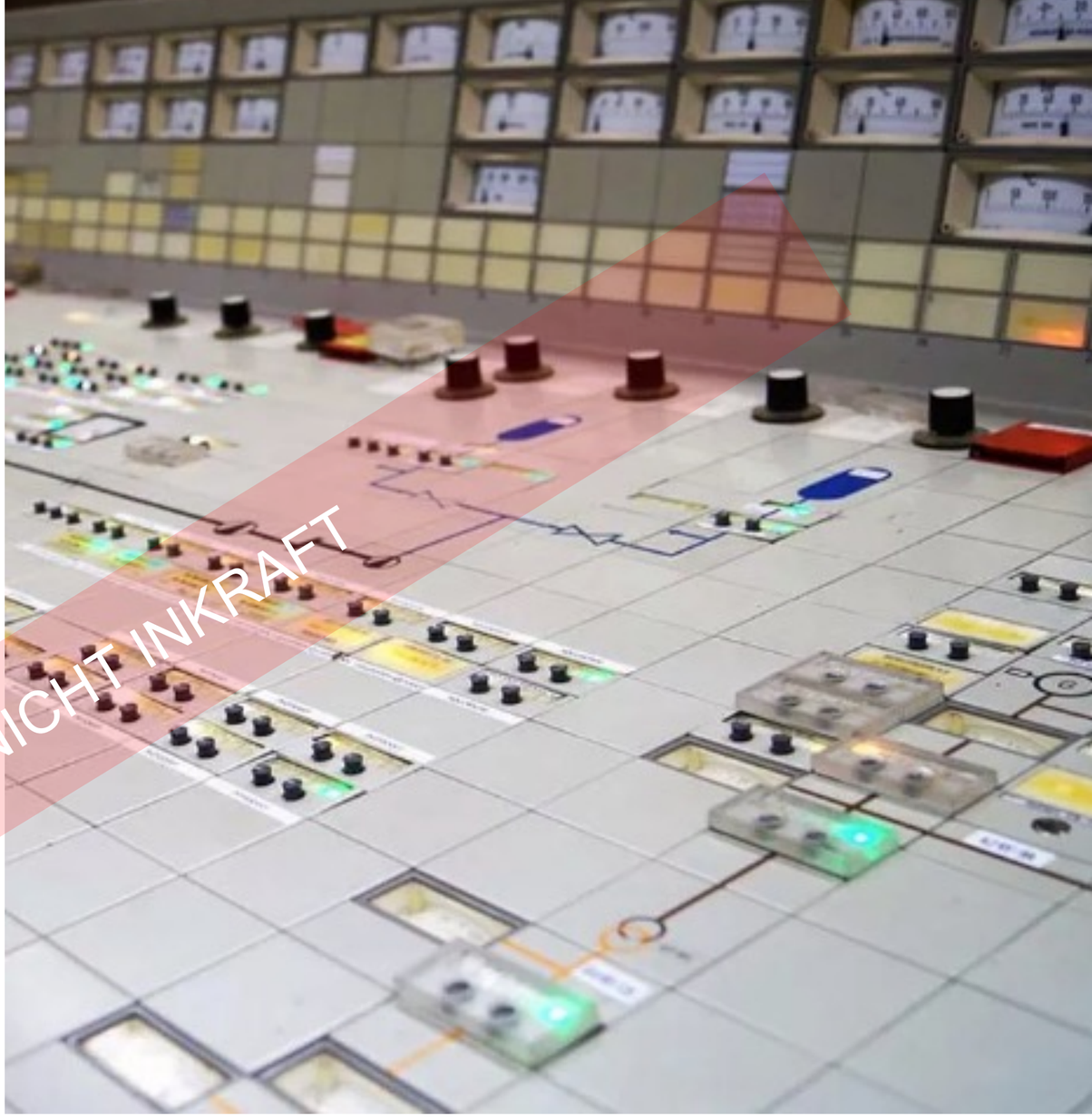


Quelle: https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/kritische-infrastrukturen_node.html

Neu – NIS2UmsGC-E

Definition:
Kritische Anlage
(§ 2 Nr. 22 NIS2UmsuCG)

- Eine Anlage, die für die Erbringung einer kritischen Dienstleistung erheblich ist; die kritischen Anlagen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 56 Absatz 4 näher bestimmt;



Neu – NIS2UmsGC-E

Definition:
Besonders wichtige Einrichtung
(§ 28 Abs. 1 NIS2UmsuCG)

- sonstige natürliche oder juristische Personen oder rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft,
  - mindestens 250 Mitarbeiter
  - Jahres**umsatz** 50 Millionen Euro und zudem
  - eine **Jahresbilan**zsumme über 43 Millionen Euro

NOCH NICHT IN KRAFT

Neu – NIS2UmsGC-E

Definition:

Wichtige Einrichtung

(§ 28 Abs. 2 NIS2UmsuCG)

- Vertrauensdiensteanbieter
- Anbieter öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze,
  - weniger als 50 Mitarbeiter
  - Jahresumsatz und eine Jahresbilanzsumme von jeweils 10 Millionen Euro oder weniger

Neu – NIS2UmsGC-E

NOCH NICHT IN KRAFT

Übersicht der betroffenen Unternehmen

Unternehmen	Sektoren	Mitarbeiter	Umsatz	Bilanz-summe
Besonderes wichtige Einrichtungen	NIS2 – Anlage 1	≥ 250 MA	> 50€ Mio	> 43€ Mio
Wichtige Einrichtungen	NIS2 – Anlage 1 NIS2 – Anlage 2	≥ 50 MA	> 10€ Mio	> 10€ Mio
Kritische Anlagen	KRITIS-Sektoren	Schwellenwerte gem. BSI-KritisVO		

