secunet

Technische Maßnahmen gegen Spionage

vom Quick Win bis zur High-End-Sicherheit

Tobias Schmidt, 24.09.2025

secunet auf einen Blick

Daten & Fakten

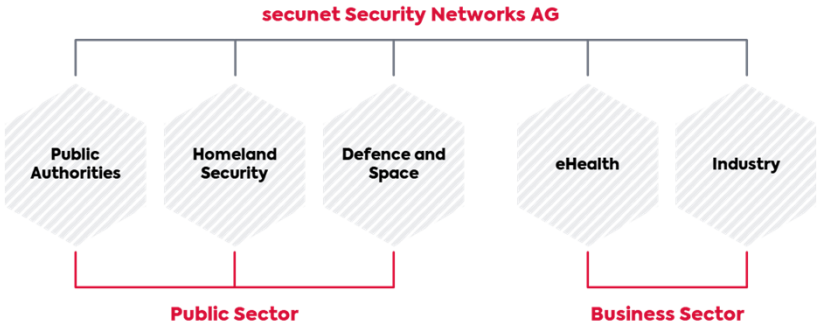
- Gegründet 1997
- 407m Euro Umsatz (24)
- 42m Euro EBIT (24)
- 13 Standorte in Deutschland
- ~1.200 Mitarbeiter
- 75% Hauptanteilseigner:
- IT Sicherheitspartner

Kunden

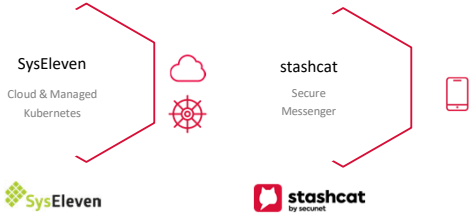
Bundeswehr, NATO OTAN, Lufthansa, Bechtle, Berliner Wasserbetriebe, ELSTER, Bundesamt für Sicherheit in der Informationstechnik, BMW, SIEMENS, CLAAS, DLR, WESTNETZ

... und viele mehr

Firmenstruktur



Tochtergesellschaften



Beispiele aus dem Kerngeschäft

- > 250.000 Installationen hochsicherer IT-Infrastruktur
- 25 Jahre PKI Erfahrung
- > 480 installierte easygates in ganz Europa
- > 84.000 Telematikinfrastruktur-Konnektoren installiert
- secunet edge: IIoT-Gateway zur Anbindung von Maschinen an Cloud-Plattformen für Industrie 4.0
- > 1,3 Millionen aktive stashcat Benutzer (Business-Messenger)
- Cybersicherheitsberatung für DAX-Konzerne & Behörden
- Entwicklung eines hochsicheren Cloud-Ökosystems

