TEAL
ALWAYS CHALLENGING IT

FB PRO GMBH
System Hardening & Secure Configuration

# Zu Systemhärtung verpflichtet, und jetzt? Wie Sie Sicherheitslücken endlich schließen!

08.10.2025

Teal Technology Consulting GmbH & FB Pro GmbH

# Fabian Böhm

CEO & Founder von TEAL

https://www.teal-consulting.de/

LinkedIn


# Active Directory

# Architektur

TEAL
ALWAYS CHALLENGING IT

# Florian Bröder

CEO & Founder von FB Pro

https://www.fb-pro.com/

LinkedIn

# Matthias Laux

Analyst Secure Configuration
von FB Pro

https://www.fb-pro.com/

LinkedIn

# Systemhärtung

# IT-Infrastruktur

FB PRO GMBH
System Hardening & Secure Configuration

# Agenda – Congress @ ITSA

**TEIL 1**

1. Einleitung & Vorstellung Teal & FB Pro (10 Min.)
2. Identity is the new perimeter (25 Min.)
3. Systemhärtung – Die Theorie (15 Min.)
4. Systemhärtung – Regulatorische Anforderungen (15 Min.)
5. Systemhärtung – Vorgaben im Rahmen einer Policy (15 Min.)

**15-MINÜTIGE PAUSE – Getränke und Gewinnspiel**

**TEIL 2**

6. Systemhärtung – Die Praxis / Enforce Administrator (30 Min.)
7. Rollout Modelle (15 Min.)
8. TEAL Expertise Community (25 Min.)
9. Siegerehrung Gewinnspiel (5 Min.)
10. Q&A & Abschluss (10 Min.)

TEAL ALWAYS CHALLENGING IT

FB PRO GMBH
System Hardening & Secure Configuration

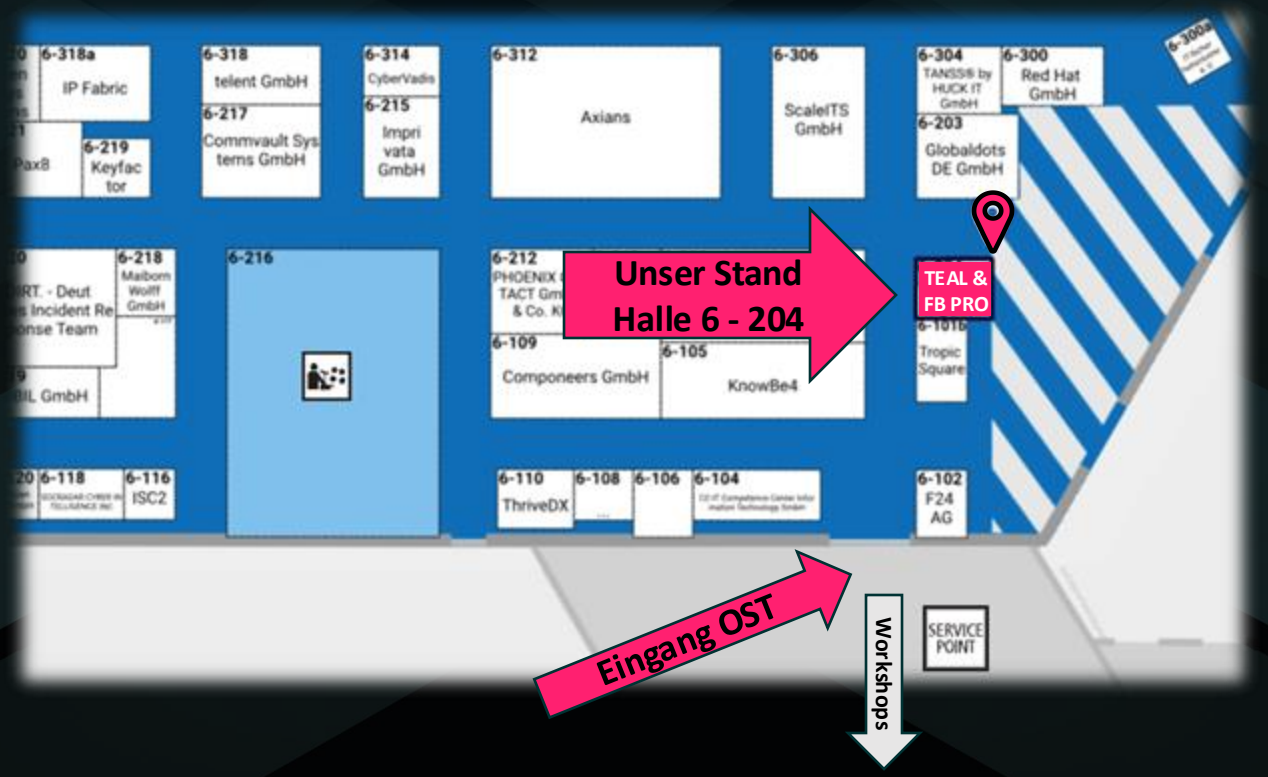
TEAL
ALWAYS CHALLENGING IT

FB PRO GMBH
System Hardening & Secure Configuration

# Vor Ort auf der it-sa 2025:

Besuchen Sie uns in **Halle 6 - Stand 204**

Wir freuen uns auf weiteren Austausch nach dem Workshop.



