Kritische Infrastruktur

Wer fällt darunter? Was ist zu tun?

Henrik Knoblauch & Daniel Moosbauer
Bechtle Systemhaus Regensburg/München

Agenda

Vorstellung

KRITIS und das IT-Sicherheitsgesetz

Stand der Technik?

Erste Schritte Cyber-Security-Strategie

Anforderungen an ein ISMS

ISMS-Managementsysteme

Q&A

Henrik Knoblauch

Cybersecurity Specialist
APT Responder

Henrik.Knoblauch@bechtle.com

LinkedIn

Daniel Moosbauer

System Engineer/Consultant Security
Incident Response Coordinator

Daniel.Moosbauer@bechtle.com

LinkedIn

Security @ Bechtle.

>50

VENDOR PARTNER

Höchster Partner Status bei den Marktführern...

Auswahl Bechtle Focus Partners:

Check Point · paloalto · TREND MICRO · SOPHOS · CISCO · Trellix · Microsoft · FORTINET

>280

Mitarbeiter mit technischem Security-Profil

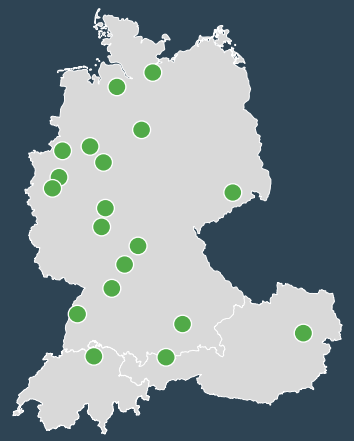
[ERMT 01/2022]

>1.200

INDIVIDUELLE ZERTIFIZIERUNGEN

16 SECURITY COMPETENCE CENTER IN DACH

Bechtle Security Kompetenz-Landkarte



> 30 Security-Teams in DACH

BECHTLE IST 2021 DER 3. GROESSTE **SECURITY INTEGRATOR IN DEUTSCHLAND**

Bechtle ist qualifizierter APT Response Dienstleister

Bundesamt für Sicherheit in der Informationstechnik

Managed Security Services 24x7x365

Zentrale und dezentrale Service-Einheiten

>100

REFERENZEN

6

Security Practices

KRITIS

Bin ich mit dabei?

„Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“

KRITIS-Definition der Bundesressorts

Quelle: BSI - Allgemeine Informationen zu KRITIS (bund.de)


Maßnahmen für eine offene Risikokommunikation
Kontaktstelle benennen
Absicherung prüfen lassen
KRITIS-Anforderungen
IT-Störungen melden
Präventionsmaßnahmen und Reaktionspläne ausarbeiten
Stand der Technik umsetzen
© TÜV NORD Akademie

Stand der Technik

Technisch und Organisatorisch

Technische Maßnahmen

Endpoint Detection Response	Network Detection Response	Log Management	Micro-Segmentierung	Reverse Proxy / WAF
Server Hardening	Vulnerability Scanning	Backup Konzept	Notfallplanung Cyberbedrohung	MFA

Organisatorische Maßnahmen

Organisation	Kontinuierliche Überwachung	Resourcen	IT-Dokumentation
Incident Management	Risk Management	Mitarbeiter Schulung	Notfallplanung Cyberbedrohung