Quelle: https://www.openkritis.de/r/OpenKRITIS_NIS2_KRITIS-Dachgesetz_Betreiber.pdf

Synopse BSIG 2.0 vs. NIS2UmsCG-E (Stand 02.10.2024) 1/2

NOCH NICHT INKRAFT

Kategorie	BSIG	§	NIS2UmsuCG	§
Betroffene Unternehmen	Betroffen sind KRITIS-Betreiber und bestimmte Unternehmen im öffentlichen Interesse (UNBÖFI).	§8a, §8f	Erweitert auf eine breitere Gruppe, einschließlich "**wichtiger (wE)**" und "**besonders wichtiger Einrichtungen (bwE)**" ", was mehr Unternehmen erfasst, z.B. größere Mittelständler, dadurch auch die Zulieferer betrifft, da diesen den Anf. Entsprechen müssen	§28 (1), (2)
Risikomanagement	Verpflichtung zur Umsetzung von IT-Sicherheits-maßnahmen bei KRITIS, spezifische Prüfungen.	§8a	Umfassendere Anforderungen an das Risikomanagement für **wichtiger**" und "**besonders wichtiger Einrichtungen**“ und **Betreibern kritischer Anlagen,** Maßnahmen nach Stand der Technik, inklusive Sicherheit der Lieferkette, Systeme zur Angriffserkennung	§30 (1, 2 Nr. 4), §31
Meldepflichten	Pflicht zur Meldung erheblicher Sicherheits-vorfälle an das BSI, jedoch auf KRITIS-Anlagen beschränkt.	§ 8b	Gestaffelte Meldepflichten, innerhalb von 24 und 72 Stunden bei Sicherheitsvorfällen, Zwischen- und Abschlussmeldung nach spätestens einem Monat	§32

Synopse BSIG 2.0 vs. NIS2UmsCG-E (Stand 02.10.2024) 2/2

NOCH NICHT INKRAFT

Kategorie	BSIG	§	NIS2UmsuCG	§
Governance	Überwachung durch das BSI, spezifische Anforderungen an die Nachweise der KRITIS-Betreiber.	§8a, §8f	Umfassendere Governance-Anforderungen, eine **explizite Haftung der Geschäftsleitung** für Verstöße und Verpflichtung der **regelmäßigen** Teilnahme an Schulungen	§38
Nachweispflicht	Regelmäßiger (alle 2 Jahre) Nachweis der IT-Sicherheit durch externe Prüfungen und Vorlage beim BSI.	§8a (3), §8a (4)	Regelmäßiger (alle 3 Jahre) Nachweis der IT-Sicherheit durch externe Prüfungen und Vorlage beim BSI.	§39
Sanktionen	Bußgelder bei Verstößen, bis zu 20 Millionen Euro oder 4% des weltweiten Umsatzes.	§14	Bußgelder bis zu 7 (wE) / 10 (bwE) Millionen Euro bzw. 2,0% (bwE) / 1,4% (wE) des weltweiten Umsatzes, plus spezifische Sanktionen für verschiedene Einrichtungen.	§65 (5) – (7)

Pflichten der betroffenen Unternehmen

Sicherheit der IT Kritischer Infrastrukturen

- **Betreiber:** Muss angemessene Vorkehrungen nach dem **“Stand der Technik”** treffen
- **Betreiber:** Muss Systeme zur Angriffserkennung einsetzen
- **Betreiber /Branchenverbände:** Können “Branchenspezifischer Sicherheitsstandards” (B3S) vorschlagen
- **Betreiber:** Auditierungspflicht (mindestens alle 3 Jahre)
- **Betreiber:** Nachweis gegenüber BSI von Ergebnissen und Sicherheitsmängeln (ggf. auch Dokumentation)
- **BSI:** Bei Sicherheitsmängeln → ggf. Einbindung der jeweilig zuständigen Aufsichtsbehörde

Melde- und Informationswesen (zentrale Meldestelle)

- **BSI:** Erstellung/Verteilung von Warnungen & Lagebildern
- **Betreiber:** Meldepflicht von (erheblichen) Störungen
- **Betreiber:** hat Informationsrecht

Bildquelle: The noun project , https://geschaeftskunden.telekom.de/vernetzung-digitalisierung/digitale-angebote/business-continuity-solutions

BSI-Gesetz (BSIG)

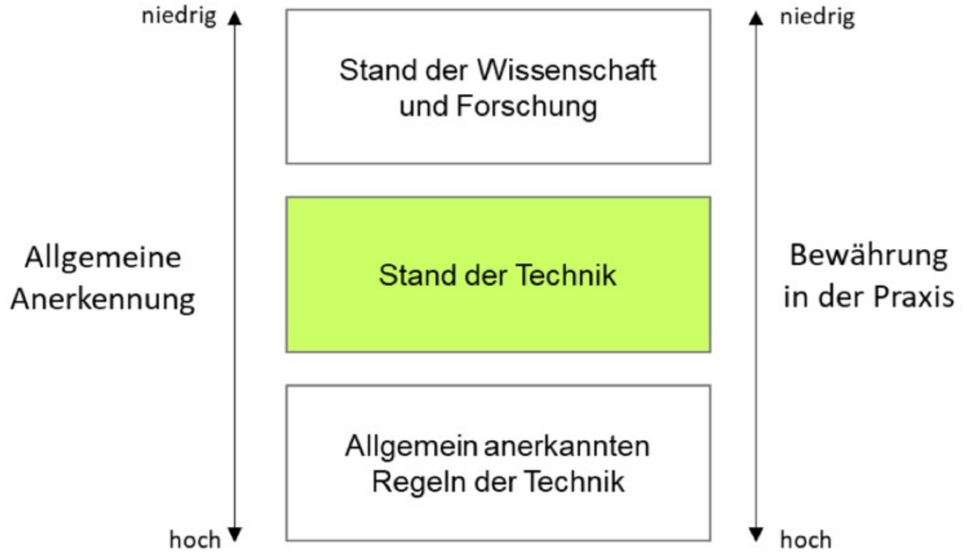
Stand der Technik

Drei-Stufen-Theorie nach Kalkar-Entscheidung d. Bundesverfassungsgerichts 1978*

„Der Stand der Technik bezeichnet die am Markt verfügbare Bestleistung eines Subjekts zur Erreichung eines Objekts.

