CYBER- UND INFORMATIONSRAUM

Vorstellung des Zentrum für Cyber-Sicherheit der Bundeswehr

Vortragender: DirZITBw Hans-Ulrich Schade, Direktor u. Leiter ZCSBw

BUNDESWEHR

BEDROHUNGEN IM CYBERUMFELD

WELT

Wieder Russen von APT28? Hackerangriff auf deutsches Regierungsnetz

Von **Sabine Sans** mit **dpa** • Zuletzt aktualisiert: 28/02/2018

POL National Cyber Security Center reports intrusion using CVE-2020-0688 attributed to known APT28 C2 infrasctructure

Warsaw, May 2020

welivesecurity BY eset

Norway's parliament struck by hackers

Unknown threat actors were able to exfiltrate information from the email accounts of several parliamentarians

Amer Owaida

2 Sep 2020 - 03:27PM

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

STRONTIUM —

Microsoft catches Russian state hackers using IoT devices to breach networks

Fancy Bear servers are communicating with compromised devices inside corporate networks.

JOSHUA DAVIS 08.21.07 12:00 PM

Hackers Take Down the Most Wired Country in Europe

Suspected Chinese Cyber Espionage Group (TEMP.Periscope) Targeting U.S. Engineering and Maritime Industries

March 16, 2018 | by FireEye

FOCUS Online Samstag, 22.08.2020, 17:54

Hacker-Angriff auf Bundestags-Fahrdienst: Bundeswehr sollte erpresst werden

Hinter dem Hacker-Angriff auf den Fahrdienst von Bundeswehr und Bundestag steckte nach neuen Erkenntnissen ein Erpressungsversuch.

THREAT LIFE CYCLE: DETECT – ANALYSE – DECIDE – DEFEND

welivesecurity BY eset

Norway's parliament struck by hackers

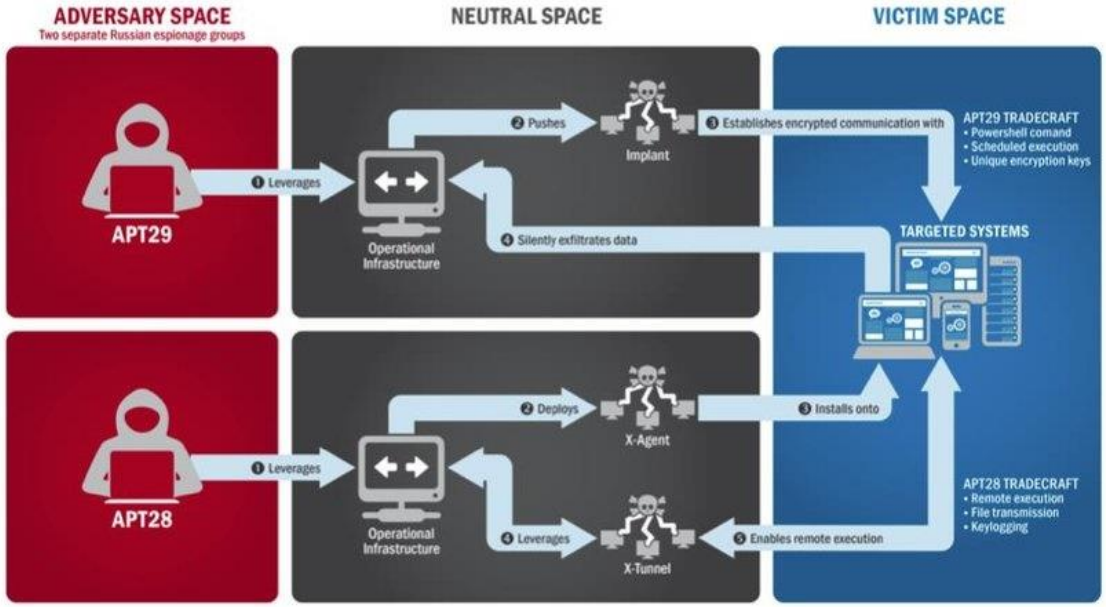
Unknown threat actors were able to exfiltrate information from the email accounts of several parliamentarians

Amer Owaida

2 Sep 2020 - 03:27PM

[WELIVESECURITY.NET]

Threat Intelligence



[RESEARCHGATE.NET]

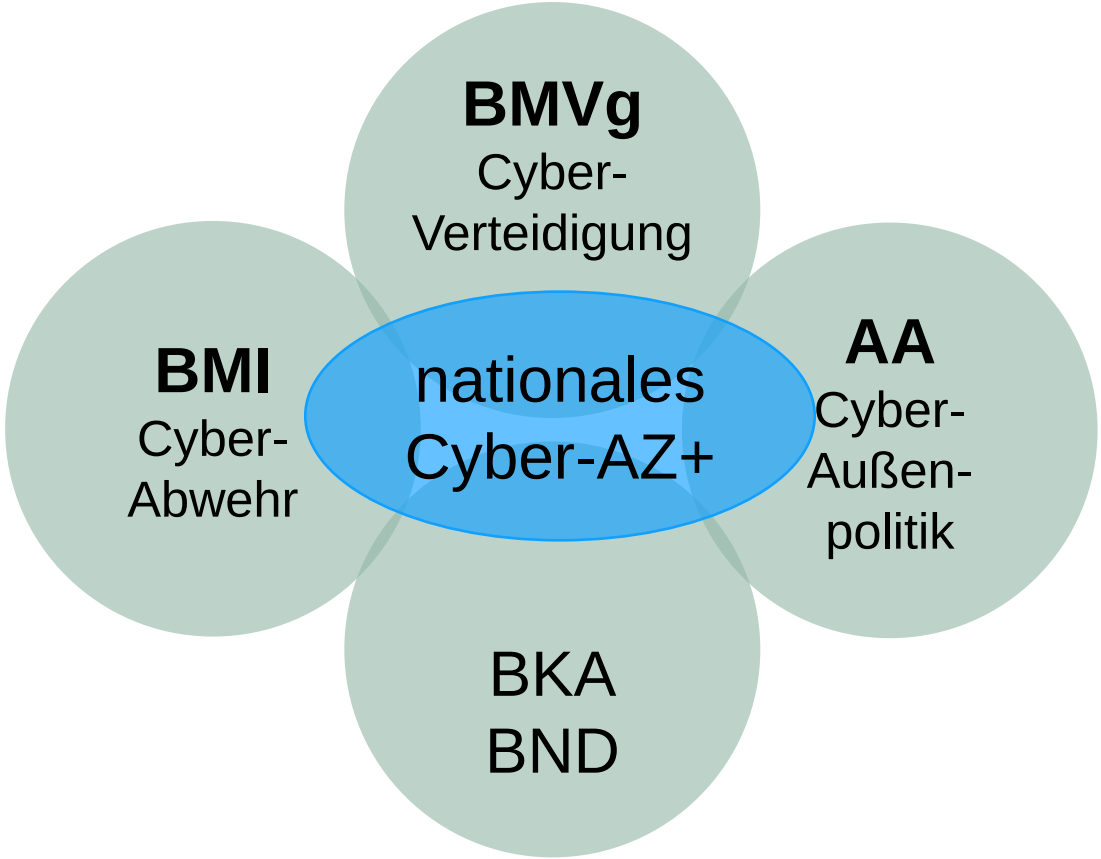
Indicators of Compromise (IoCs)