Unsere Produkte

... und viele mehr

01

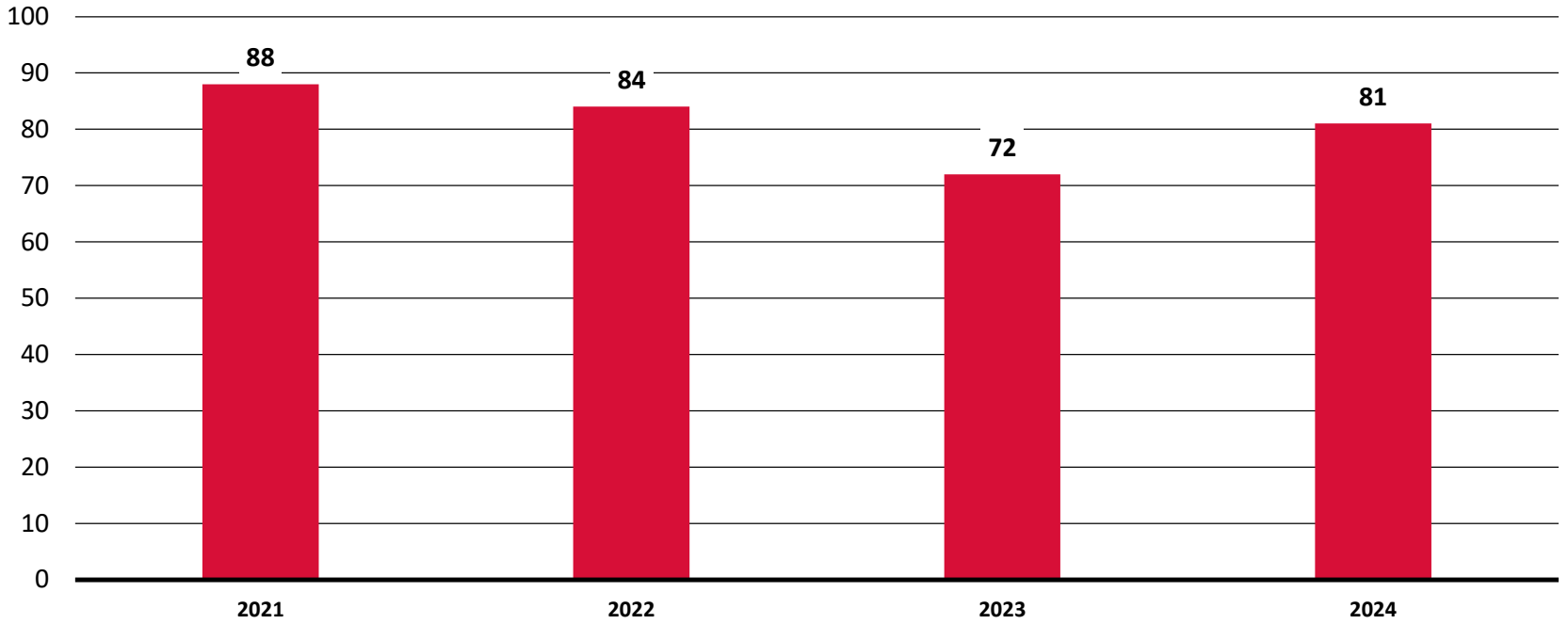
Einleitung

Gefährdungslage und Bedrohungen

> "Die Gefährdungslage ist so hoch wie nie!"
>
> Claudia Plattner, Präsidentin des BSI (2024)

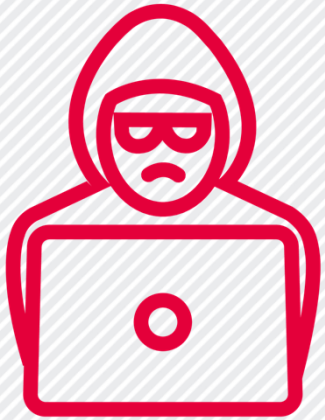
Gefährdungslage

War Ihr Unternehmen innerhalb der letzten 12 Monate von Diebstahl, Industriespionage oder Sabotage betroffen?



Anmerkung: eigene Darstellung nach Bitkom Wirtschaftsschutz 2024

Typische Bedrohungen

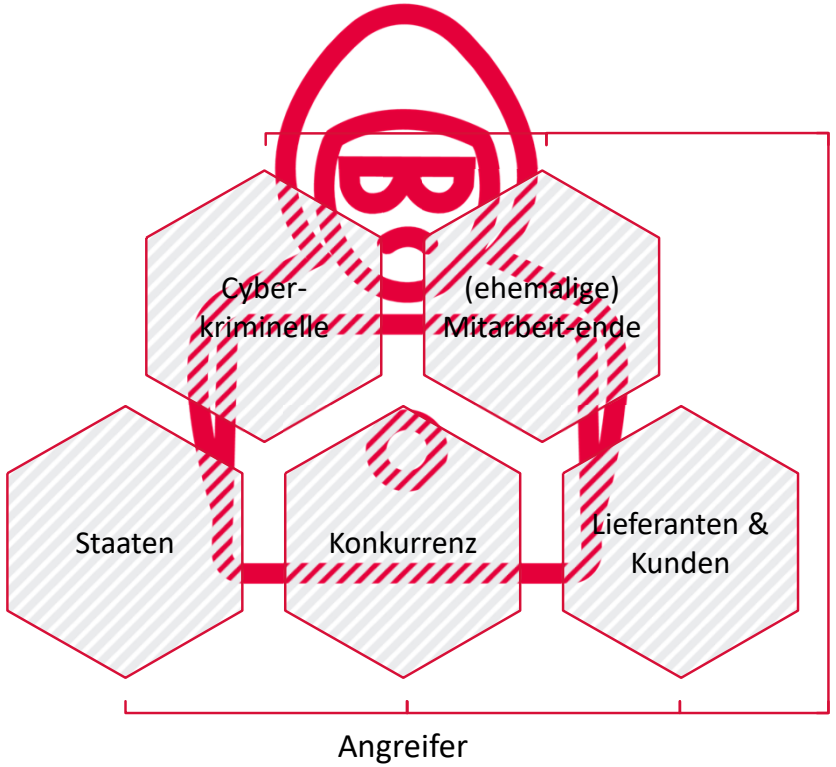


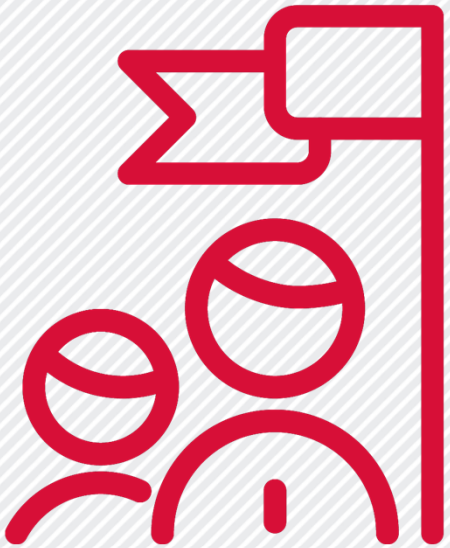
Cyberspionage

(Digitale) Sabotage von Systemen und Anlagen

Lieferkettenangriff

Bedeutung & Angreifer





Management trägt
Verantwortung für
Informationssicherheit

Aktuelle Entwicklungen zu Cyber Security Gesetzgebung und Regulierung

EU-Richtlinie über die Sicherheit von Netz- und Informations-systemen (EU-NIS-2-Richtlinie)