Subjekt ist die **IT-Sicherheitsmaßnahme**;

Objekt ist das **gesetzliche IT-Sicherheitsziel**.“**



* BVerfGE, 49, 89 [135 f]
** Bundesverband IT-Sicherheit e.V. (TeleTrust) Handreichung zum „Stand der Technik“ technischer und organisatorischer Maßnahmen, Stand 2020, S. 11
Bundesverband IT-Sicherheit e.V. (TeleTrust) / European Network and Information Security Agency (enisa) Guideline „State of the art“ – Technical and organisational measures, Vers. 2021, p. 11

Neu – NIS2UmsGC-E

Nachweispflichten für Betreiber kritischer Anlagen § 30 / § 39 NIS2UmsuCG

NOCH NICHT INKRAFT

1. Besonders wichtige Einrichtungen und kritische Einrichtungen sind verpflichtet, **geeignete, verhältnismäßige** und **wirksame technische und organisatorische Maßnahmen**, die nach Absatz 2 konkretisiert werden, zu ergreifen.

2. Die Einhaltung der Verpflichtung […] ist durch die Einrichtungen zu dokumentieren.

3. Maßnahmen nach Absatz 1 **sollen den Stand der Technik einhalten** […] und müssen zumindest Folgendes umfassen.

4. **Sicherheit der Lieferkette** einschließlich sicherheitsbezogener Aspekte der Beziehungen.

Pflichten der betroffenen Unternehmen

Sicherheit der IT Kritischer Infrastrukturen

- **Betreiber:** Muss angemessene Vorkehrungen nach dem **“Stand der Technik”** treffen
- **Betreiber:** Muss Systeme zur Angriffserkennung einsetzen

- **Betreiber /Branchenverbände:** Können “Branchenspezifischer Sicherheitsstandards” (B3S) vorschlagen
- **Betreiber:** Auditierungspflicht (mindestens alle 3 Jahre)
- **Betreiber:** Nachweis gegenüber BSI von Ergebnissen und Sicherheitsmängeln (ggf. auch Dokumentation)
- **BSI:** Bei Sicherheitsmängeln → ggf. Einbindung der jeweilig zuständigen Aufsichtsbehörde

Melde- und Informationswesen (zentrale Meldestelle)

- **BSI:** Erstellung/Verteilung von Warnungen & Lagebildern
- **Betreiber:** Meldepflicht von (erheblichen) Störungen
- **Betreiber:** hat Informationsrecht

Bildquelle: The noun project , https://geschaeftskunden.telekom.de/vernetzung-digitalisierung/digitale-angebote/business-continuity-solutions

Pflichten der KRITIS-Betreiber

Einsatz von Systemen zur Angriffserkennung (SzA)

§ 8 a (1a) BSIG (2.0)
§ 31 Abs. 2 BSIG (3.0)

Bildquelle: Free-Photos auf Pixabay

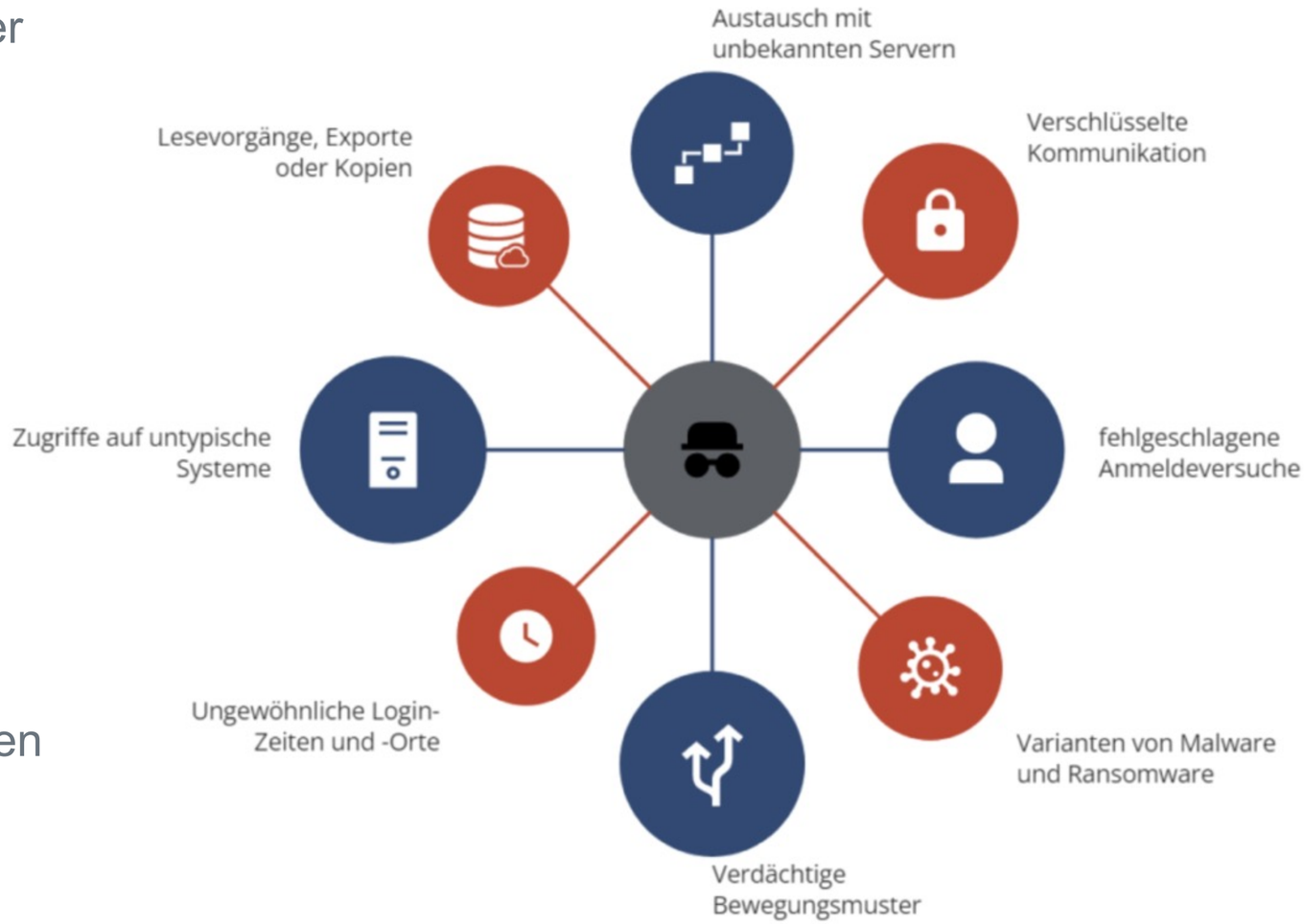
- Die Verpflichtung […] angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst ab dem […] auch den Einsatz von Systemen zur Angriffserkennung.

- Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten.

Systeme zur Angriffserkennung (SaZ)

Systeme zur Angriffserkennung sind nach der Definition aus § 2 Absatz 9b Satz 1 BSIG Prozesse, die durch technische Werkzeuge und organisatorische Einbindung unterstützt werden,

- zur fortlaufenden Auswertung der gesammelten Informationen (Protokollierung)
- um sicherheitsrelevante Ereignisse erkennen (Detektion)
- zur Angriffserkennung, um mit Maßnahmen Störungen infolge von Angriffen zu verhindern oder auf sie zu reagieren (Reaktion)



Quelle: Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung, V. 1.0 v. 26.09.2022, S. 6,7

Systeme zur Angriffserkennung

Netzwerksicherheit:

IDS (Intrusion Detection System)

Vorteile

- relativ zuverlässiges Erkennen von Angriffen auf Server, Computer und Netzwerke
- mögliche Identifizierung des Angreifers
- Erstellung einer Datenbasis von Angriffsmustern
- Köderfunktion möglich (Honeypot)

Nachteile

- Das IDS kann als aktive Komponente selbst zum Angriffsziel werden
- IDS dient **nur der Angriffserkennung**, nicht der Abwehr, außer es wird mit Abwehrsoftware gekoppelt -> siehe: Intrusion Prevention System (IPS)
- als rein signaturbasiertes System gegenüber völlig neuen Angriffsmustern nicht wirksam

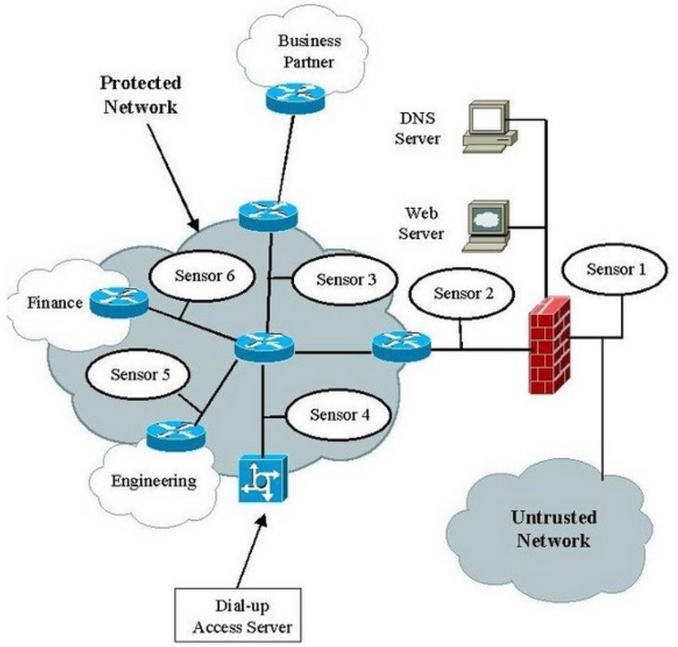
Quelle: http://www.was-ist-malware.de/it-sicherheit/intrusion-detection-system-ids/

Systeme zur Angriffserkennung

Netzwerksicherheit:

IPS (Intrusion Prevention System)

Ein IPS – Intrusion Prevention System – erkennt Angriffe auf Computer-systeme und Netzwerke. Wenn solche Angriffe erfolgen, löst das Intrusion Prevention System automatische Abwehrmaßnahmen aus.



Varianten:

- HIPS (Host-based IPS): Die Ausführung erfolgt auf dem zu schützenden Computer.
- NIPS (Network-based IPS): Das System überwacht den Netzwerkverkehr
- CBIPS (Content-based IPS): Dieses Intrusion Prevention System untersucht ankommende Inhalte auf gefährliche Komponenten.
- PAIPS (Protocol-Analysis IPS): Hiermit werden Übertragungen auf Protokollebene analysiert, um eventuelle Angriffsmuster zu entdecken.