TEAL
ALWAYS CHALLENGING IT

FB PRO GMBH
System Hardening & Secure Configuration

# Identity is the new perimeter

# Identity is the new perimeter - Organisationen werden kompromittiert

BREAKING NEWS

Laut der Bitkom-Studie „Wirtschaftsschutz 2025 vom 18.09.“ waren 87 % der deutschen Unternehmen in den letzten 12 Monaten von Datendiebstahl betroffen.

BREAKING NEWS

Der durch Cyberangriffe verursachte wirtschaftliche Schaden in Deutschland beläuft sich laut Bitkom auf 289,2 Mrd. € in den letzten 12 Monaten.

BREAKING NEWS

Laut The Guardian musste nach einem schweren Cyberangriff auf Jaguar, Land Rover die Produktion stoppen, was die britische Regierung zu einer 1,5 Milliarden Pfund Kreditbürgschaft veranlasste.

BREAKING NEWS

90 % aller Cyberangriffe sind laut Mandiant, direkt oder indirekt mit dem Active Directory verbunden.

BREAKING NEWS

Laut dem aktuellen BSI-Lagebericht waren kritische Infrastrukturen besonders betroffen, darunter gezielte Angriffe auf Active Directory-Systeme, die zur Eskalation von Rechten genutzt wurden.

| Datum | Betroffene | Land | Sicherheitsvorfall |
|---|---|---|---|
| 06.10.2025 | The Lewis Group | US | Hacker kompromittieren Daten von 1.246 Personen. » Details |
| 06.10.2025 | Space Coast Vascular | US | Hacker kompromittieren Daten. » Details |
| 06.10.2025 | AppFolio | US | Cyber-Angriff. » Details |
| 03.10.2025 | Chemieunternehmen | DE | Spezialchemie-Hersteller mit Ransomware attackiert. » Details |
| 03.10.2025 | Superior Vision | US | Mitarbeiter von Brillenversicherer fällt auf Phishing-Mail herein. » Details |
| 03.10.2025 | People Encouraging People | US | Daten von 13.083 Patienten via Ransomware exfiltriert. » Details |
| 03.10.2025 | IKEA | SE | 14 Millionen Datensätze von schwedischem Möbelkonzern kompromittiert. » Details |
| 03.10.2025 | Moore & Van Allen PLLC | US | Hacker kompromittieren Daten. » Details |
| 03.10.2025 | Brightstar Global Solutions Corporation | US | Hacker kompromittieren Daten von 103.879 Personen. » Details |
| 03.10.2025 | Toyota Motor Corporation | JP | 64 GB aus Salesforce-Datenbank von Auto-Konzern gestohlen. » Details |

| Datum | Betroffene | Land | Sicherheitsvorfall |
|---|---|---|---|
| 03.10.2025 | KFC | US | Salesforce: Hacker stehlen offenbar 1,3 GB Daten von Fastfood-Gigant. » Details |
| 03.10.2025 | ASICS | JP | Japanischer Sportartikelhersteller von Salesforcehack betroffen. » Details |
| 03.10.2025 | UPS | US | Versanddienstleister ebenfalls von Salesforce-Hack betroffen. » Details |
| 03.10.2025 | GAP | US | Salesforce: 1 GB sensibler Datensätze von Modekonzern gestohlen. » Details |
| 03.10.2025 | Methodist Homes of Alabama & Northwest Florida | US | Hacker kompromittieren Daten von 25.579 Personen. » Details |
| 02.10.2025 | Red Hat | US | Angriff bestätigt: 570 GB aus GitLab-Repositories gestohlen. » Details |
| 02.10.2025 | Harbor | US | Hacker greifen 1 Woche lang auf Patientendaten zu. » Details |
| 02.10.2025 | The Rasevic Companies | US | Hacker kompromittieren Daten. » Details |
| 02.10.2025 | Safety Net Works/MVD Express OS | US | Hacker kompromittieren Daten von 1.892 Personen. » Details |

Sicherheitsvorfall-Datenbank: Datenpannen, Cyber-Atacken und andere Sicherheitsvorfälle | dsgvo-portal.de

Details zum Sicherheitsvorfall

heise online

Anmelden

heise+ Newsticker IT & Tech Security KI Developer Entertainment Wissenschaft Digital Heal

heise online > Politik > Cyberwar > Cyberangriff > Cyberattacke auf Dienstleister behindert Flughäfen in Europa

# Cyberattacke auf Dienstleister behindert Flughäfen in Europa

Ein europaweiter Dienstleister für Check-in und Boarding an Flughäfen ist Opfer eines Cyberangriffs geworden. Auch der Flughafen BER ist betroffen.

