

Grundsätze der OT-Sicherheit



Bundesamt
für Sicherheit in der
Informationstechnik

Agenda

- Überblick zu Bedrohungen & Vorfällen und deren Auswirkungen auf die OT
- Gesetzliche Anforderungen NIS2, CRA, Arbeitsschutz
- Wo kann ich weitere Informationen finden, was sollte ich tun?

Überblick zu Bedrohungen & Vorfällen und deren Auswirkungen auf die OT

Ransomware – Internationale Schlagzeilen

Department of Justice Launches Global Action Against NetWalker Ransomware

NetWalker Defendant Charged, Dark Web Resource Disabled, Nearly \$500,000 Seized

Infrastruktur der Emotet-Schadsoftware zerschlagen

Deutschland initiiert „Takedown“ im Rahmen international koordinierter Maßnahmen – Schadsoftware auf zahlreichen Opfersystemen für die Täter unbrauchbar gemacht

Ransomware Egregor: Mehrere Affiliates verhaftet, Leak-Website offline

Emotet malware is back and rebuilding its botnet via TrickBot

JBS paid \$11 million to REvil ransomware, \$22.5M first demanded

Kaseya: Roughly 1,500 businesses hit by REvil ransomware attack

DarkSide: Server der Pipeline-Erpresser sind offline, Geld ist angeblich weg

Das Ransomware-Partnerprogramm DarkSide, das für den Ausfall der Colonial Pipeline in den USA verantwortlich gewesen sein soll, wurde offenbar dichtgemacht.

Ransomware-Gruppe ist plötzlich offline

Das REvil-Rätsel

Seit Dienstag sind die Websites der Erpressergruppe REvil nicht mehr erreichbar. Ist es das Werk von US-Behörden oder der russischen Regierung? Machen die Kriminellen nur Urlaub? Alle diese Theorien haben Schwächen.

Colonial Pipeline zahlt fast 5 Millionen Dollar Lösegeld an DarkSide-Erpresser

NACH CYBERANGRIFF AUF ANHALT-BITTERFELD

Spekulationen um Name der Hackergruppe - „Pay or Grief“ soll hinter Lösegeldforderung stecken

Schwachstellen in Produkten



Das BSI

Themen

IT-Sicherheitsvorfall

Karriere

Service



BEDROHUNGSSTUFE
2 Hoch

BSI-IT-SICHERHEITSMITTEILUNGEN • SICHERHEITSHINWEIS • 11.04.2025

Version 1.0: Fortinet FortiOS - Angreifende installierten persistenten Lesezugriff auf Firewalls

BEDROHUNGSSTUFE
3 Sehr hoch

BSI-IT-SICHERHEITSMITTEILUNGEN • SICHERHEITSHINWEIS • 09.04.2025

Version 1.1: Ivanti Connect Secure - Kritische Schwachstelle in End-of-Support und ungepatchten Systemen ausgenutzt

BEDROHUNGSSTUFE
1 Mittel

BSI-IT-SICHERHEITSMITTEILUNGEN • SICHERHEITSHINWEIS • 01.04.2025

Information zur Umstellung beim Versand von Warnungen

BEDROHUNGSSTUFE
2 Hoch

BSI-IT-SICHERHEITSMITTEILUNGEN • SICHERHEITSHINWEIS • 25.03.2025

Version 1.0: Kubernetes - Kritische Schwachstelle im Ingress NGINX Controller ermöglicht Clusterübernahme

BEDROHUNGSSTUFE
2 Hoch

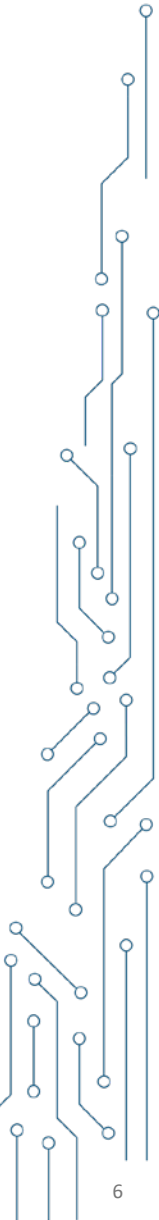
BSI-IT-SICHERHEITSMITTEILUNGEN • SICHERHEITSHINWEIS • 31.01.2025