Tactics, Techniques, and Procedures (TTPs)

Sensorik / Penetrationstests / IT Forensik

Incident Response / (Re-)Active Cyber Operations

NATIONALE CYBER-SICHERHEITSARCHITEKTUR



SICHERHEIT IM CYBER- UND INFORMATIONSRAUM
ANTEIL CYBER-VERTEIDIGUNG

Strategie und Konzeption

- Weißbuch 2016
- Cyber-Sicherheitsstrategie 2016
- Strategische Leitlinie Cyber-Verteidigung 2015

Bundeswehr-Fähigkeiten

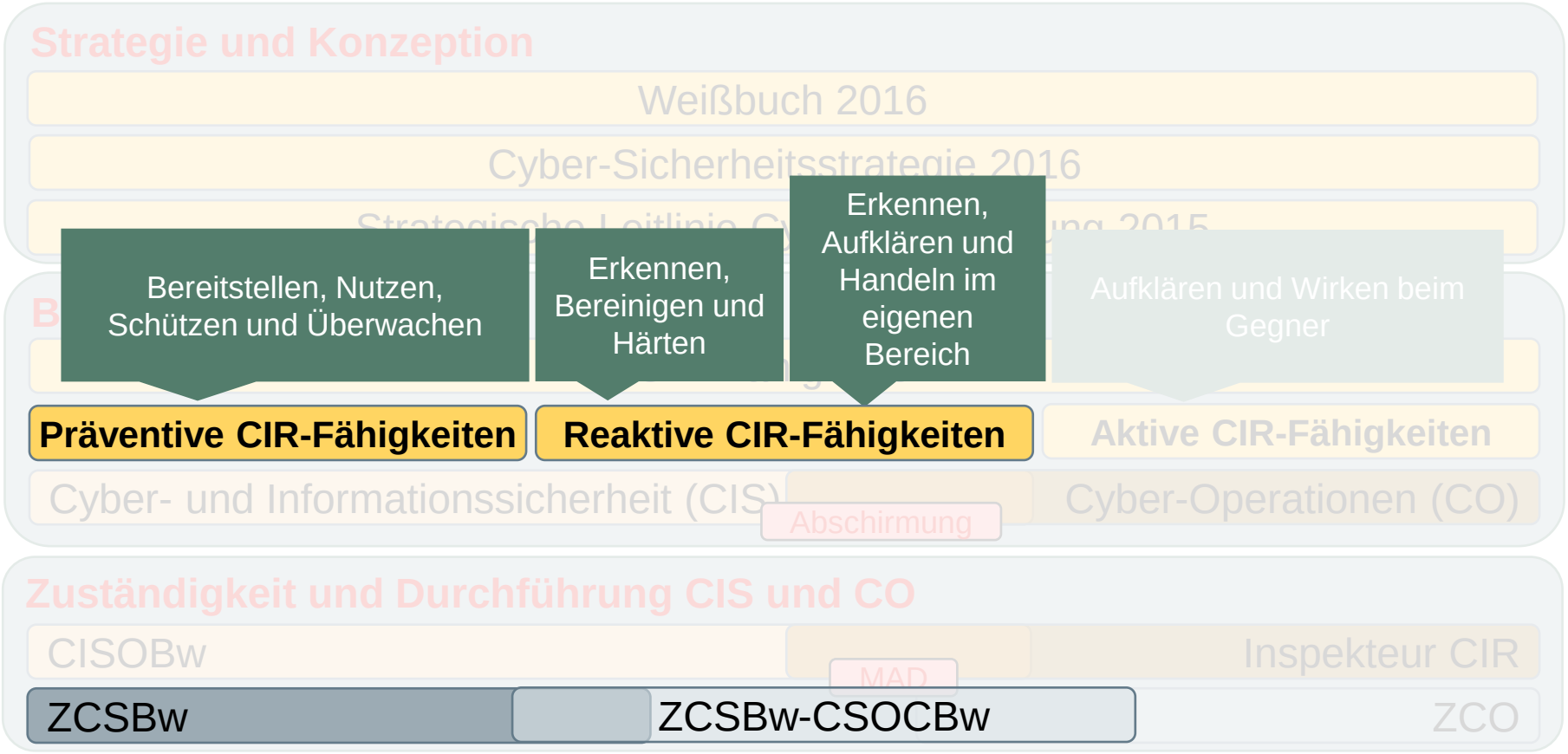
CIR-Fähigkeiten

Präventive CIR-Fähigkeiten	**Reaktive CIR-Fähigkeiten**	**Aktive CIR-Fähigkeiten**
Cyber- und Informationssicherheit (CIS)	Abschirmung	Cyber-Operationen (CO)