64

22.09.2025: Heise Online

[Sicherheitsvorfall-Datenbank: Datenpannen, Cyber-Atacken und andere Sicherheitsvorfälle | dsgvo-portal.de]

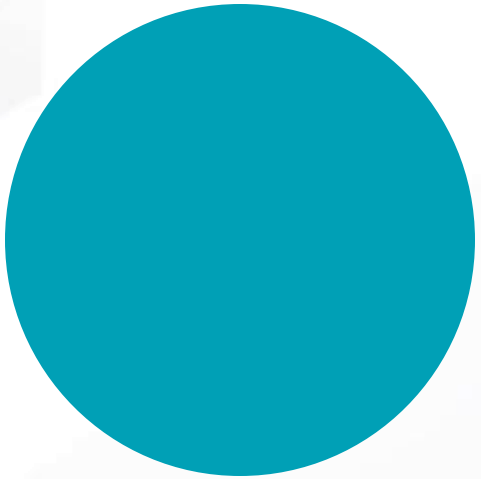
# Identity is the new perimeter - Wer das AD knackt, gewinnt alles

**Zentrale Bedeutung digitaler Identitäten:**
Digitale Identitäten, darunter Benutzerkonten, Service Accounts, Administratorzugänge sowie Maschinenidentitäten bilden den zentralen Zugangspunkt zu sämtlichen IT-Systemen. Wer diese Identitäten kontrolliert, hat die Kontrolle über das gesamte Unternehmen.

**Schutz von AD und Entra ID als strategisches Fundament:**
Der Schutz von Active Directory und Entra ID ist kein optionales Sicherheitsfeature. Er bildet das Fundament jeder wirksamen Zero-Trust-Strategie.

# Wie schützen sich Unternehmen heute?

# Wie schützen sich Unternehmen heute?

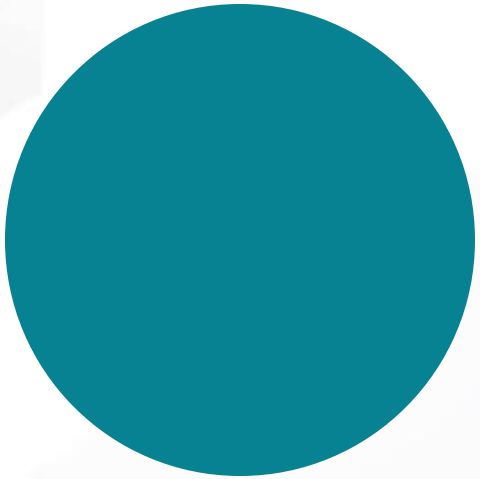


**Pentests werden ausgeführt**

# Wie schützen sich Unternehmen heute?

**Tools wie XDR, Schwachstellenscanner oder SIEM etc. werden eingeführt**

# Wie schützen sich Unternehmen heute?



**Firewalls und klassische Antivirus-Software**

# … und reicht das aus?

# NEIN!

# Wieso funktioniert das nicht?

1. **Ergebnisse von Pentests / Schwachstellen-Scans werden nur teilweise angegangen.** Danach landen die Berichte wieder in der Schublade.

2. **Angriffsfläche wird nicht konsequent verkleinert**

   Unsichere Protokolle und Konfigurationen sind vorhanden, weil die Auswirkungen unklar sind.

3. **Keine Zeit für die kontinuierliche Bearbeitung von Schwachstellen.** Das Tagesgeschäft gewinnt immer.