Quelle: http://www.was-ist-malware.de/it-sicherheit/intrusion-prevention-system/

Systeme zur Angriffserkennung

Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR) ist ein Technologiekonzept und eine Lösung zum Schutz und zur Abwehr von Cyberbedrohungen von Endgeräten wie PCs, Laptops, Tablets und Smartphones oder Server.

EDR zeichnet das Verhalten der Endgeräte auf und analysiert diese Daten.

Bei erkanntem verdächtigem Verhalten bietet EDR automatisierte Reaktionen zur Abwehr wie die Isolierung der Endgeräte.

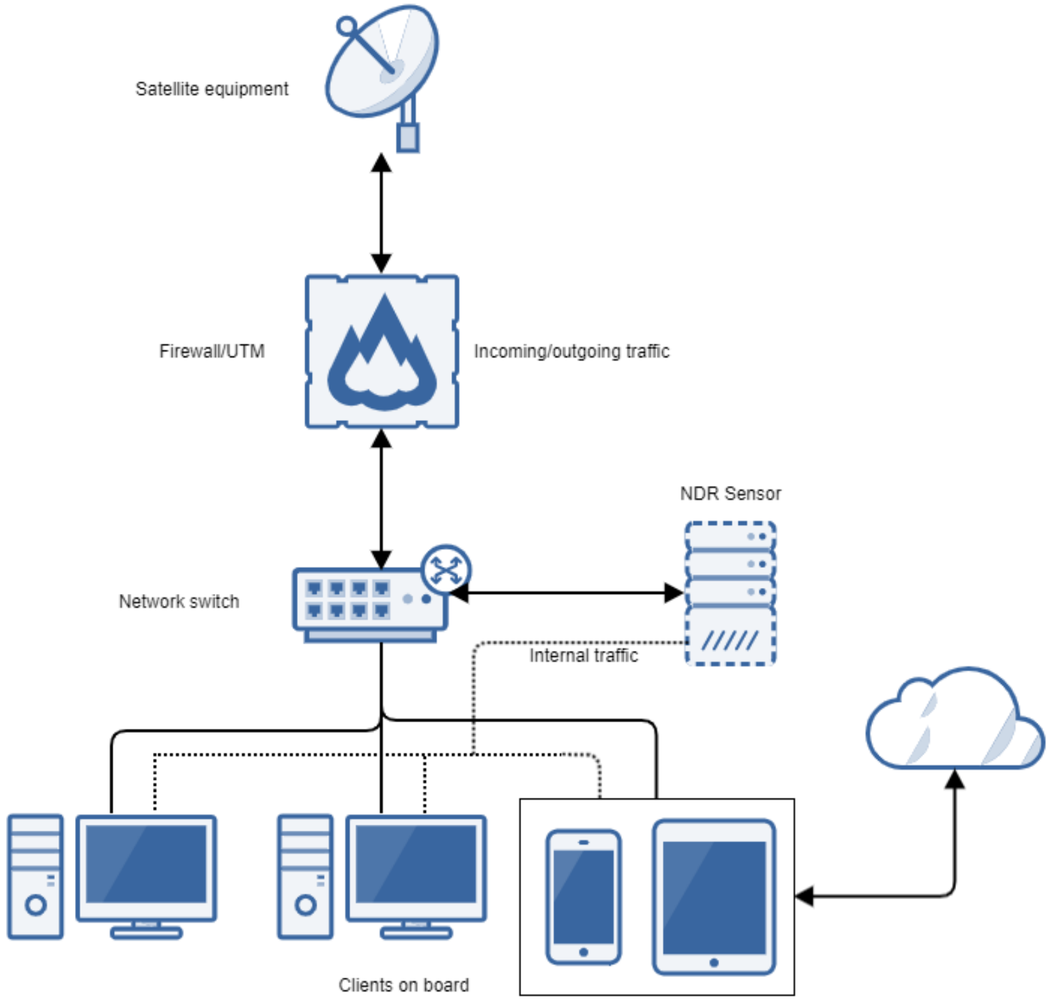


Bild: https://www.port-it.nl/cybersecurity-solutions/ndr/
Quelle: https://www.security-insider.de/was-ist-network-detection-and-response-ndr-a-1094255/

Systeme zur Angriffserkennung

Security Information and Event Management (SIEM)

Die Grundidee eines **SIEM** ist alle für die IT-Sicherheit relevanten Daten an einer zentralen Stelle zu sammeln und durch Analysen Muster und Trends zu erkennen, die auf gefährliche Aktivitäten schließen lassen.

Das Sammeln und die Interpretation der Daten erfolgen in Echtzeit. Sämtliche Informationen sind manipulations- und revisionssicher gespeichert.

SIEM-Lösungen sind zwar sehr gut im Erkennen von Cyber-Angriffen, sie erfordern aber ein manuelles Eingreifen der Sicherheitsexperten zur Abwehr.