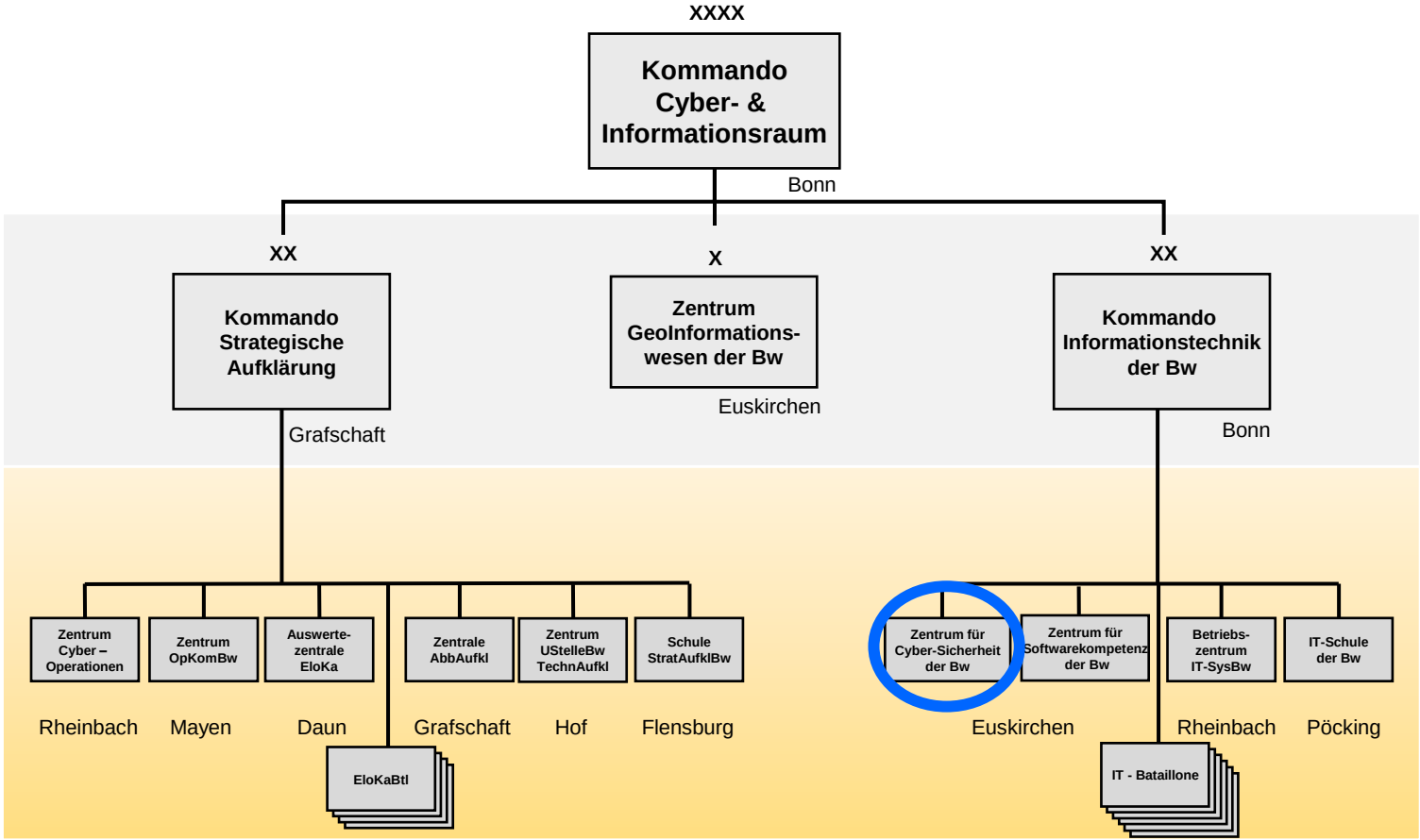
Zuständigkeit und Durchführung CIS und CO

CISOBw	MAD	Inspekteur CIR
ZCSBw	ZCSBw-CSOCBw	ZCO

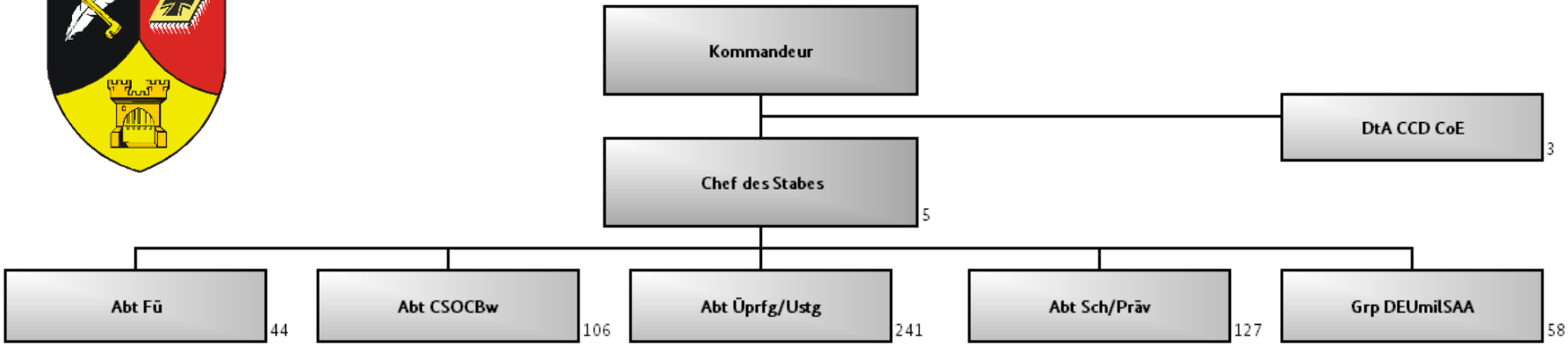
SICHERHEIT IM CYBER- UND INFORMATIONSRAUM
ANTEIL CYBER-VERTEIDIGUNG



ORGANISATIONSBEREICH CYBER- UND INFORMATIONSRAUM



ZENTRUM FÜR CYBER-SICHERHEIT DER BUNDESWEHR



Auftrag

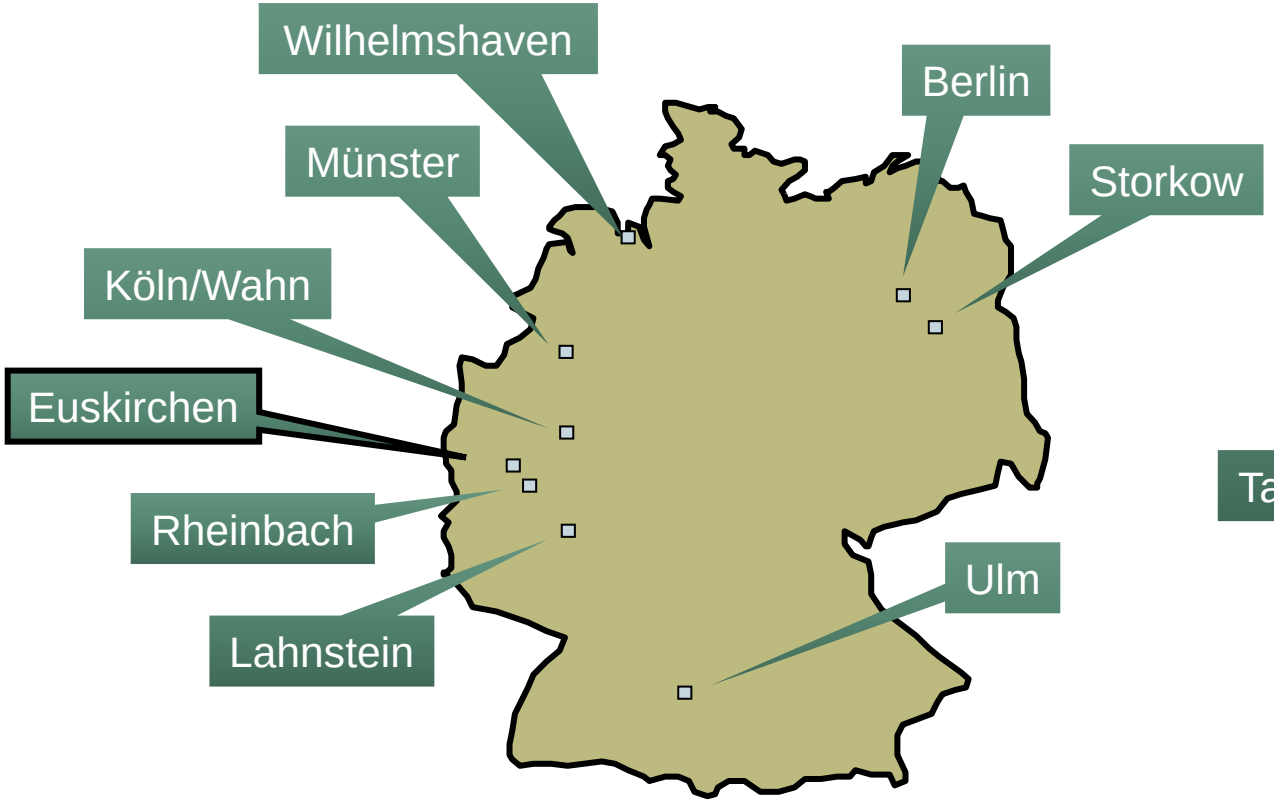
Das Zentrum für Cyber-Sicherheit der Bundeswehr ist die