Ziel: Hoher gemeinsamer Level an Cybersecurity in der EU

- Neue Behörden und Befugnisse
- Neuordnung und Erweiterung der betroffenen Sektoren

» In Kraft seit **16.01.2023**

EU-Gesetz zur Cyber-Resilienz (EU CRA)

Ziel: Sicherheit für Anwender & Lieferkette durch Sicherheits-prozesse und -elemente

- Pflichten für Hersteller, Importeure und Distributoren von Produkten mit digitalen Elementen

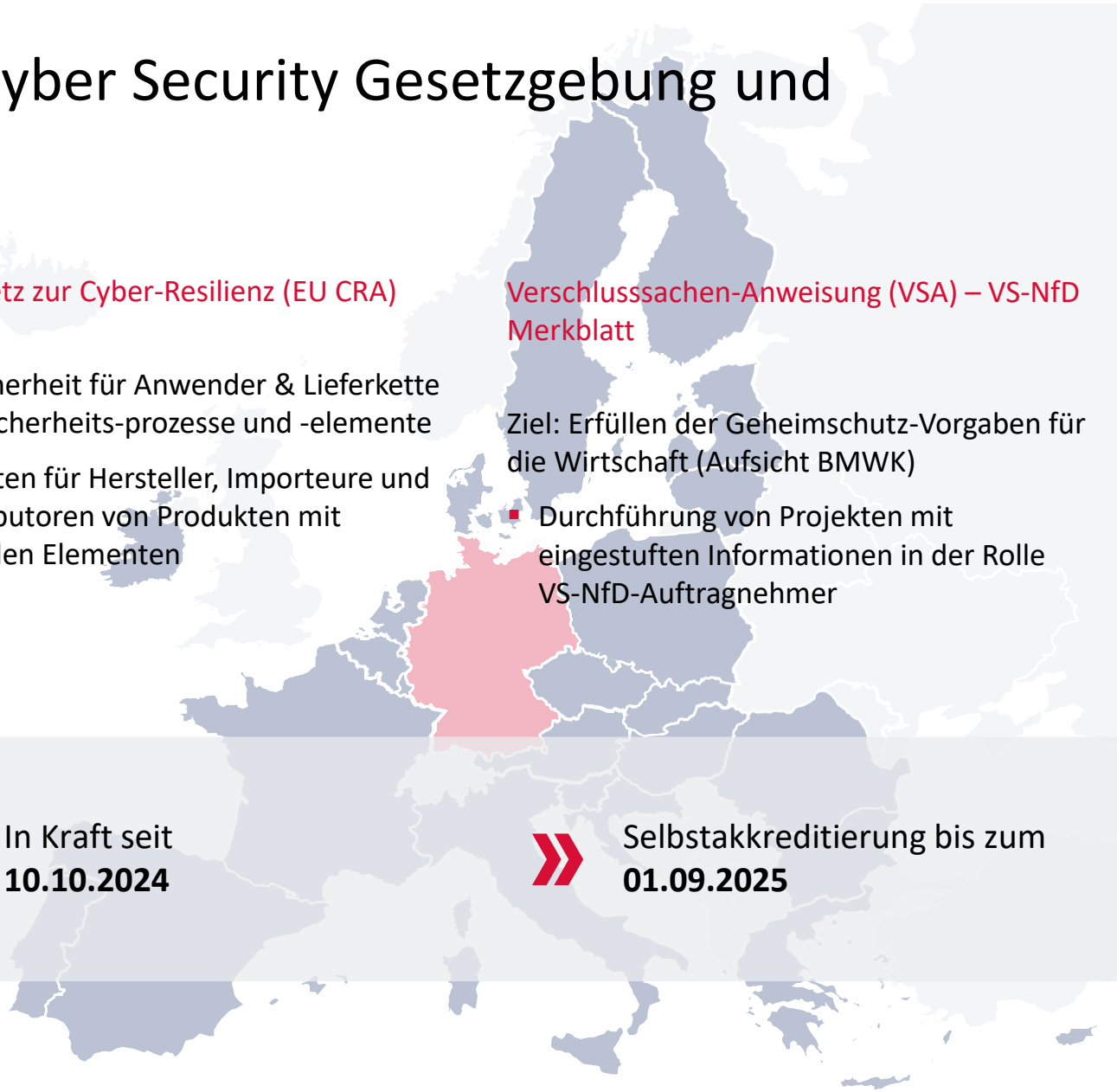
» In Kraft seit **10.10.2024**

Verschlusssachen-Anweisung (VSA) – VS-NfD Merkblatt

Ziel: Erfüllen der Geheimschutz-Vorgaben für die Wirtschaft (Aufsicht BMWK)

- Durchführung von Projekten mit eingestuften Informationen in der Rolle VS-NfD-Auftragnehmer

» Selbstakkreditierung bis zum **01.09.2025**



02

Maßnahmen

Technische Lösungen zur Verhinderung von Spionage

Datenverschlüsselung

WAS?