Version 1.0: SonicWall SonicOS - Proof-of-Concept Exploit für Schwachstelle im SSLVPN veröffentlicht

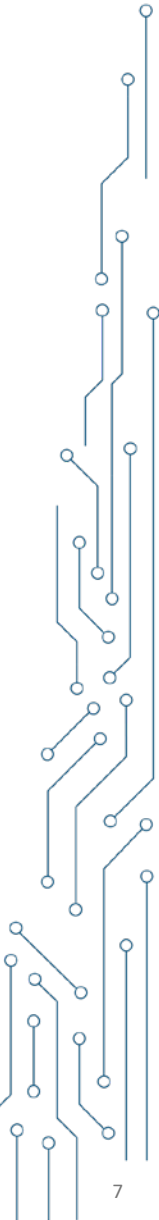
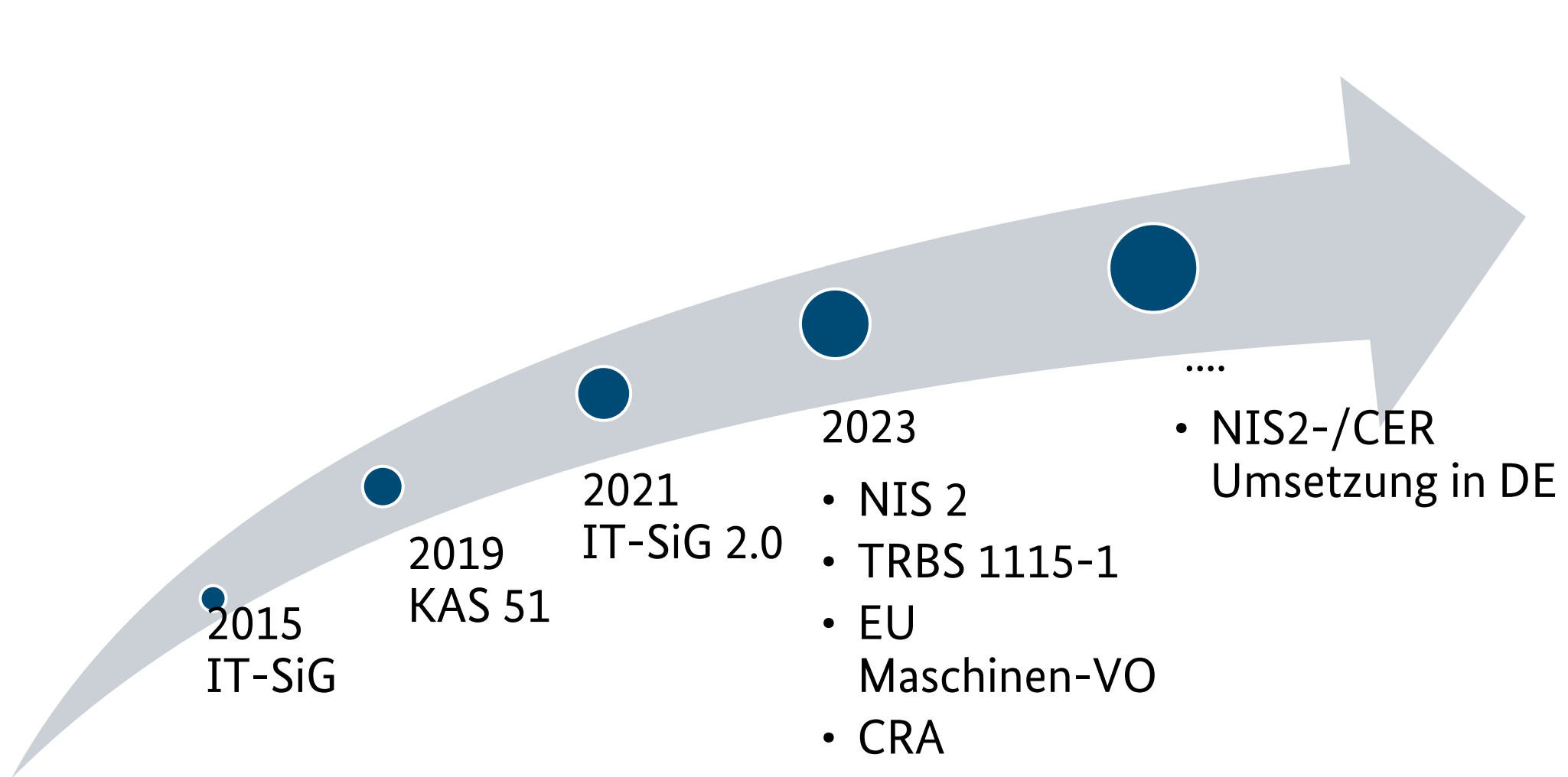
BEDROHUNGSSTUFE
2 Hoch