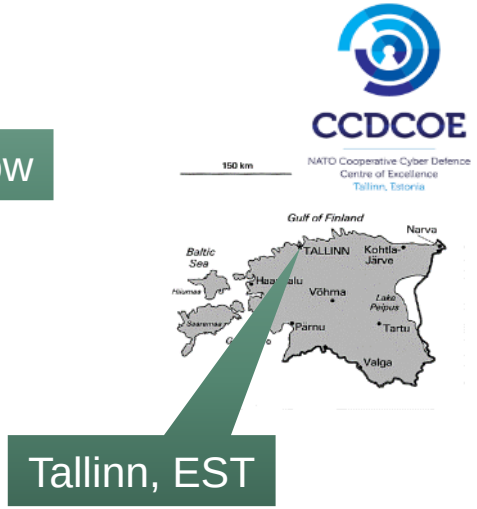
zentrale Dienststelle zur Gewährleistung eines umfassenden Schutzes der Interessen, IT-Services und IT-Systeme der Bundeswehr im Cyber- und Informationsraums

unter Umsetzung der Schutzziele der Informationssicherheit als Teil der Cyber-Verteidigung

585 Dienstposten

DISLOZIERUNG ZCSBW





ABTEILUNG
CYBER SECURITY OPERATIONS CENTRE BUNDESWEHR

ABTEILUNG CSOCBW
GLIEDERUNG UND AUFGABEN

- Abteilung CSOCBw
  - Dez Technisches Lagebild
  - Dez Lage- und Überwachungszentrum
  - Dez CERTBw
  - Dez Cyber-Bedrohung und Risikoanalyse
  - Dez Betrieb ZCSBw Systeme

Hauptaufgaben

- Betrieb & Ausbau von **Schutz- und Überwachungssystemen**
- Bereitstellung eines technischen Lagebildes der Cyber-Sicherheit (Dashboard z.B f. ISB EinsKtgt)
- 24/7 **Netzwerküberwachung**
- Führen eines zentralen **Cyber-Sicherheitslagebildes**
- **Incident Response**
- **IT-forensische Untersuchungen**
- **Cyber-Bedrohungs- & Trendanalyse**
- Erstellung Handlungsempfehlungen (**Advisories**)

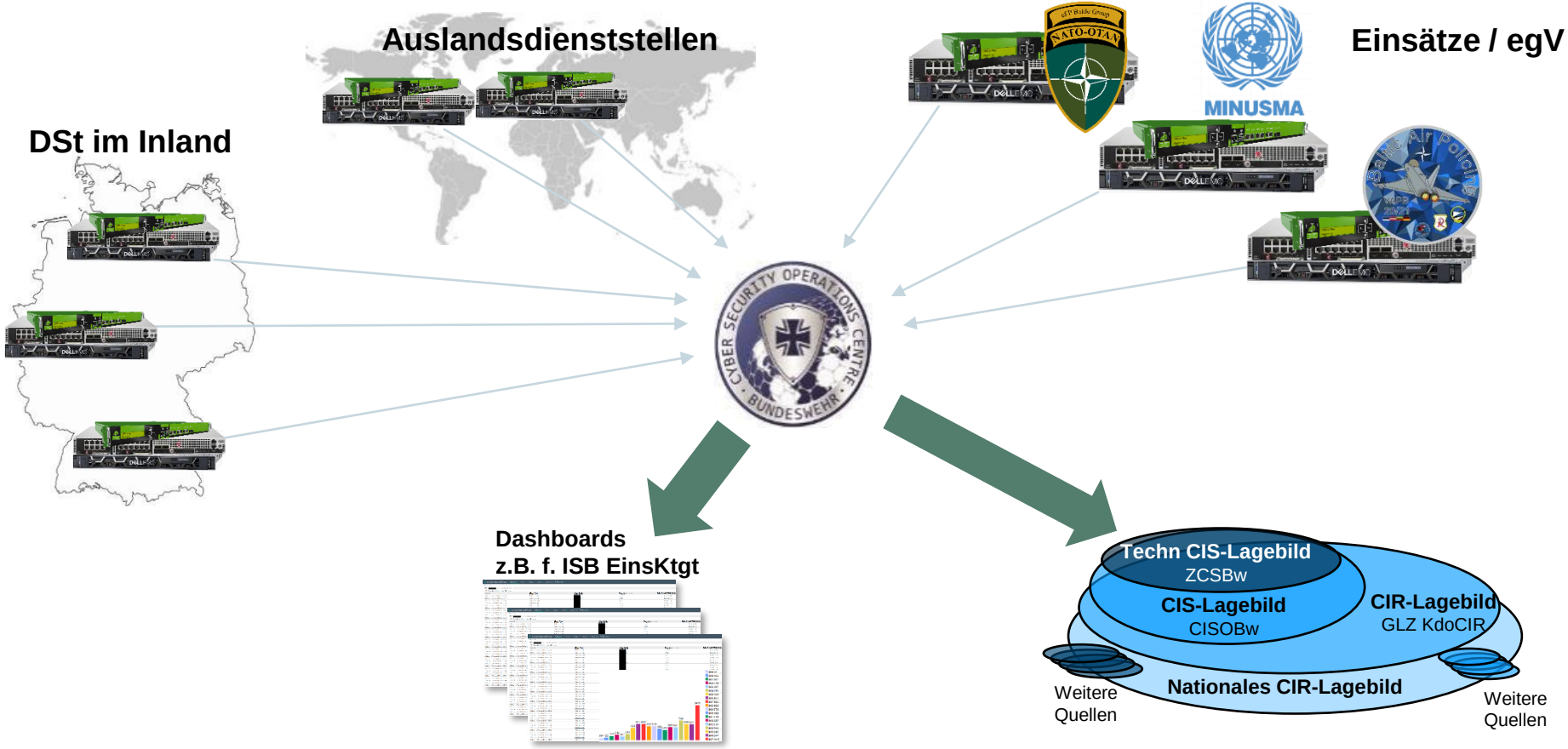
ABTEILUNG CSOCBW
ÜBERWACHUNG UND SCHUTZ IM IT-SYSBW

Intrusion Prevention Systeme (IPS):
Erkennen, Alarmieren und Abwehren von Bedrohungen im Netzwerkverkehr