- Schutz sensibler Daten im Ruhezustand & bei Übertragung
- Einsatz sicherer Standards

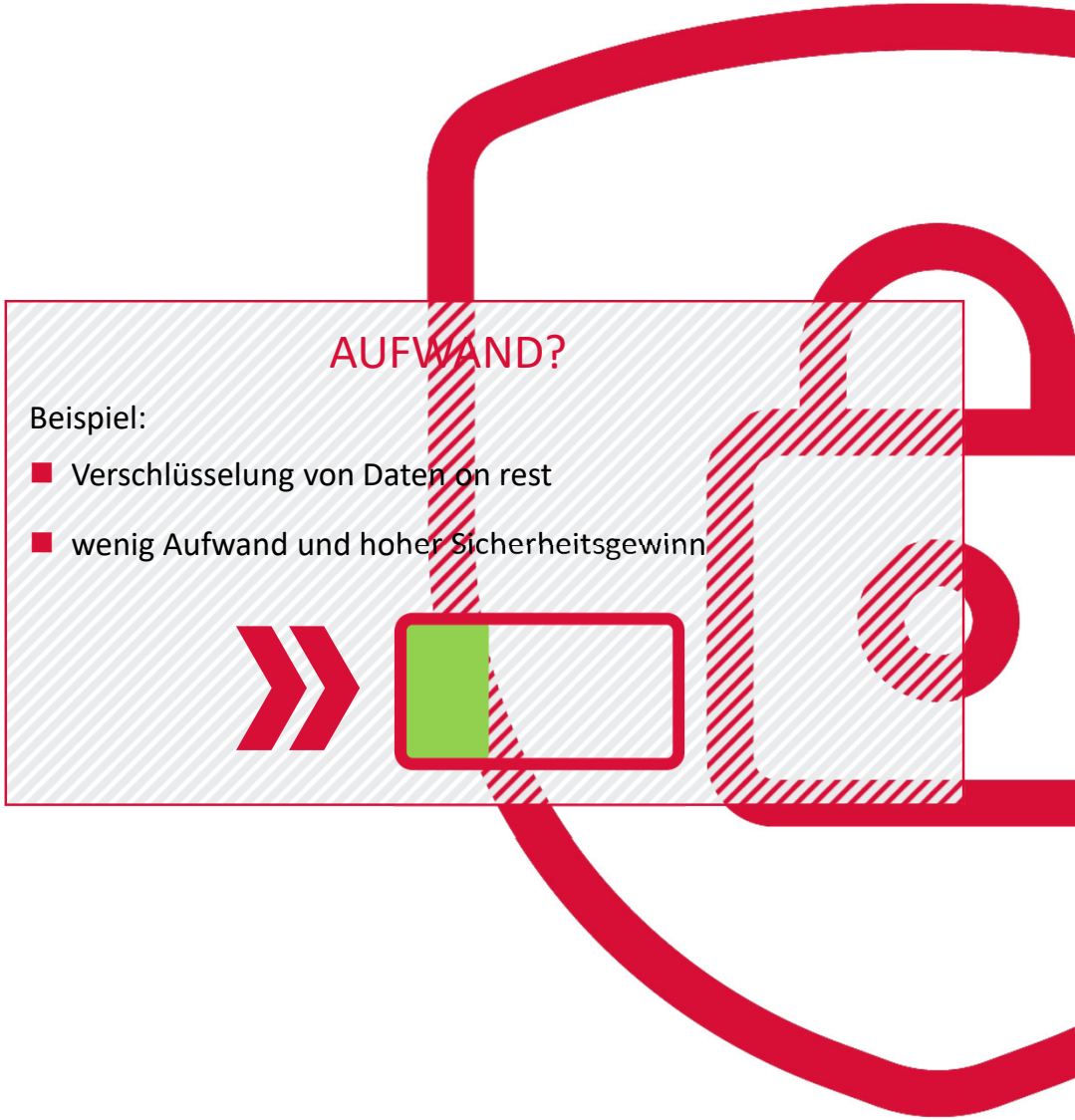
WARUM?

- Schutz der Vertraulichkeit
- Sicherstellung von Vertrauen
- Einhaltung gesetzlicher Vorgaben

AUFWAND?

Beispiel:

- Verschlüsselung von Daten on rest
- wenig Aufwand und hoher Sicherheitsgewinn



Zutrittsschutz

WAS?

- Kontrolle der Zutritte zu Unternehmensräumen
- Nutzung von Token, Schlüsselkarten oder PIN-Systemen für sensible Bereiche

WARUM?

- Schutz vor unberechtigtem Zutritt
- Schutz von Mitarbeitenden und Betriebsmitteln
- Nachvollziehbarkeit

AUFWAND?

- Mittlerer initialer Aufwand
- geringer laufender Aufwand

Absichern der mobilen Arbeit

WAS?