- > Security Orchestration Automation and Responses (SOAR)

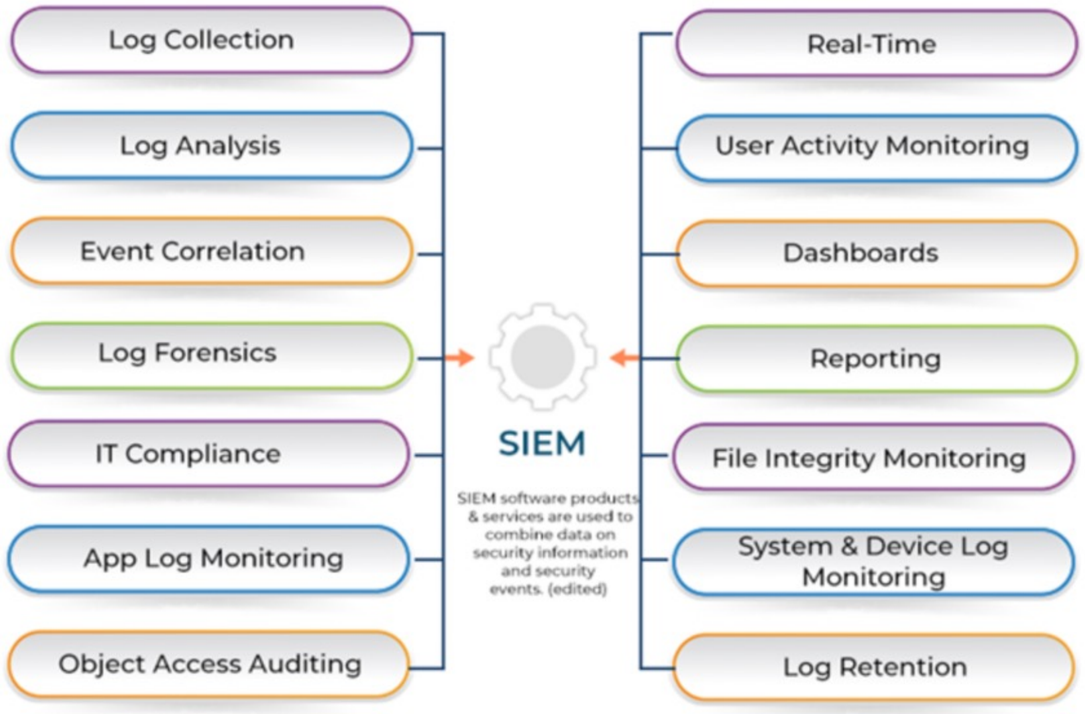


Bild Quelle: https://www.security-insider.de/was-ist-ein-siem-a-772821/

Systeme zur Angriffserkennung

Security Information and Event Management (SIEM)