BSI-IT-SICHERHEITSMITTEILUNGEN • SICHERHEITSHINWEIS • 23.01.2025

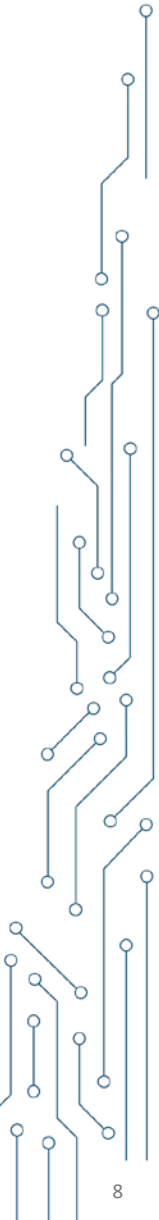
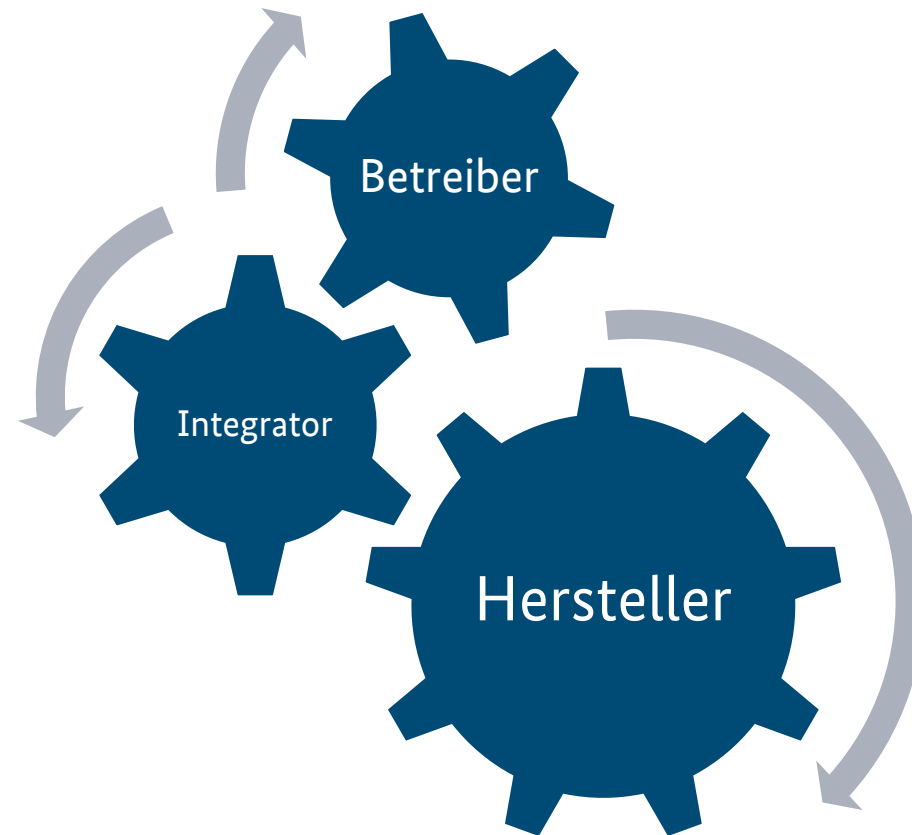
Version 1.0: SonicWall SMA 1000 Serie - Zero-Day Schwachstelle in Management Konsole geschlossen