4. Wenn Zeit, **dann fehlt das konkrete Wissen**, wie eine Schwachstelle geschlossen wird.

5. **Altlasten werden nicht angegangen.**

   z.B. Veraltete Betriebssysteme an Produktions-maschinen oder die Abschaltung alter ERP-Systeme

TEAL
ALWAYS CHALLENGING IT

FB PRO GMBH
System Hardening & Secure Configuration

Kontinuität

Angriffsfläche verkleinern

Wissensaufbau

# Wie schütze ich mich richtig?

technische Schulden beseitigen

# 5 Schritte zur sicheren Infrastruktur

01 Regelmäßige Passwort-Überprüfungen

02 **Systemhärtung**

03 Zugriffsbeschränkungen (RBAC / least privileges)

04 Klassifizierung (Tiering-Strategie + PAW)

05 Identifikation kritischer Angriffswege

TEAL
ALWAYS CHALLENGING IT

FB PRO GMBH
System Hardening & Secure Configuration

# Systemhärtung

## Die Theorie

# Systemhärtung – Die Theorie

BREAKING NEWS

Laut der Bitkom-Studie „Wirtschaftsschutz 2025 vom 18.09.“ waren 87 % der deutschen Unternehmen in den letzten 12 Monaten von Datendiebst

BREAKING NEWS

he Schaden in
d. € in den letzten 12 Monaten.

Laut The Guardian musste
stoppen, was die britische
ste.

BREAKING NEWS

% aller Cyberangriffe sind laut Mandiant, direkt oder indirekt mit dem Active Directory verbunden.

BREAKING NEWS

Laut dem aktuellen BSI-Lagebericht waren kritische Infrastrukturen besonders betroffen, darunter gezielte Angriffe auf Active Directory-Systeme, die zur Eskalation von Rechten genutzt wurden.

Beispiele hatten wir schon genug.
Alle hier im Raum wissen, dass etwas
getan werden muss!

TEAL
ALWAYS CHALLENGING IT

FB PRO GMBH
System Hardening & Secure Configuration

# Es trifft jeden!

## Wenn es jeden trifft,...

# …dann stellen sich folgende Fragen

1. Wie gut greifen Maßnahmen, um Auswirkungen auf das Unternehmen zu verhindern?

2. Wie kann man Auswirkungen auf bestimmte Bereiche / einzelne Systeme / Services einschränken?

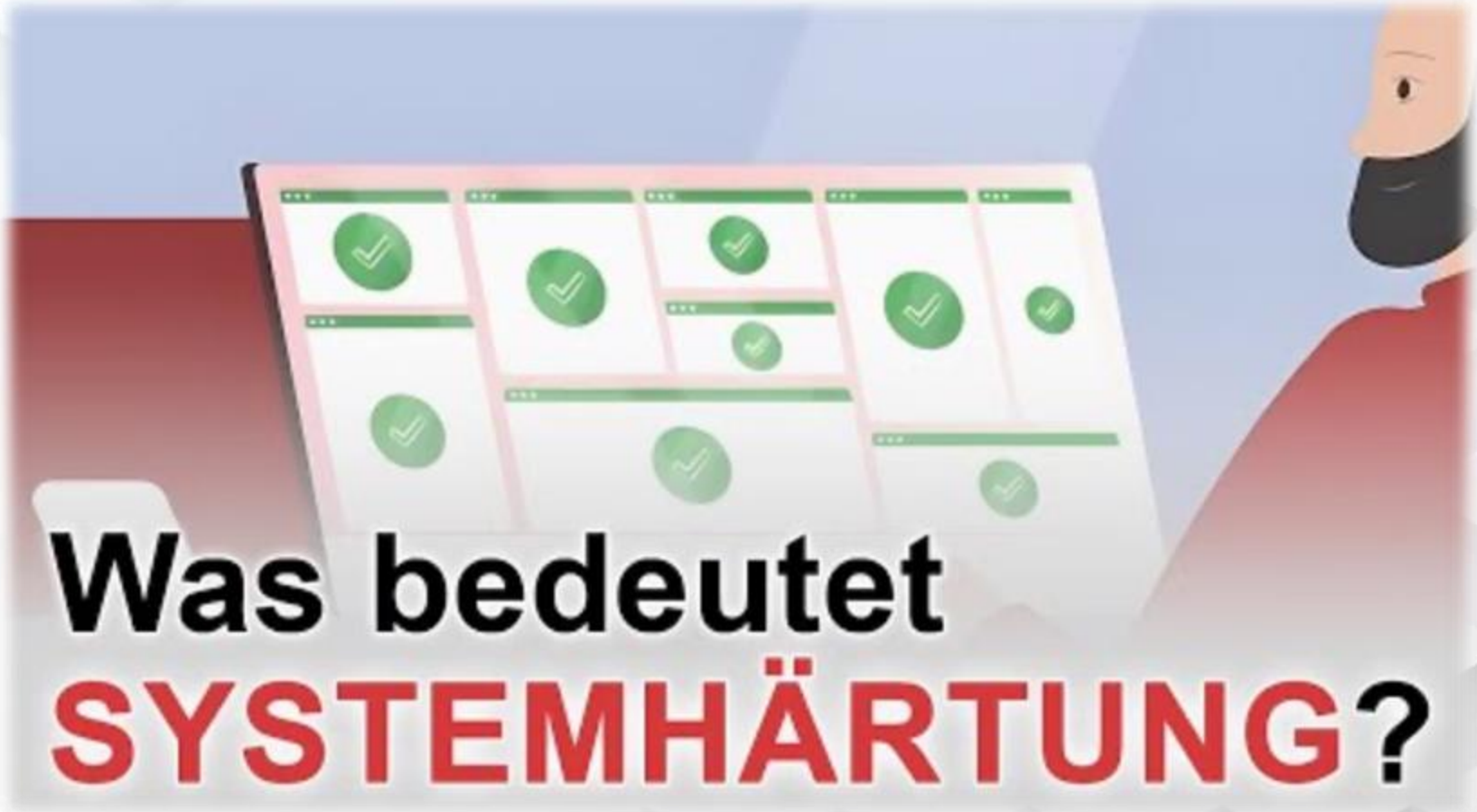
3. Wie lassen sich die Auswirkungen von Sicherheitsvorfällen, die zum totalen Erliegen führen, auf Kunden, Aktienkurs und Reputation sowie die resultierende Schadenshöhe so gering wie möglich halten?