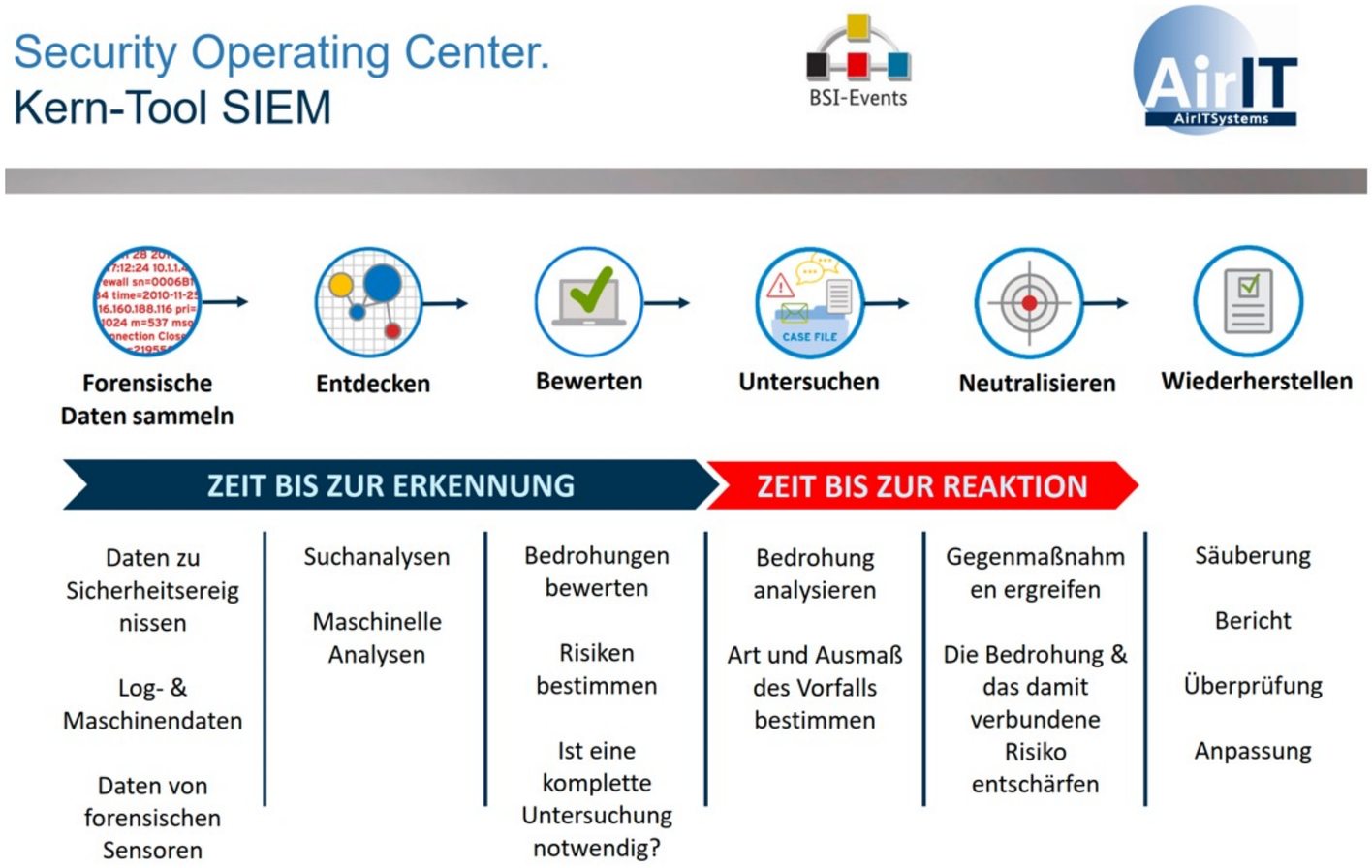


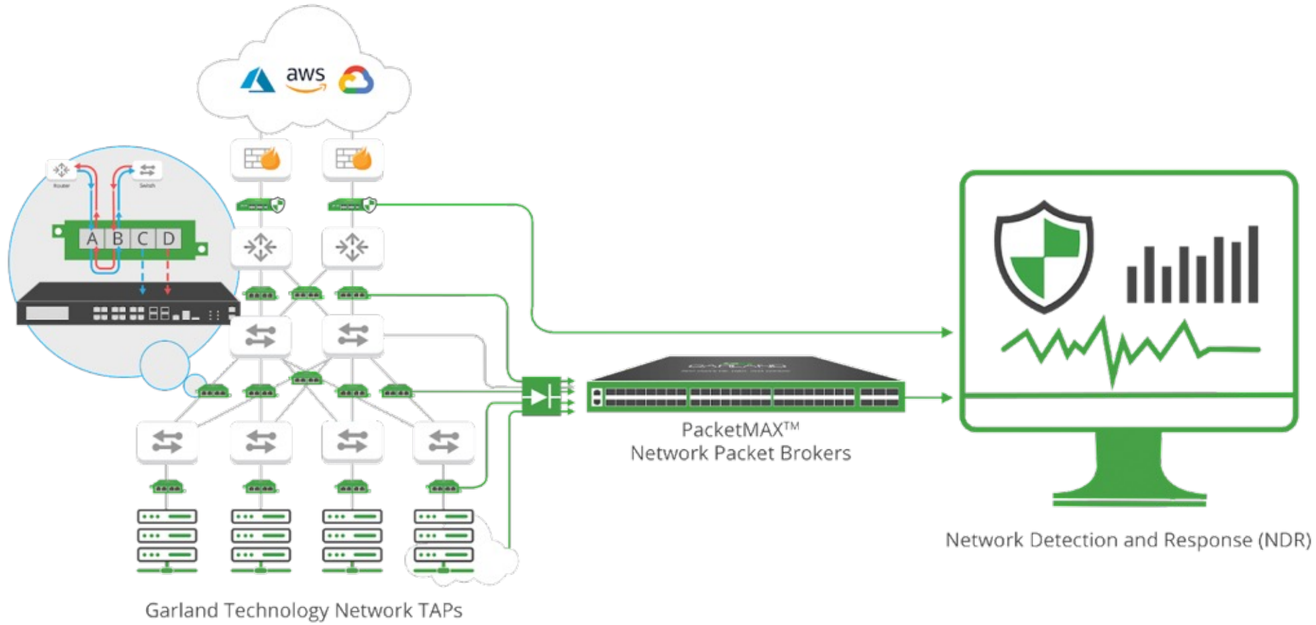
Bild: Tim Cappelmann - Aufbau und Implementierung eines SOC - Vortrag anläßlich des 16. Deutschen IT-Sicherheitskongresses in Bonn vom 21-23. Mai 2019
Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/ITSiKongress/16ter/Vortraege_22-05-2019/TimCappelmann.html

Systeme zur Angriffserkennung

Network Detection and Response (NDR)

Network Detection and Response (NDR) beschreibt Sicherheitslösungen, die den Netzwerkverkehr kontinuierlich überwachen und analysieren, um verdächtigen Datenverkehr zu erkennen und darauf automatisiert zu reagieren.

Zur Analyse des Netzwerkverkehrs und zum Erkennen von Anomalien kommen Verfahren der **Künstlichen Intelligenz (KI)** und des **Maschinellen Lernens (ML)** zum Einsatz.



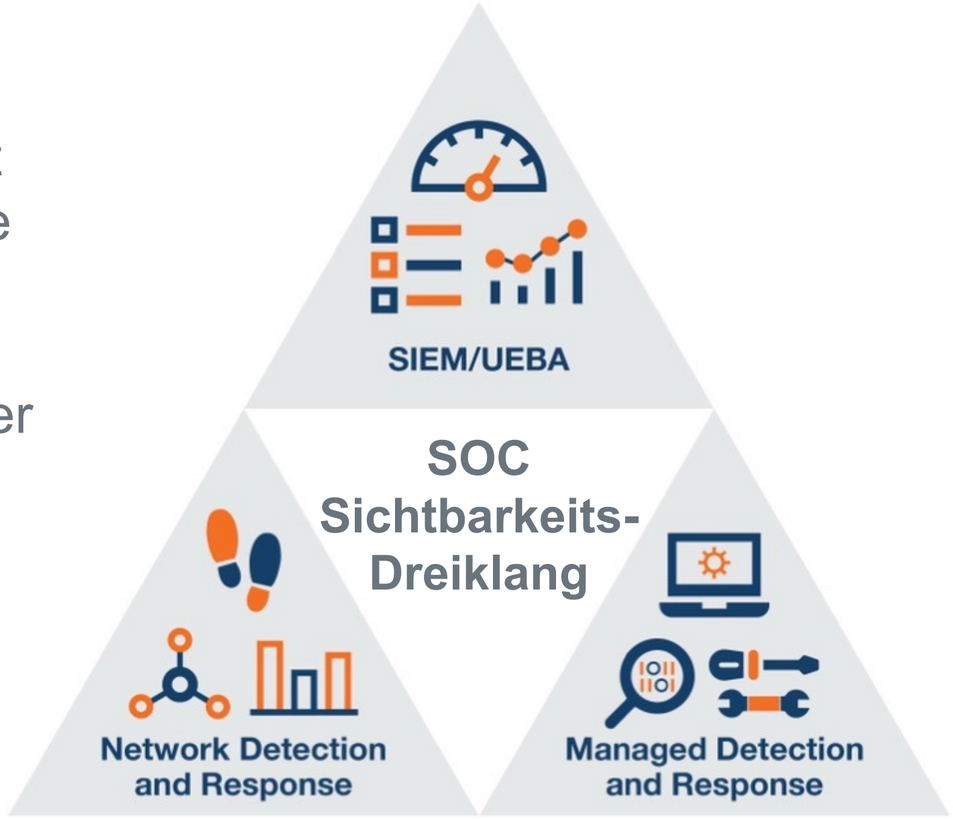
Quelle:
Bild: https://www.garlandtechnology.com/blog/adding-visibility-to-improve-network-detection-and-response-ndr