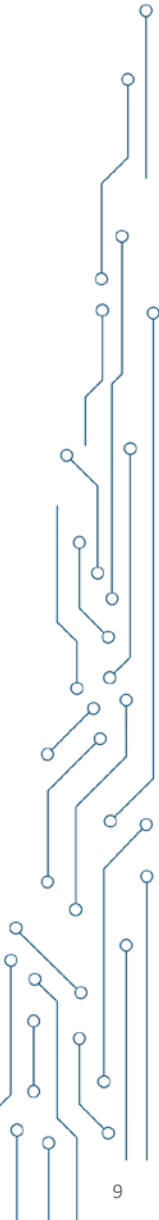
Pflichten zur Cybersicherheit in der OT



Verantwortung für Cybersicherheit



Herausforderungen für das erfolgreiche Umsetzen



Bestandsaufnahme

Assetmanagement

- Was habe ich in meiner Anlage?

Netzplan

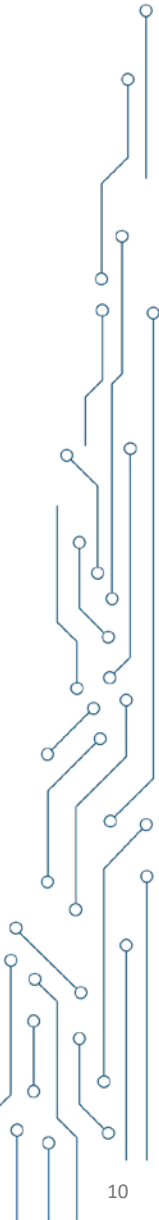
- Welche (Kabel-) Verbindungen habe ich in meiner Anlage?

Kommunikationsverbindungen

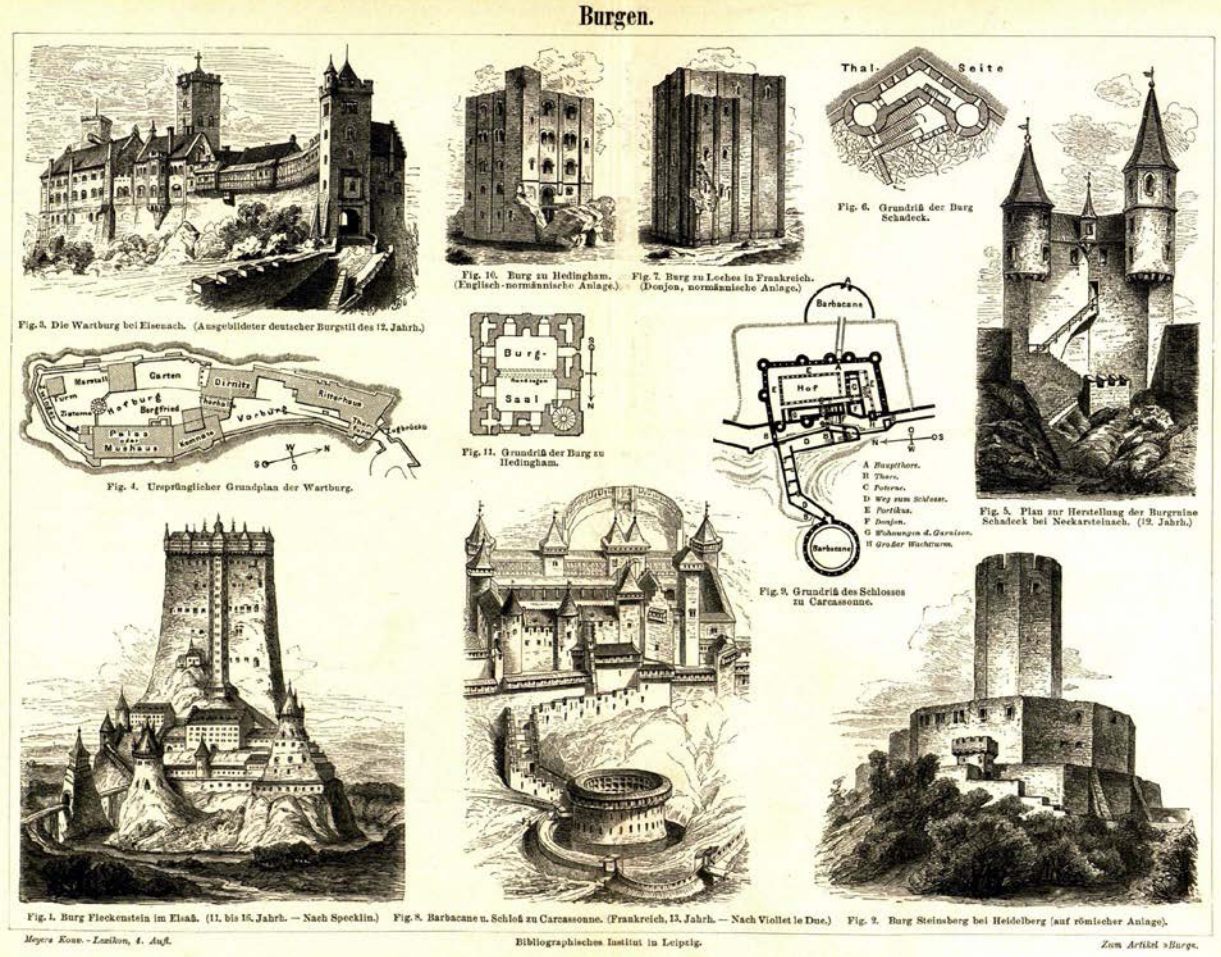
- Welche Systeme kommunizieren wie und warum miteinander?