Schwachstellenscanner:
Erkennen und Melden von veralteten Softwareversionen & Fehlkonfigurationen

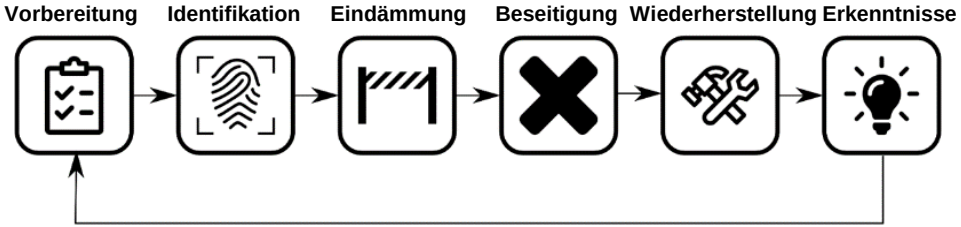
Security Information and Event Management (SIEM):
Sammeln, Aufbereiten und Darstellen von sicherheitsrelevanten Protokolldaten und Systemmeldungen

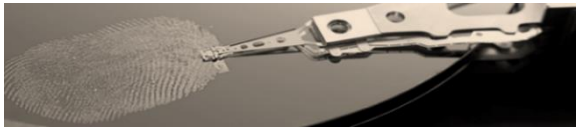
ABTEILUNG CSOCBW
ÜBERWACHUNG UND SCHUTZ IM IT-SYSBW



Incident Response für Dienststellen im Inland, Ausland und in Einsätzen der Bundeswehr

- Mobile Beweissicherungsfähigkeiten von digitalen Daten und IT-Systemen
- Erstbewertungsfähigkeit mobil
- Umfängliche Untersuchungsfähigkeiten stationär und aus der Distanz u.a.
  - Malwareanalyse
  - Netzwerkforensik
  - Mobilgeräteforensik
- **Rufbereitschaft + weltweite Verlegefähigkeit**





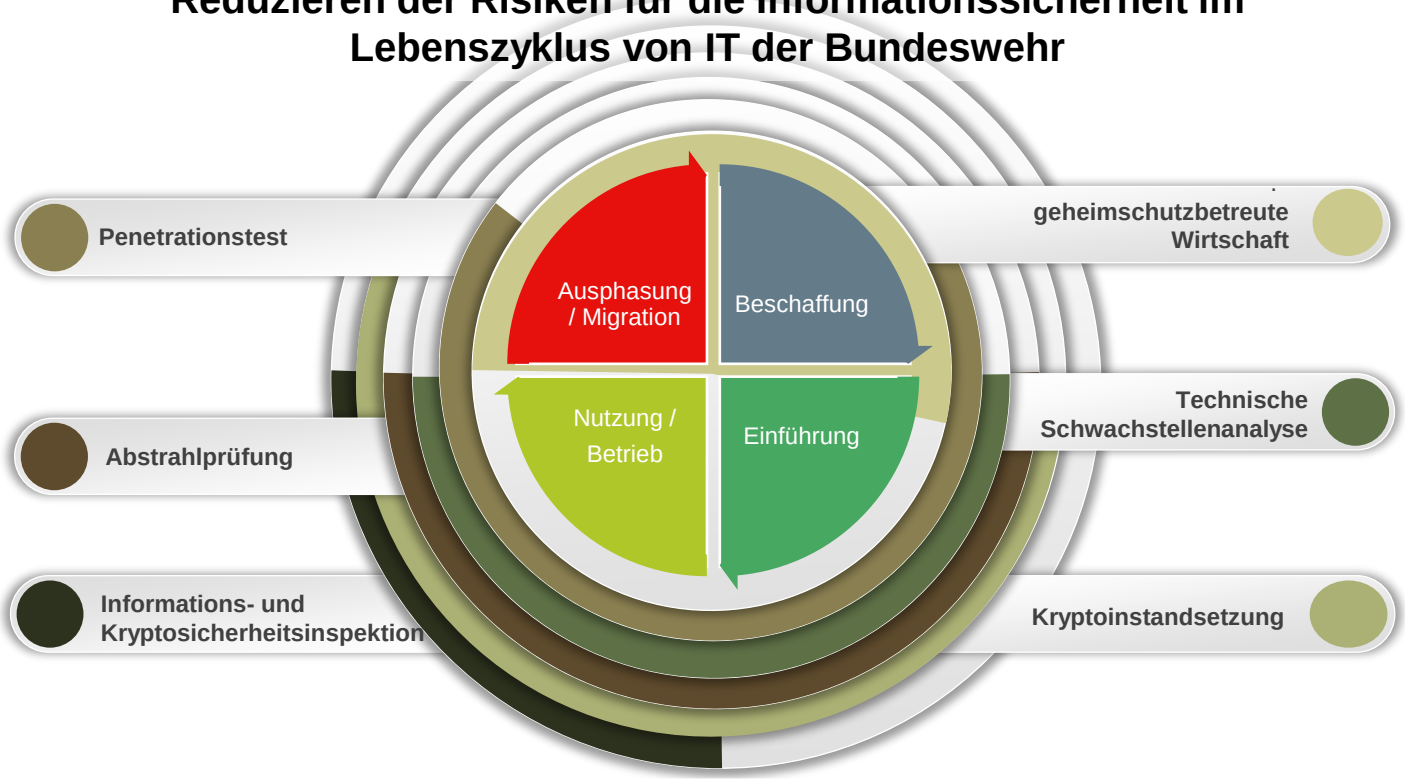
ABTEILUNG CSOCBW
CYBER THREAT INTELLIGENCE & CSOCBW ADVISORY

- Verfolgen diverser Quellen (z.B. News, Blogs, Foren, MISPBw) bzgl. Indikatoren
- Auswertung der gewonnenen Informationen
  - ➢ APT-Kampagnen → Tactics, Techniques and Precedures (TTP)
  - ➢ Schwachstellen → Hotfixes, Patches
- Bewertung auf Relevanz für die Bundeswehr
- Multinationale und ressortübergreifende Zusammenarbeit
- CSOCBw Advisories als Handlungsempfehlung für IT-Admins

ABTEILUNG
ÜBERPRÜFUNG UND UNTERSTÜTZUNG

ABTEILUNG ÜPRFG/USTG
GLIEDERUNG UND AUFGABEN

Reduzieren der Risiken für die Informationssicherheit im Lebenszyklus von IT der Bundeswehr



- nah am Bedarfsträger durch Dislozierung in der Fläche -

ABTEILUNG ÜPRFG/USTG
INSPEKTIONEN

Informationssicherheitsinspektion

- Regelmäßige Inspektionen von Dienststellen im Inland, im Ausland und Einsätzen
- Fokus: Umsetzung Informationssicherheits-management (ISM) Prozesse
- Bw-einheitliche Prüfliste, erlassen vom CISOBw
- Ergebnisbericht mit Empfehlungen zur Mängelbeseitigung
- Beitrag zum Lagebild CISOBw und Verbesserung der InfoSichh in den Dienststellen