Systeme zur Angriffserkennung

SOC-Sichtbarkeits Dreiklang (SOC-Triad)

Das so genannte **Security Operations Center (SOC),** versteht sich als Zentrale für alle sicherheitsrelevanten Services im IT-Umfeld von Organisationen oder Unternehmen.

Es schützt die IT-Infrastruktur und Daten vor internen und externen Gefahren.



Die Kombination der drei Säulen (EDR, NDR, SIEM) in einem sog. **SOC-Sichtbarkeits Dreiklang (SOC-Triad),** führt dazu, dass Unternehmen über ein vielschichtiges, effizientes und umfassendes Cyber-sicherheitssystem verfügen, mit dem sie modernen Cyber-Bedrohungen wirksam begegnen können.

Bild: https://blob.hkbn.net/es-aio-static/ir
Quelle: https://www.security-insider.de/was-ist-ein-security-operations-center-soc-a-617980/

Systeme zur Angriffserkennung

Orientierungshilfe des BSI zum Einsatz von Systemen zur Angriffserkennung

Das Dokument soll eine Orientierung für Betreiber Kritischer Infrastrukturen sowie prüfenden Stellen zu SzA und den Anforderungen bei deren Umsetzung bieten.

Wichtig:

Eine Selbstprüfung durch die Betreiber ist aufgrund der zwingend notwendigen Unabhängigkeit und Neutralität einer prüfenden Instanz nicht gültig/möglich.

Siehe auch:

FAQ zum Einsatz von SzA

Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.pdf?__blob=publicationFile&v=16

Systeme zur Angriffserkennung

Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen (MST PD)

Um Cyber-Angriffe auf die Bundesverwaltung erkennen und behandeln zu können, reguliert dieser Mindeststandard die Protokollierung und Detektion von sicherheitsrelevanten Ereignissen in der Kommunikationstechnik des Bundes.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat neuen Version (2.0) des Mindeststandards zur Protokollierung und Detektion von Cyber-Angriffen erstellt veröffentlicht.

Quelle https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/PDCA/PDCA_node.html

Systeme zur Angriffserkennung

Beurteilungsstufen durch den Prüfer

0. Es sind bisher **keine Maßnahmen** zur Erfüllung der Anforderungen umgesetzt und es bestehen auch keine Planungen zur Umsetzung von Maßnahmen.

1. Es bestehen **Planungen** zur Umsetzung von Maßnahmen zur Erfüllung der Anforderungen, jedoch für mindestens einen Bereich noch keine konkreten Umsetzungen.

2. In allen Bereichen wurde mit der **Umsetzung von Maßnahmen** zur Erfüllung der Anforderungen **begonnen.** Es sind noch nicht alle MUSS-Anforderungen erfüllt worden.

3. **Alle MUSS-Anforderungen*** wurden für alle Bereiche **erfüllt.** Idealerweise wurden **SOLLTE-Anforderungen** hinsichtlich ihrer Notwendigkeit und Umsetzbarkeit **geprüft.** Ein kontinuierlicher Verbesserungsprozess wurde etabliert oder ist in Planung.

4. **Alle MUSS- Anforderungen** wurden für alle Bereiche erfüllt. **Alle SOLLTE-Anforderungen*** wurden erfüllt, außer sie wurden stichhaltig und nachvollziehbar begründet ausgeschlossen. Ein **kontinuierlicher Verbesserungsprozess** wurde etabliert.

5. Alle **MUSS-Anforderungen** wurden für alle Bereiche erfüllt.
Alle **SOLLTE-Anforderungen** und **KANN-Anforderungen*** wurden für alle Bereiche **erfüllt,** außer sie wurden stichhaltig und nachvollziehbar begründet ausgeschlossen. Für alle Bereiche wurden sinnvolle zusätzliche Maßnahmen entsprechend der Risikoanalyse / Schutzbedarfsfeststellung identifiziert und umgesetzt. Ein kontinuierlicher Verbesserungsprozess wurde etabliert

*siehe IT-Grundschutzkatalog

Quelle: Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung, V. 1.0 v. 26.09.2022, S. 15
Bildquelle: https://www.fernuni-hagen.de/zli/blog/kennen-sie-schon-das-fuenf-stufen-modell/

Systeme zur Angriffserkennung

Quelle: https://www.security-insider.de/was-ist-ein-security-operations-center-soc-a-617980/

SECaaS.IT
eine Marke der XaaS Enterprise GmbH

WIR SIND BEI RÜCKFRAGEN GERNE FÜR SIE DA!

SECaaS – Security as a Service
XaaS Enterprise GmbH
Sebastian-Kneipp-Straße 41
60439 Frankfurt

Patrick Wolf
+49-69-5060-76777
+49-152-2868-3848
pw@SECaaS.IT

IT-SICHERHEIT MUSS EINFACH SEIN!

MIT SCHNELLEN SCHRITTEN IN EINE SICHERE ZUKUNFT STARTEN