- Minimieren der Risiken der mobilen Arbeit
- Viele Optionen denkbar

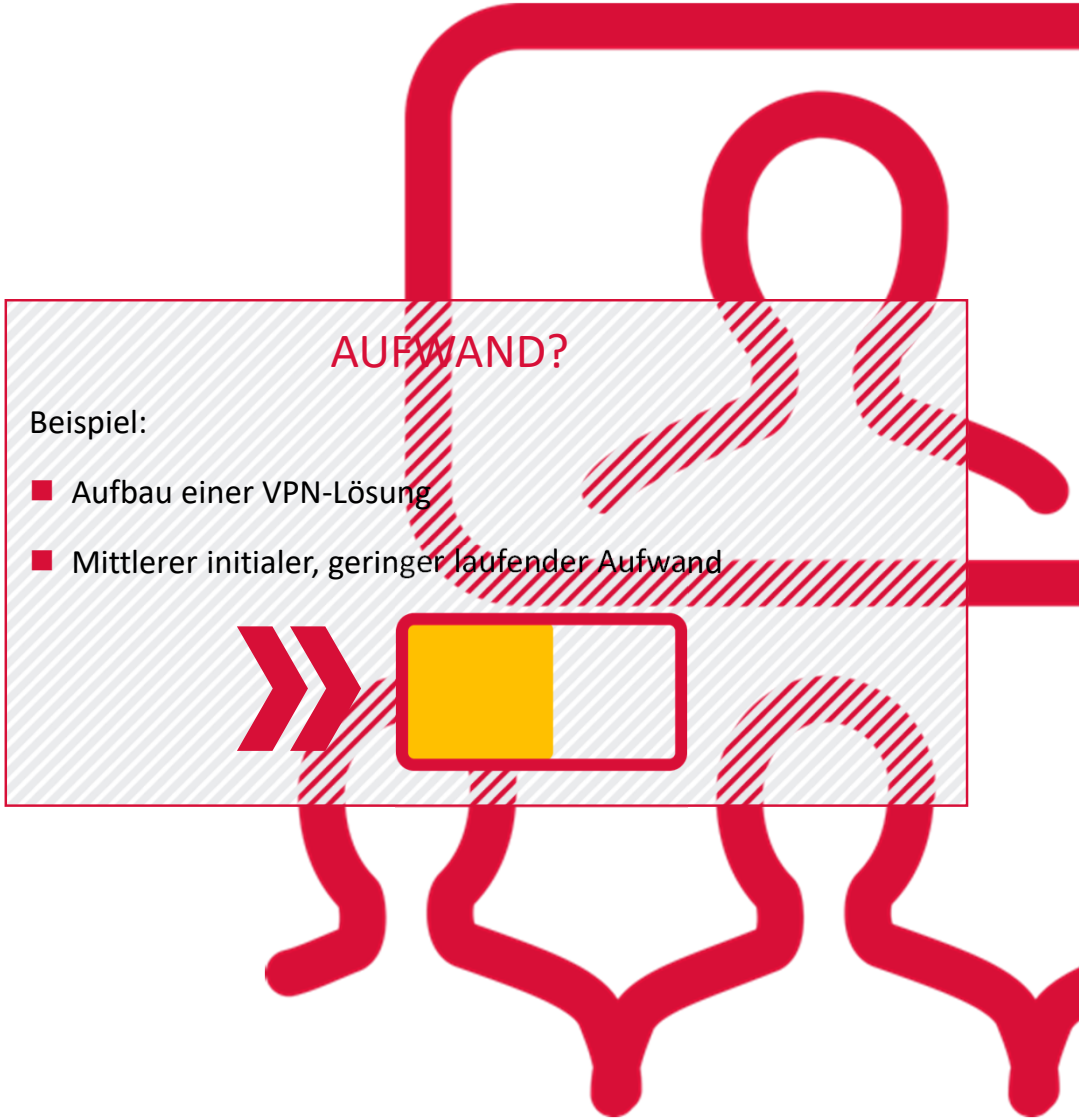
WARUM?

- Außerhalb des Büros ist ein anderes Angreiferprofil vorhanden
- Schutz vor Datenverlust und -diebstahl

AUFWAND?

Beispiel:

- Aufbau einer VPN-Lösung
- Mittlerer initialer, geringer laufender Aufwand



Patchmanagement

WAS?