Kryptosicherheitsinspektionen

- Jährliche Inspektionen von Dienststellen im Inland, im Ausland und Einsätzen
- Fokus: Personal, Vollzähligkeit, Nachweisführung, Absicherung
- Bw-einheitliche Prüfliste, erlassen vom CISOBw
- Ergebnisbericht mit Empfehlungen zur Mängelbeseitigung

Geheimschutzbetreute Wirtschaft

Kryptosicherheitsinspektionen im Auftrag des

Bundesministerium
für Wirtschaft
und Energie

ABTEILUNG ÜPRFG/USTG
TECHNISCHE PRÜFUNGEN

Schwachstellenanalyse

- Identifizieren von bekannten Schwachstellen
- u.a. Betriebssysteme, Applikationen, aktive Netzwerkkomponenten, Sicherheitsprodukte
- manuell und werkzeuggestützt
- IT in Dienststellen, Projekten, Einsätzen und Übungen
- Schwerpunkte: Unterstützung der Akkreditierung von IT-Systemen, Vervollständigung der Aussagekraft von Informationssicherheitsinspektionen
- Ergebnisbericht mit Empfehlungen zur Mängelbeseitigung

Penetrationstest

- aufbauend auf Schwachstellenanalyse
- tiefgehende technische Systembetrachtung von IT und operationeller Technologie
- Fokus: Ausnutzbarkeit von identifizierten Schwachstellen
- Ergebnisbericht mit Risikobewertung

Abstrahlprüfung

- Prüfung des Abstrahlverhaltens von IT-Gerät und taktisch-mobilen Systemen
- Prüfung der Abschirmung/Dämpfung von Infrastruktur
- verlegefähige und stationäre Ausstattung und Labore

ABTEILUNG ÜPRFG/USTG
UNTERSTÜTZENDE AUFGABEN

Kryptozentrum Nord

- Instandsetzung von Kryptogeräten
- Verteilung von Krytomitteln
- Fokus: sehgehende Einheiten der Marine

SINA Registration Authority Marine

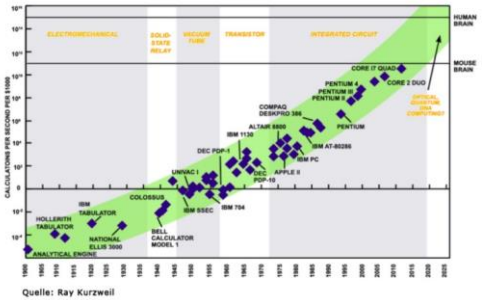
- Betrieb der SINA RA der Marine

Akkreditierung und Beratung

- Fokus: Projekte
- Unterstützung der DEUmilSAA

Standardisierung

- kontinuierliches Fortschreiben der Prüfverfahren der Abteilung
- zeitgemäße innovative Ausbildungsverfahren mit industrieller Unterstützung für das eigene Personal
- eigenverantwortliche Verbesserung und Ergänzung der materiellen Ausstattung



Quelle: Ray Kurzweil

Abb.: Darstellung des technologischen Fortschritts

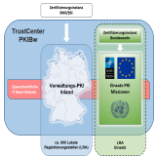
ABTEILUNG
SCHUTZ UND PRÄVENTION

ABTEILUNG SCH/PRÄV
GLIEDERUNG UND AUFGABEN

Informationssicherheit der Bundeswehr – Schützende und präventive Maßnahmen

Kryptomittelproduktion, -versorgung und -nachweisführung

Digitale zertifikatsbasierte Verschlüsselung und Authentifizierung



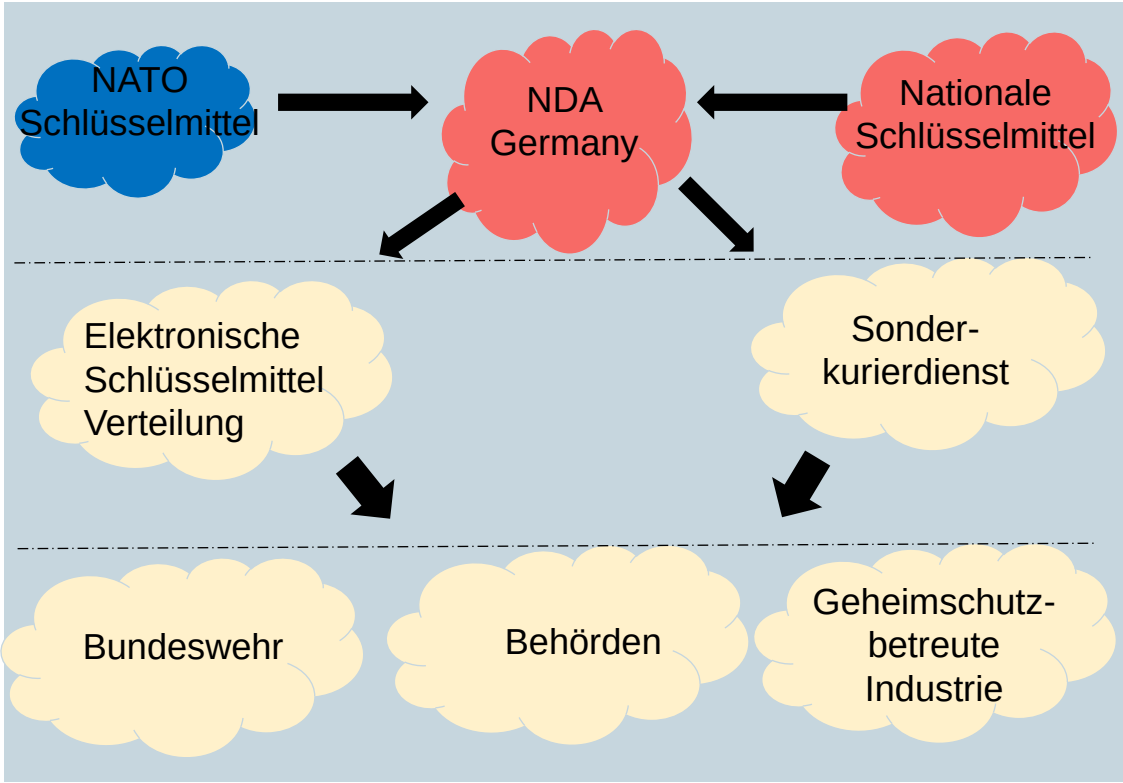
Cyber-Verteidigungsübungen und Sensibilisierungs-maßnahmen für Nutzer

Architekturen und -vorgaben für HW-/SW-Produkte sowie für Waffen- und Sondersysteme