TEAL
ALWAYS CHALLENGING IT

FB PRO GMBH
System Hardening & Secure Configuration

# Was ist eigentlich Systemhärtung / "sichere Konfiguration"?

# Systemhärtung – zum Einstieg ein Video




[Was ist Systemhärtung? Die wichtige IT-Security-Maßnahme in nur 1 Minute erklärt (youtube.com)]

# Systemhärtung – kurz erläutert

„System Hardening“ oder „Secure Configuration“ ist eine technische Präventivmaßnahme.
Durch Systemhärtung werden mögliche ausnutzbare Schwachstellen deaktiviert und können nicht mehr ausgenutzt werden.

Bei einer professionellen Systemhärtung wird ein IT-System **tiefgehend technisch konfiguriert**. Eine Anomalie-Erkennung sorgt dafür, dass **Änderungen an Sicherheitskonfiguration erkannt** und im **Rahmen prozessualer Integration** an Security-Teams gemeldet werden**. Berichte weisen den Härtungsgrad** der Systeme zentral aus, um ein ausreichendes Schutzniveau sicherzustellen, zu halten und transparent zu machen. **Konfigurationsdoku (SOLL/IST) kann auf Knopfdruck exportiert** werden und liefert so schnell **Transparenz** im Rahmen regulatorischer ANforderungen!

**Mehrwert**

- Dauerhafte **Erhöhung und Kontrolle des Schutz-Niveaus**
- **Reduzierung der Wahrscheinlichkeit** eines erfolgreichen Angriffs
- **Risikominimierung** bei erfolgreichen Angriffen
- **Verlangsamung von Schad-Software-Ausbreitung** im Fall der Fälle
- **Nachweiserzeugung** für Cyber-Versicherungen

Systemhärtung in Zahlen – da kommen schnell an die 1000 Einstellungen zusammen

**Betriebssystem-Ebene:**

- BSI Empfehlungen für Windows 10: 393 Einstellungen
- CIS Benchmarks für Windows 11: 600 Einstellungen
- MS Security Baselines Windows 11: 415 Einstellungen
- CIS Benchmarks Server 2025: 495 Einstellungen
- MS Security Baseline Server 2025: 591 Einstellungen

**Logging- / Audit-Funktionen.**

- CIS Benchmarks: 40 Einstellungen
- BSI Empfehlungen: 50 Einstellungen

**Browser-Konfiguration**

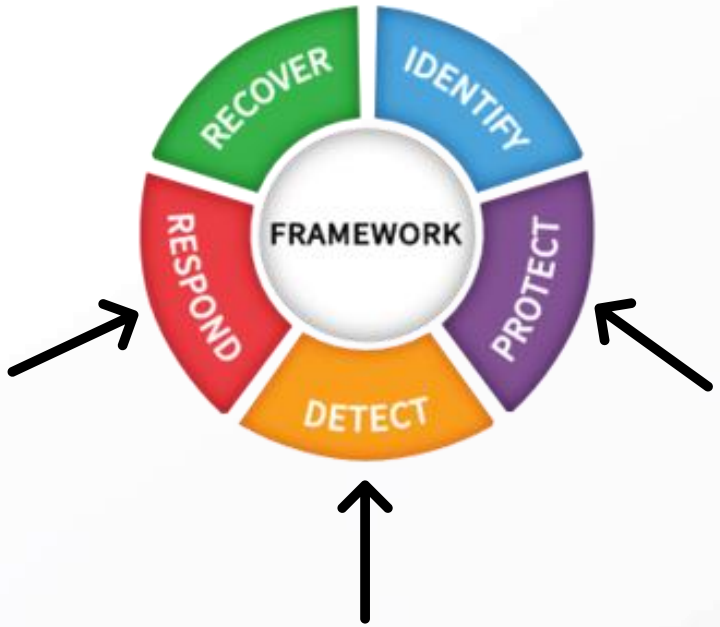
- CIS MS Edge: 135 Einstellungen
- CIS Chrome: 67 Einstellungen
- MS Security Baseline: 19 Einstellungen