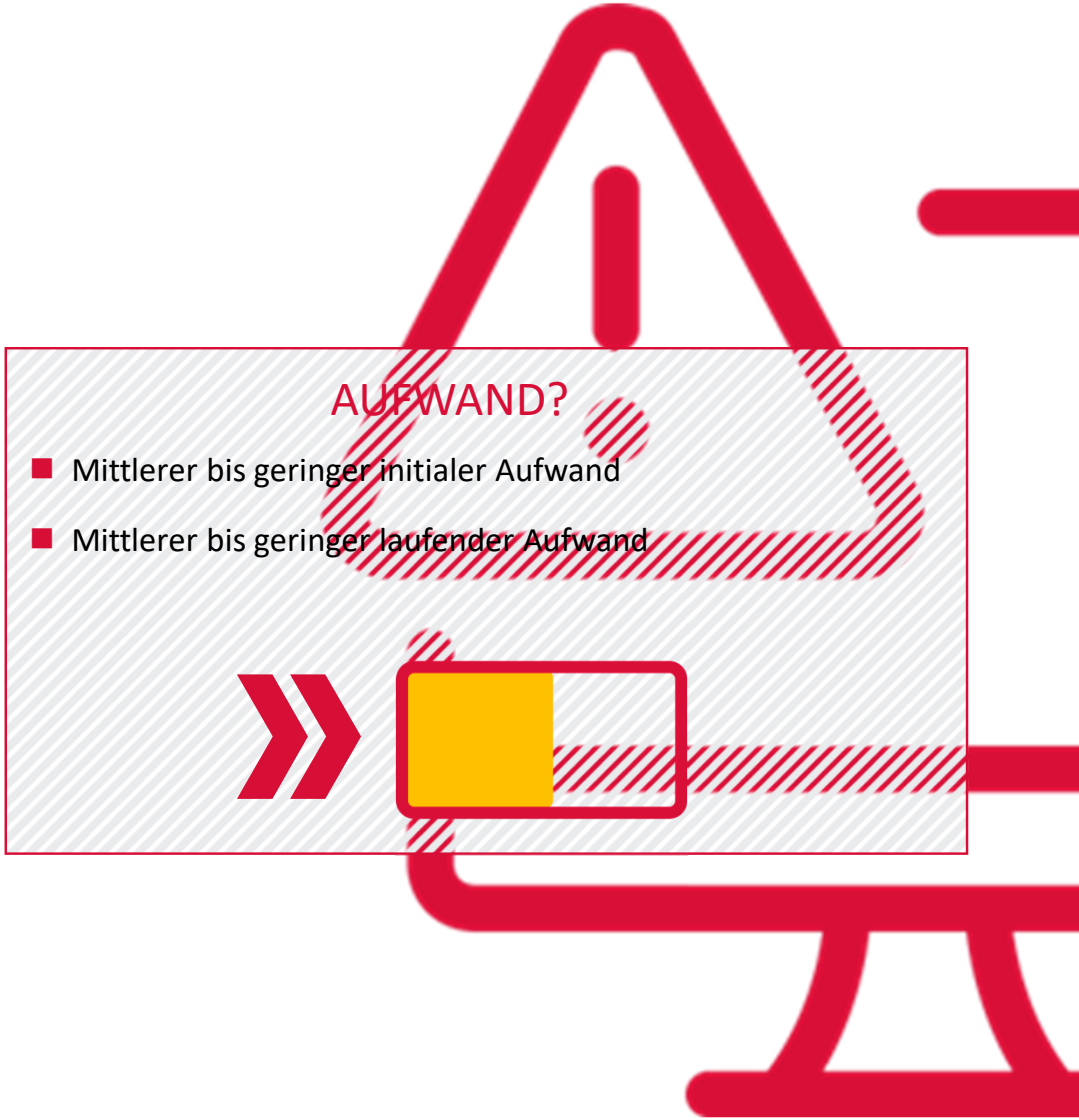
- Zentrale Funktionsprüfung und Verteilung von Sicherheits-Updates
- Patch-Management-Strategien für Server, Clients & IoT-Geräte

WARUM?

- Schließen von Sicherheitslücken in Betriebssystemen & Anwendungen
- Priorisierung nach Kritikalität

AUFWAND?

- Mittlerer bis geringer initialer Aufwand
- Mittlerer bis geringer laufender Aufwand



Netzwerksegmentierung

WAS?