Bereitstellung von Kryptomitteln

Aufgaben

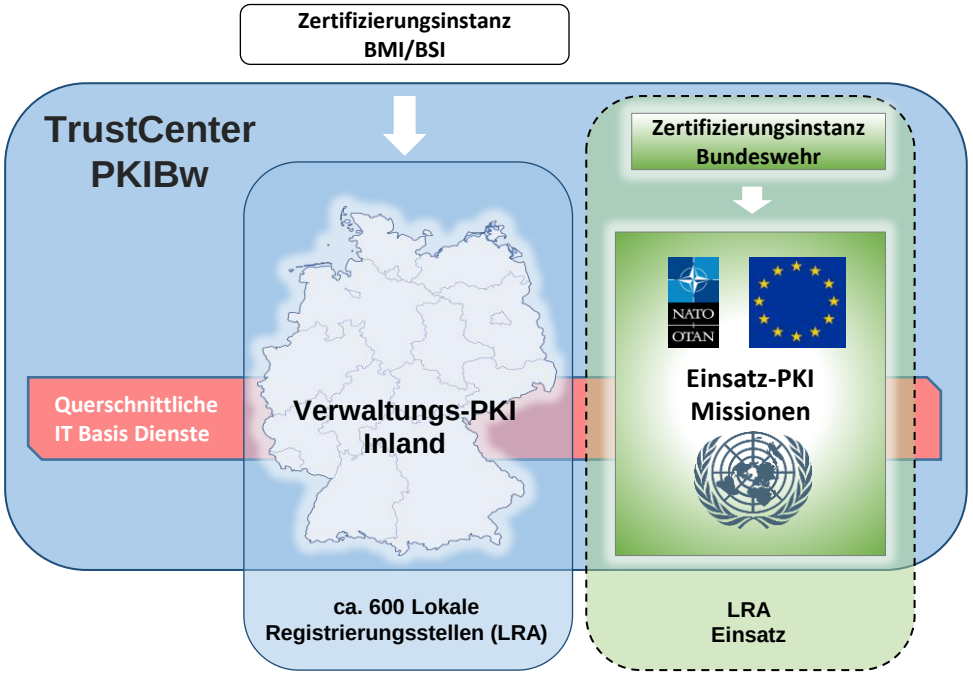
- Betreibt für die Bw Systeme zur nationalen elektronischen Schlüsselmittelerzeugung und -verteilung
- Produziert nationale Kryptounterlagen
- Betreibt NATO Schlüssel-Management-System für die Bw
- Vervielfältigt NATO-Kryptounterlagen
- Sonderkurierdienst liefert Kryptomittel für Bw, Behörden und geheimschutzbetreute Industrie
- Bearbeitet Kryptoverstöße in der Bw im Auftrag des CISOBw
- Berät Bundeswehrprojekte (z.B. A400M, F125, Eurofighter) zum Kryptomanagement



Bereitstellen einer PKI-Infrastruktur

Aufgaben

- Trust Center (TC) PKIBw erzeugt, verteilt und validiert als einzige Stelle im Geschäftsbereich BMVg elektronische Schlüssel und Zertifikate
- Realisiert für die Bw gesicherte digitale Netz- und Kommunikationsverbindungen sowie die digitale Identität von Personen
- Verwaltungs-PKI im Inland und zukünftig Einsatz-PKI für Auslandseinsätze als IT-Service über HaFIS/FMN
- Ca. 600 Servicestellen (LRA) in der Bw zwischen dem TC PKIBw und den Nutzern für eDTAs (ca. 293000) und PKI-Karten (ca. 26000)



ABTEILUNG SCH/PRÄV
ÜBUNGEN UND SENSIBILISIERUNG

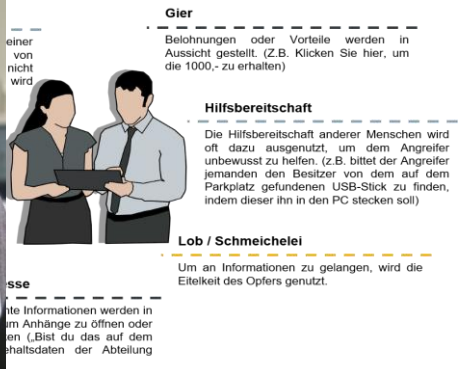
Gefahren für die Informationssicherheit erkennen und abwehren

Im Team

LOCKED SHIELDS

Vorbereitung und Begleitung von Cyber-Verteidigungsübungen der Bw

Für jeden Nutzer

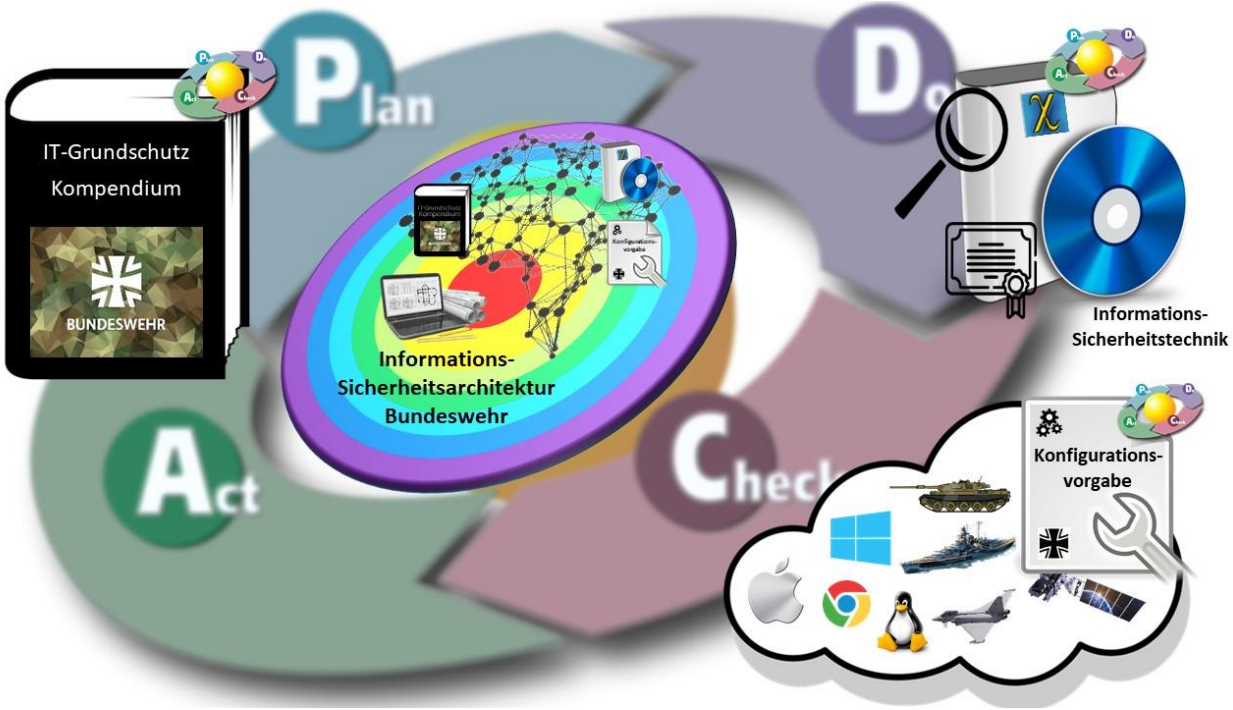


Awareness-Maßnahmen und Kampagnen zur Unterstützung von Dienststellen

Architekturen führen die verschiedenen Elemente des Informationssicherheitsmanagements zusammen