**Office-Konfiguration**

- CIS Empfehlungen: 216 Einstellungen

# Systemhärtung – kurz erläutert

Es gibt verschiedene Rahmenwerke wie bspw. vom NIST (amerikanische Standardisierungsorganisation), die kritische Funktionen identifizieren.




| Technology | PROTECT | DETECT | RESPOND |
|---|---|---|---|
| Anti-Malware solutions | | X | X |
| Threat-Intel solutions | | X | X |
| EDR/XDR solutions | | X | X |
| MDR solutions | | X | X |
| Vulnerability scanner | | X | |
| SIEM solutions | | X | X (SOC, IM process) |
| Compromise Assessment | | X | X |
| Hardening | X | | |
| Enforce Administrator | X | X | IM process |

**Was macht mehr Sinn**? Ein 24/7 Team, das die Tür überwacht oder doch eher eine verschlossene Tür?

# Systemhärtung – Mitigation für das TOP Risiko

**A plea for network defenders and software manufacturers to fix common problems.**

## EXECUTIVE SUMMARY

The National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint cybersecurity advisory (CSA) to highlight the most common cybersecurity misconfigurations in large organizations, and detail the tactics, techniques, and procedures (TTPs) actors use to exploit these misconfigurations.

Through NSA and CISA Red and Blue team assessments, as well as through the activities of NSA and CISA Hunt and Incident Response teams, the agencies identified the following 10 most common network misconfigurations:

1. Default configurations of software and applications
2. Improper separation of user/administrator privilege
3. Insufficient internal network monitoring
4. Lack of network segmentation
5. Poor patch management
6. Bypass of system access controls
7. Weak or misconfigured multifactor authentication (MFA) methods
8. Insufficient access control lists (ACLs) on network shares and services
9. Poor credential hygiene
10. Unrestricted code execution

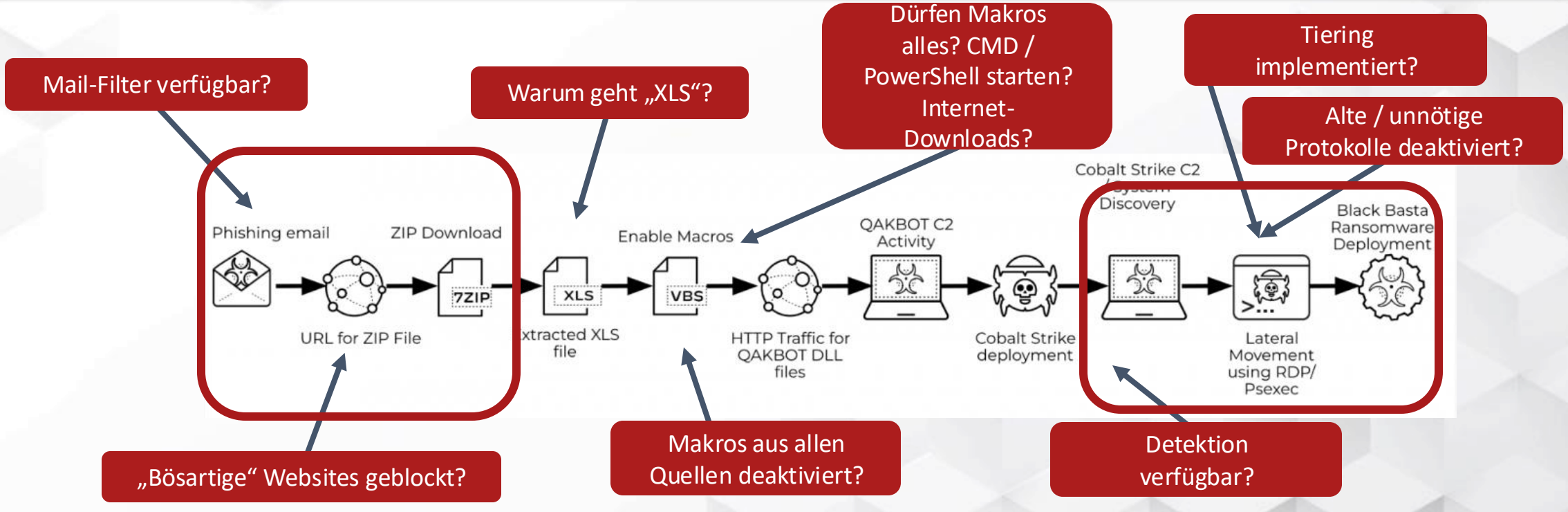
NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations | CISA