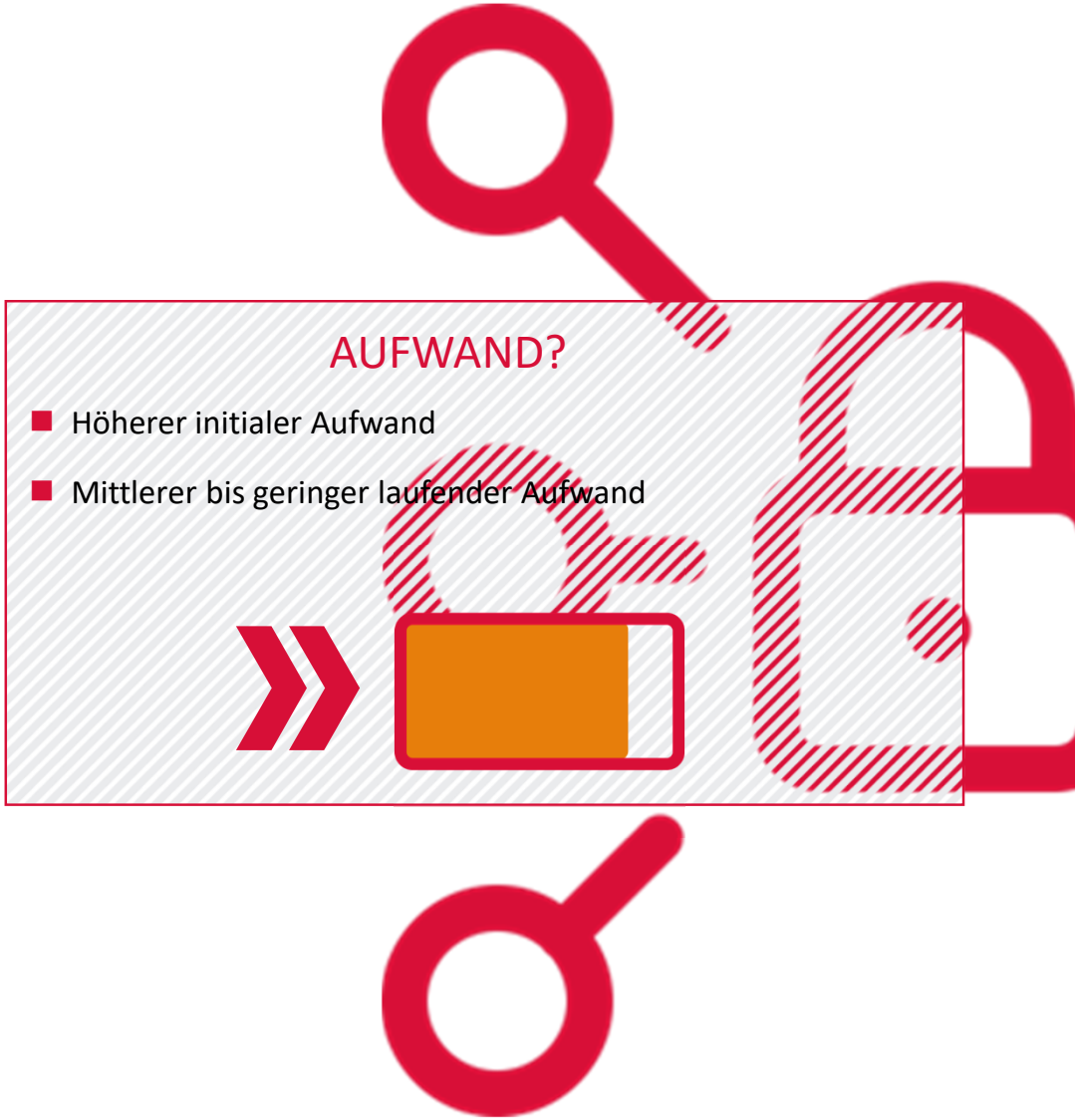
- Trennung sensibler Systeme in unterschiedliche Netzwerke
- Zero-Trust-Ansatz als Grundprinzip

WARUM?

- Begrenzung der Angriffsfläche
- Isolierung von Geräten mit geringen Schutzmaßnahmen

AUFWAND?

- Höherer initialer Aufwand
- Mittlerer bis geringer laufender Aufwand



Security Information & Event Management (SIEM)

WAS?

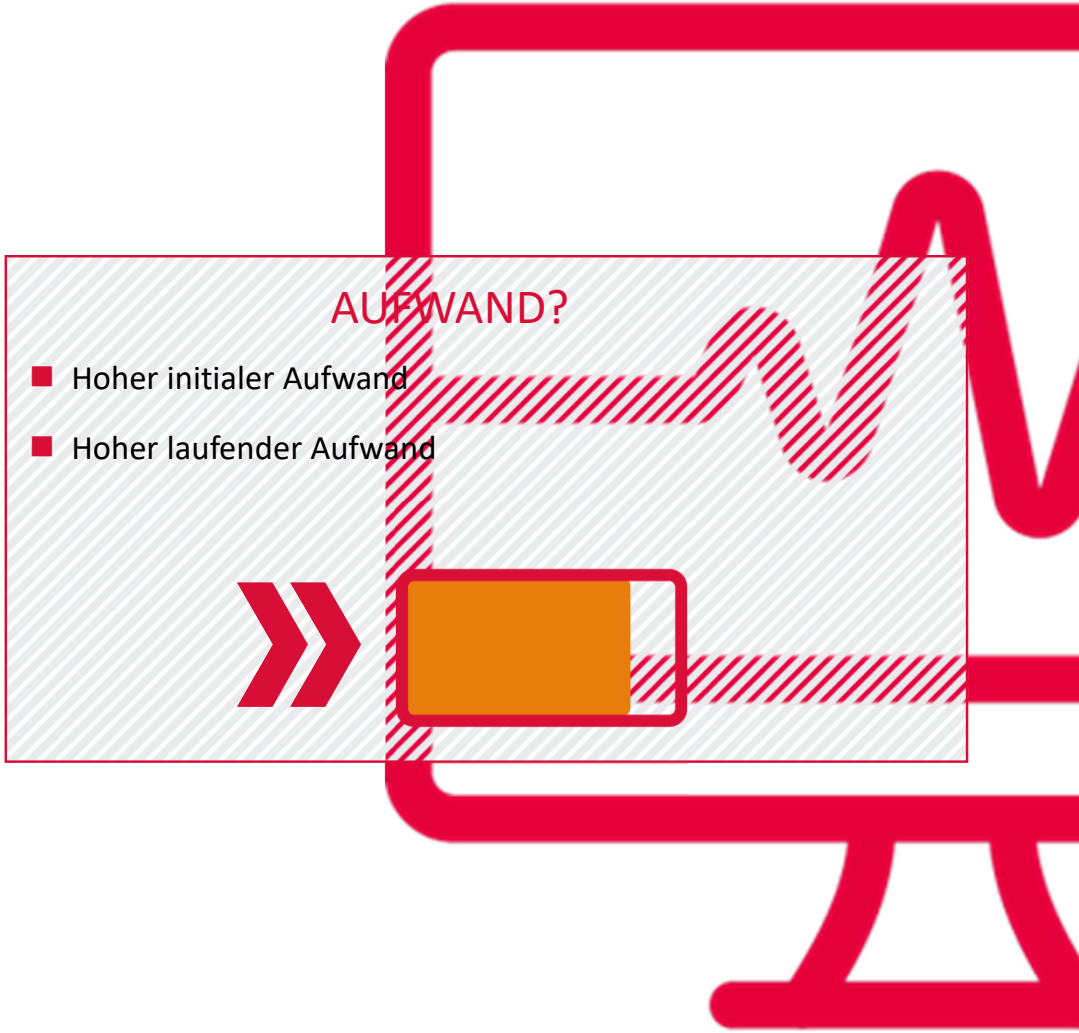
- Zentrale Erfassung sicherheitsrelevanter Ereignisse
- Präsentation von Echtzeitwarnungen