Informationen zum „Stand der Technik:“

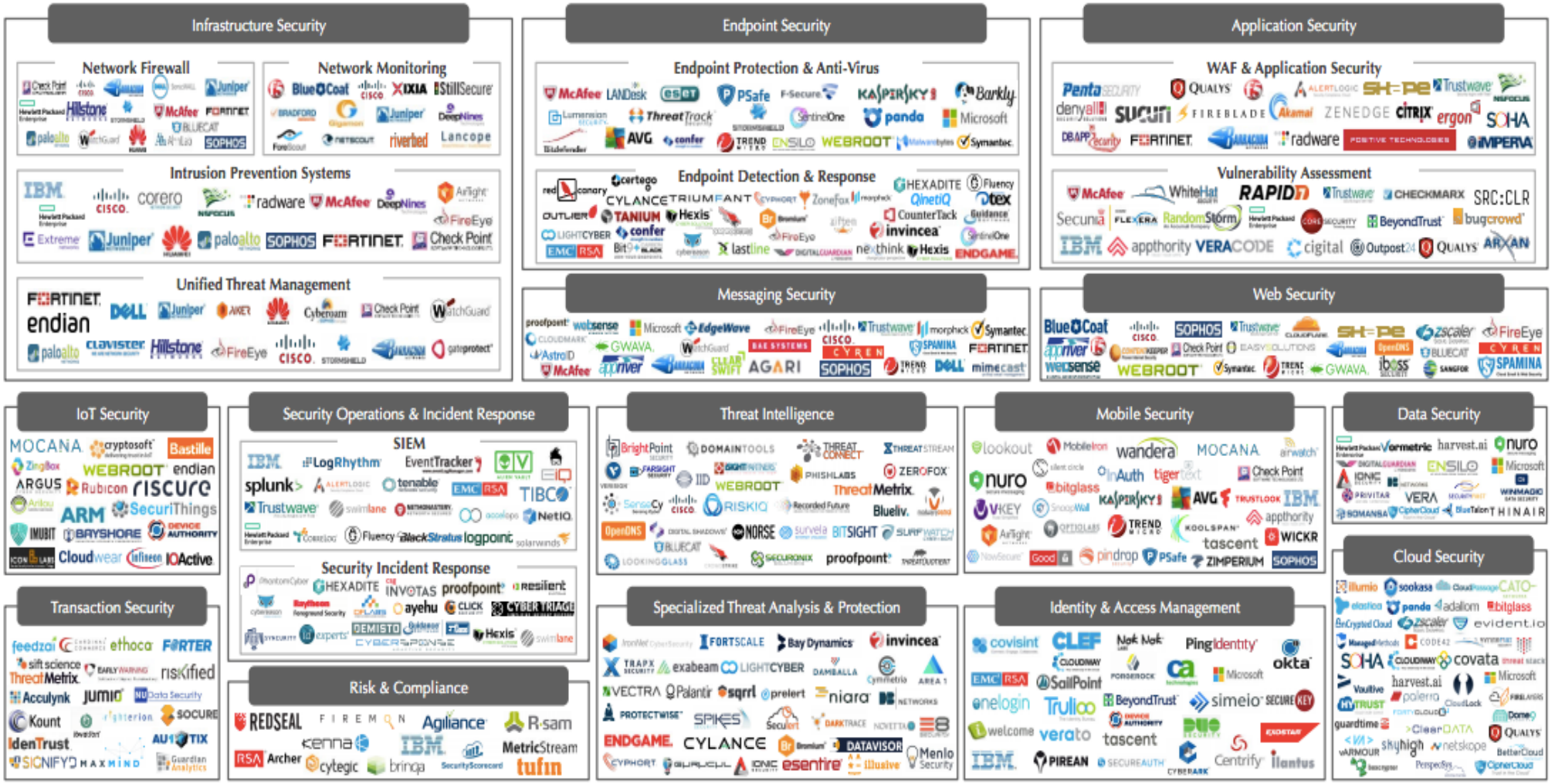
https://www.bsi.bund.de/dok/ohb3s

Stand der Technik?

Vielfältig und sehr komplex...

Security-Hersteller weltweit

- 2018 ca. 1.900
- 2025 ca. 4.000



Source: Momentum Partners.

Lösungsansätze.

Full Stack Security!

- Konsolidierung der Lösungen
- Ganzheitlicher Ansatz
- Security-as-a-System
  - Maximierung der Kompatibilität
  - Single-Pane-of-Glass Management
  - Automatisierte Reaktion
  - Bessere Forensik