**Kann die Antwort auf „fehlende sinnvolle / sichere Konfiguration“ auf der Ebene „detection und response“ passieren?**

**Oder eher doch auf der Ebene „richtig“ zu konfigurieren?**

# Systemhärtung – Ein Angriffsvektor

Sichere Konfiguration auf Basis von Standards nimmt hunderte von Einstellungen auf verschiedenen Ebenen vor.




Forensik überhaupt machbar? Audit-/ Eventlogs sinnvoll konfiguriert? Log-Daten / Eventlog-Daten separat gespeichert?

# Systemhärtung – gerade auch im Kontext aktueller Angriffstrends extrem wichtig!

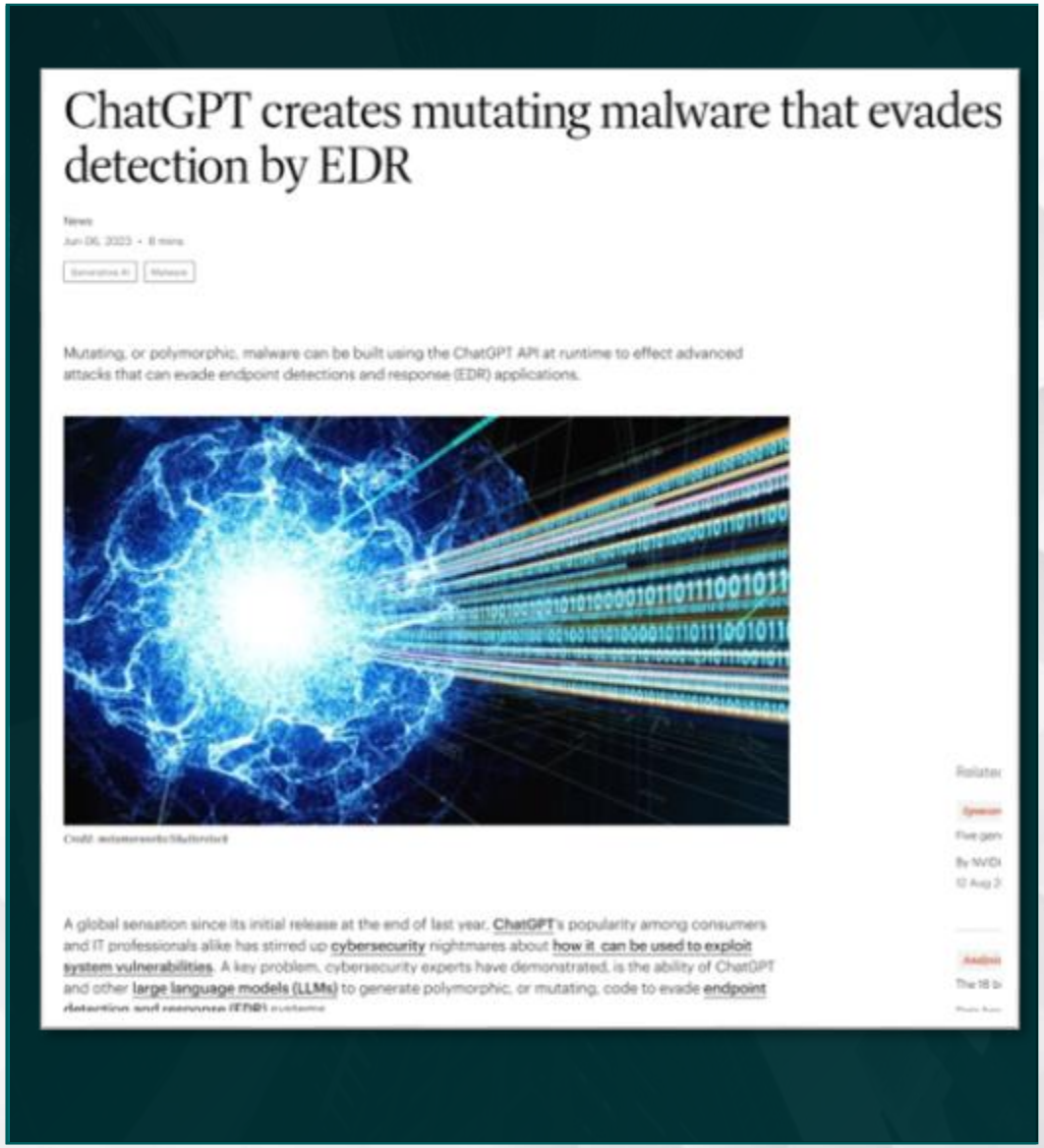
Systemhärtung als Präventivmaßnahme ist auch in “modernen” Angriffsszenarien eine wirkungsvolle Maßnahme, bspw. bei

- KI- / AI-basierten Angriffsmethoden,
- “Polymorpher Malware” (“mutating malware”) oder anderen.