WARUM?

- Frühzeitige und nachvollziehbare Erkennung verdächtiger Aktivitäten
- Korrelation von Daten aus mehreren Quellen

AUFWAND?

- Hoher initialer Aufwand
- Hoher laufender Aufwand



03

Zusammen-fassung & Ausblick

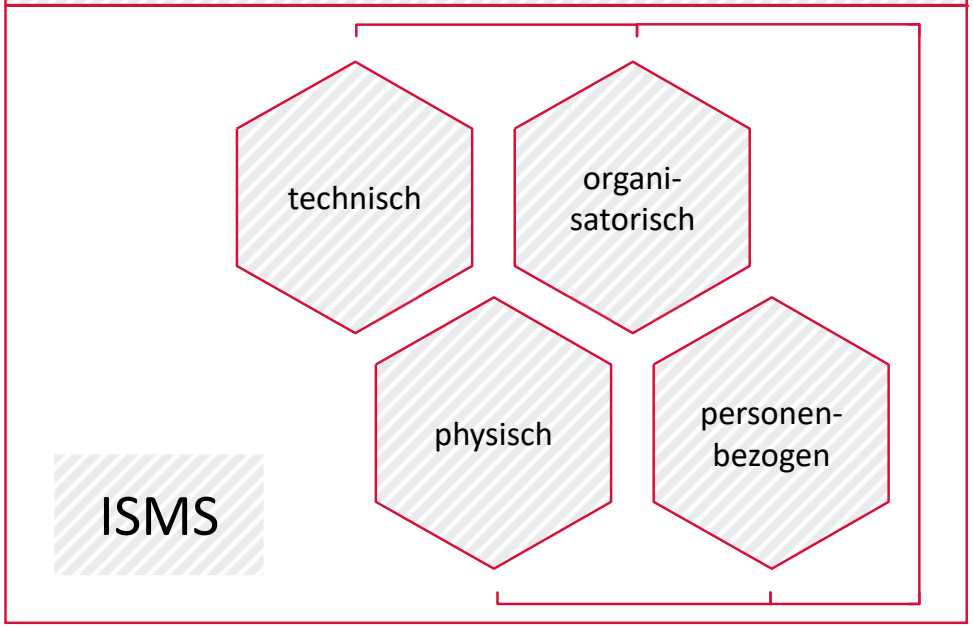
Zusammenfassung & Ausblick

Bedrohungslage ist ernst & dynamisch

Management muss Rahmenbedingungen & Ressourcen sichern

Sicherheit kostet Geld, aber nichts zu tun ist teurer!

Kombination mehrerer Maßnahmen notwendig




secunet

Ihre Ansprechpartner

Christoph Schambach
Senior Key Account Manager

Christoph.schambach@secunet.com

Tobias Schmidt
Senior Consultant

Tobias.schmidt@secunet.com

it-sa 2025

07. bis 09. Oktober 2025 | Messe Nürnberg

HOME OF IT SECURITY

Sie finden uns in in **Halle 9, Stand 516**.

Folgende Ausstellungsschwerpunkte stehen bei secunet 2025 im Fokus:

SINA Mobile: Ihr Smartphone wird zum VS-NfD Arbeitsplatz

SINA Workstation S: Gesamtlösung für den sicheren Arbeitsplatz für unterwegs und im Home-Office

SINA Communicator H: Das quantensichere Multikrypto-Telefon für Behörden und Streitkräfte, zugelassen für GEHEIM

SINA Workflow: Das erste und einzige durchgängig digitale Managementsystem für Verschlusssachen

Edge Computing: Sichere und regelkonforme Vernetzung von Geräten und Maschinen sowie Integration in digitale Dienste

Netzwerk-Überwachung: Systeme zur Angriffserkennung gemäß IT-Sicherheitsgesetz 2.0

Beratung zu Regulatorik: NIS-2 und CRA

secunet cloud solutions: Sichere und souveräne Open-Source-Cloud-Lösungen – on-premise, public oder auch kombiniert als flexible Hybrid Cloud

Mehr Informationen:
secunet.com

secunet