„Best of Suite“

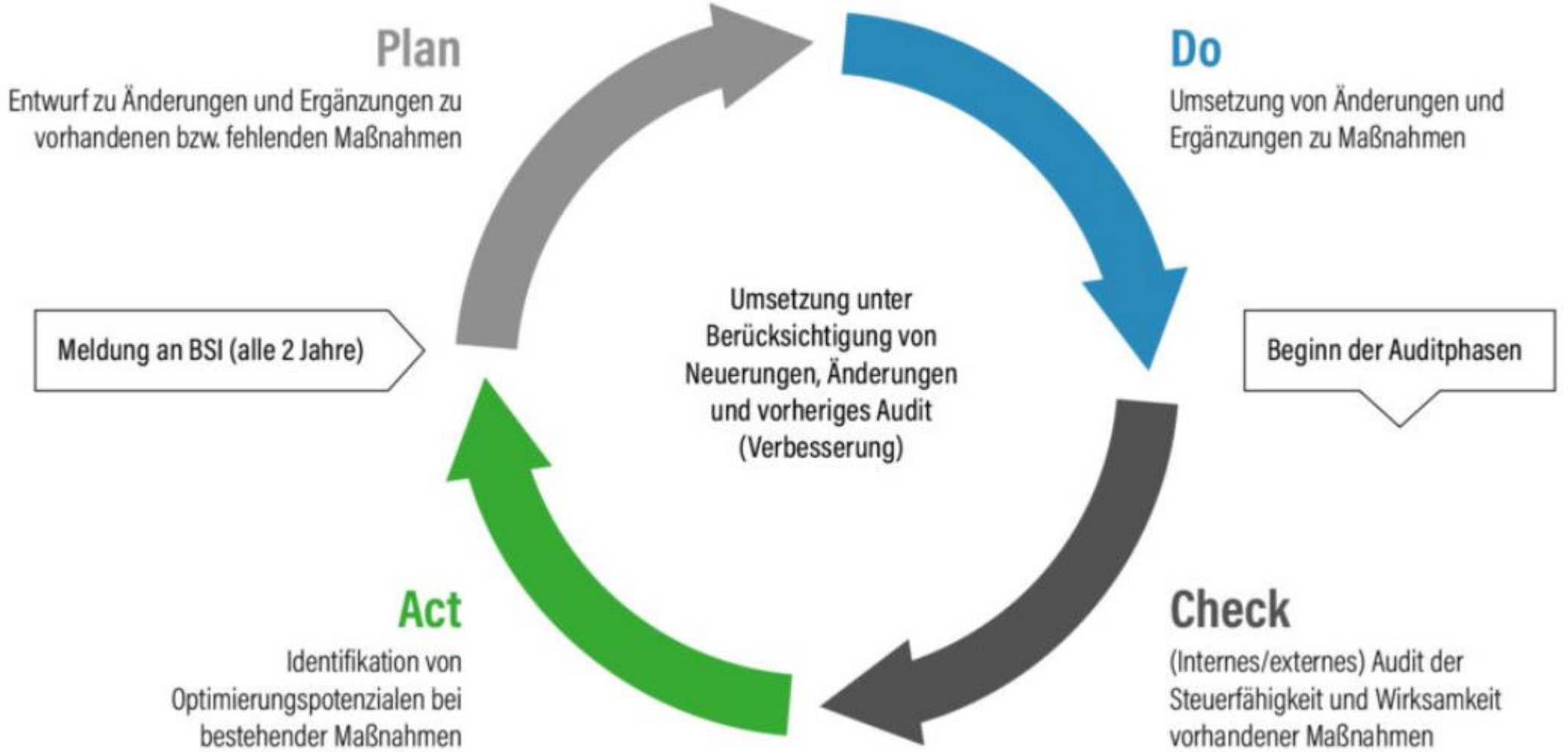
Gartner Magic Quadrant „Network Firewalls“ 2021

Erste Schritte Cyber-Security-Strategie

von Analyse bis Betrieb

Erste Schritte Cyber-Security-Strategie

PDCA-Cycle



Erste Schritte Cyber-Security-Strategie

aus der Praxis…

- Schwachstellen und Zero Day Lücken erkennen
- Risiko einschätzen
- Veraltete Systeme Upgraden/Isolieren
- Identitäten Schützen (MFA / Identitätsmangement/Rechte & Rollen)
- Expertise Schaffen
- Auditing & Monitoring (NDR;XDR;EDR;SIEM;SOC)
- Patchmanagement!
- System & Prozessüberblick

ISMS

Was es ist. Und was es nicht ist.

ISMS steht für Information Security Management System und wird genutzt, um die Sicherheit von Informationen in einer Organisation zu managen und zu schützen.

Ein ISMS ist **keine Software**. Sondern ein **gelebter Prozess**.

Dazu gehören unter anderem:

- Risikomanagement
- Informationssicherheitspolitik
- Organisation & Verantwortlichkeiten
- Awareness & Schulung
- Technische & Organisatorische Maßnahmen
- Incident Management
- Monitoring & Verbesserungen

ISMS-Managementsysteme

Es geht nicht um das Tool. Es geht darum, sich damit zu befassen.

Ein ISMS darf nicht als Pflicht betrachtet, sondern als Chance zur kontinuierlichen Verbesserung.

- ISO 27001
- IT-Grundschutz
- NIST Cybersecurity Framework
- IEC 62443
- **B3S (Branchenspezifische Sicherheitsstandards)**

Wichtig: BSI fordert das Risiken nicht nur benannt sind, sondern auch beseitigt werden müssen!