Wie wichtig sind die Assets?

- Was passiert bei einem Ausfall?



Maßnahmen

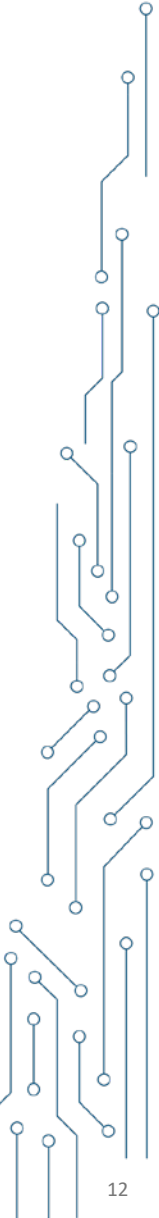


Quelle: Meyers Konversations-Lexikon, 4. Ausgabe, 3. Band



Angebote des BSI

- ICS-Security Kompendium
- IT- Grundschutz
- Allianz für Cybersicherheit



Zusammenfassung

Zusammenfassung



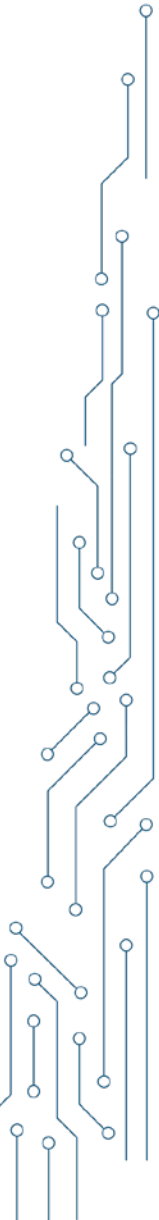
- Cyberangriffe können jeden treffen.



- Pflichten nehmen zu.



- Wenn nicht jetzt mit Cybersicherheit starten, wann dann?



Zusammenfassung



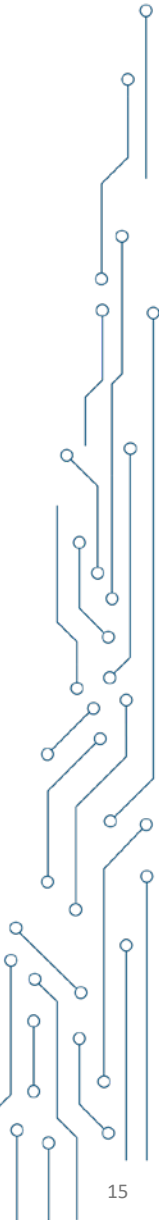
- Bestandsaufnahme machen und Abhängigkeiten identifizieren.



- Was passiert, wenn ein System nicht mehr verfügbar oder manipuliert ist?



- Schutzstrategien erarbeiten



Vielen Dank für Ihre Aufmerksamkeit!

WEKA Media GmbH & Co. KG
Römerstraße 4
D-86438 Kissing
www.weka.de



WEKA Media GmbH & Co. KG

Bei Fragen zu Lizenzen wenden Sie sich gerne an:

E-Mail: beratung@weka.de

Telefon: 08 2 33 / 23 - 7777