Aufgaben

- Anwenden des Prozessmodells PDCA* zum Umsetzen und Überwachen von Vorgaben und Maßnahmen
- Informationssicherheitsarchitektur Bw pflegen und weiterentwickeln
- IT-Grundschutzkompendium Bw konkretisiert Vorgaben und Maßnahmen des BSI für die Bw
- Informationssicherheitstechnik bewertet Interoperabilität und sicheren Betrieb von IT-Produkten
- Erstellen von Konfigurationsvorgaben zum Härten von Produkten und Waffensystemen mit IT-Anteilen



PDCA*: Plan, Do, Check, Act

GRUPPE

DEUTSCHE MILITÄRISCHE SECURITY ACCREDITATION AUTHORITY

GRUPPE DEUMILSAA
VERANKERUNG AKKREDITIERUNG IN DER BW

Auszug aus der IT-Strategie des BMVg

Zur Gewährleistung der Anforderungen des Geheimschutzes erfolgt vor der erstmaligen Freigabe eines IT-Systems eine Akkreditierung durch die für die Bundeswehr zuständige Akkreditierungsbehörde (DEUmilSAA).

ZDv A-960/1

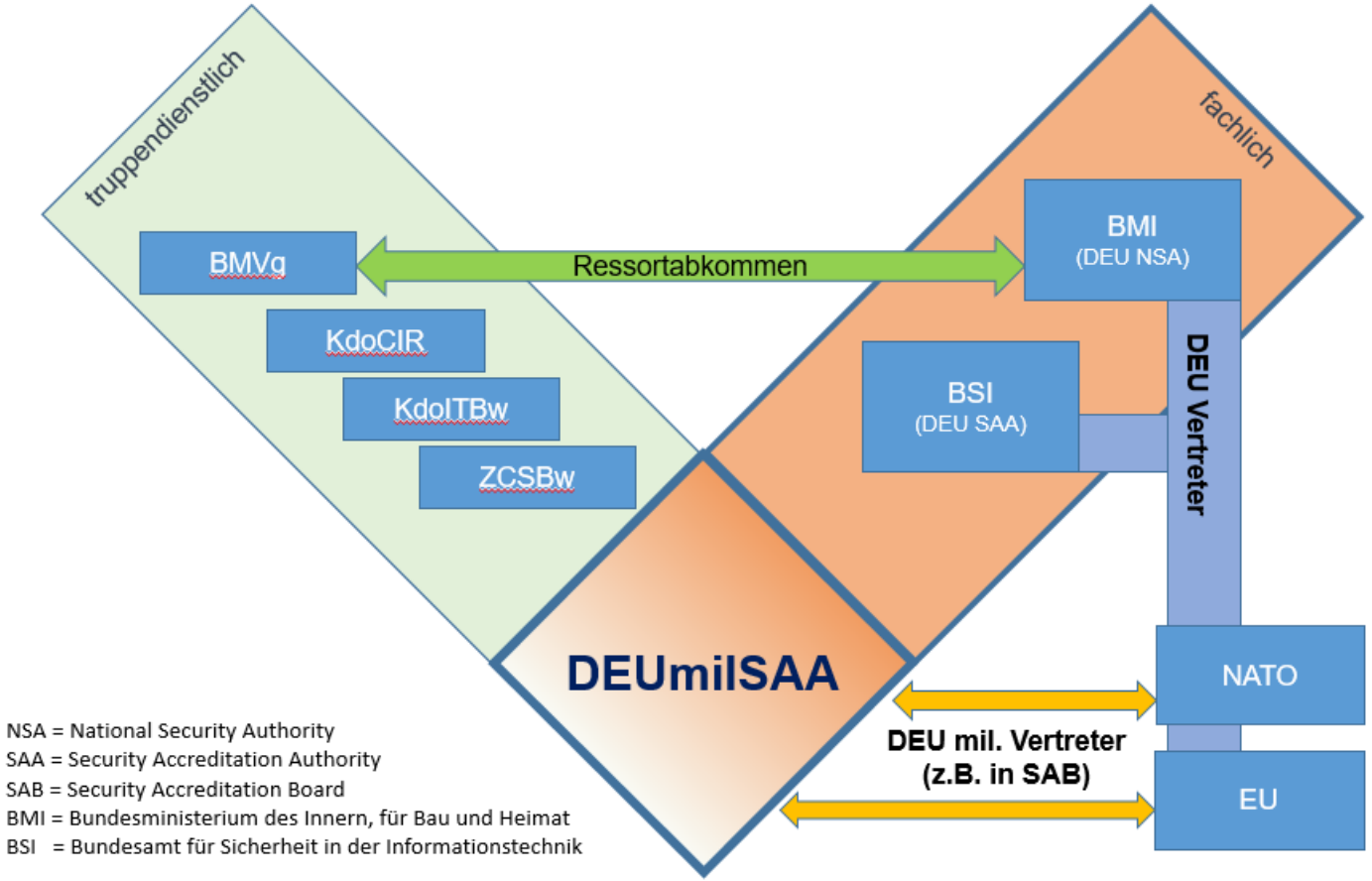
5.5 Akkreditierung

5.5.1 Allgemeines

519. Unter Akkreditierung wird ein Prüfungs- und Genehmigungsverfahren von IT unter Leitung der zuständigen Akkreditierungsstelle verstanden.

520. Eine Akkreditierung im GB BMVg ist grundsätzlich für sämtliche IT durchzuführen, mindestens

GRUPPE DEUMILSAA
UNTERSTELLUNGSVERHÄLTNISSE



NSA = National Security Authority
SAA = Security Accreditation Authority
SAB = Security Accreditation Board
BMI = Bundesministerium des Innern, für Bau und Heimat
BSI = Bundesamt für Sicherheit in der Informationstechnik

GRUPPE DEUMILSAA
AUFTRAG

Akkreditierung von IT-Systemen im Auftrag des BSI

Beratung Informationssicherheit
Prüfung InfoSichhDokumentation

SPOC Zulassung / Verfahren zur Szenariobasierten Freigabe (VSF)

Harmonisierung, Abschluss sowie Umsetzung von Vereinbarungen

Security Accreditation Boards

FRAGEN ?


DEUTSCHLANDS
FREIHEIT
WIRD AUCH IM
CYBERRAUM
VERTEIDIGT.
MACH, WAS WIRKLICH ZÄHLT.
PROJEKT
DIGITALE
KRÄFTE
Bundeswehr
bundeswehrkarriere.de