**Warum?**

Systemhärtung hat einen fundamentalen Unterschied zu anderen Maßnahmen.

- Es geht nicht darum, jede neue Methode (Mail, Pattern, Verhalten, etc) zu erkennen und dann zu hoffen, die richtige Reaktion zu haben.
- Der Ansatz ist, die Tür (“den Angriffsvektor”) zu schließen und damit den Weg an sich zu verhindern




ChatGPT creates mutating malware that evades detection by EDR | CSO Online


# Systemhärtung – wie geht die Umsetzung nicht?

**“Hey, ich hab die Firewall eingeschaltet – wir sind sicher!”**

- Besser: Standardisierte Frameworks mit hunderten Einstellungen als Basis nutzen

**“Ich habe das alte Protokoll abgeschaltet!”**

- Besser: Standardisierte, industrieerprobte Empfehlungen und Vorgaben definieren klar, welche Einstellungen / Protokolle sinnvoll sind und welche nicht

**“Ich mach das schnell von Hand oder bau mir ein Script!”**

- Für den Einzelplatzrechner oder den privaten Computer technisch machbar
- Für Unternehmen mit hunderten oder gar tausenden von Systemen kein Ansatz – übrigens einer der Gründe für den “Fachkräftemangel” (wenn alles von Hand gemacht wird)

**“Das Script läuft bei der Installation durch!”**

- Besser: Regelmäßige automatisierte Kontrolle und Einbindung in Prozesse bei Abweichungen

# Systemhärtung – NACH einem Angriff…

…ist man immer schlauer.

Wenn die „Feuerwehr“ da war, sind die Maßnahmen klar. Anbei ein Beispiel aus dem (öffentlich verfügbaren) Forensik-Bericht aus dem Umfeld der SIT NRW.

## 7.1 Kurzfristig

- **Forensik-Scan:** Alle Systeme in betroffenen Netzbereichen werden mittels THOR-Scan auf schadhafte Aktivitäten untersucht. Bei unauffälligen Ergebnissen erfolgt eine bedingte Sicherheitseinstufung.
- **Wiederherstellung aus Backup:** Systeme sollten bevorzugt aus Backups vor dem 18. Oktober 2023 wiederhergestellt werden, da eine Kompromittierung vor diesem Datum als unwahrscheinlich gilt.
- **Netzwerksegmentierung:** Einführung physischer und virtueller Trennung von Systemen und definierten Zugriffskontrollen.
- **Next-Generation-Firewall:** Konfiguration strenger Zugriffsregeln zur Minimierung von Bedrohungen und Kontrolle des Datenverkehrs.
- **Best Practices für Systemhärtung:** Implementierung grundlegender Sicherheitsmaßnahmen wie Rollen- und Berechtigungskonzepte und Deaktivierung unnötiger Dienste.
- **Absicherung von Benutzerkonten:** Einführung starker Passwortrichtlinien und Multifaktor-Authentifizierung, insbesondere für administrative Konten.
- **Endpoint Detection and Response (EDR):** Einsatz einer EDR-Lösung zur Erkennung und Reaktion auf abnormales Verhalten.
- **Protokollierung:** Erfassung und zentrale Speicherung sicherheitsrelevanter System- und Netzwerkaktivitäten.

## 7.2 Mittelfristig

- **Erweiterte Netzwerksegmentierung:** Ausarbeitung eines umfassenden Segmentierungskonzepts und Mikrosegmentierung für kritische Bereiche.
- **Firewall-Optimierung:** Analyse des verschlüsselten Datenverkehrs und regelmäßige Anpassung der Firewall-Einstellungen.
- **Erweiterte Systemhärtung:** Entwicklung und Umsetzung erweiterter Sicherheitsstandards für verschiedene Systemtypen.
- **Erweiterung der Benutzerkontenabsicherung:** Implementierung von Multifaktor-Authentifizierung für alle Nutzer und Evaluierung spezieller Lösungen für privilegierte Zugriffe.
- **Erweiterte EDR-Maßnahmen:** Einsatz zusätzlicher Schutzmodule innerhalb der EDR-Lösung, um Anomalien umfassender zu analysieren.
- **Erweiterte Protokollierung:** Einführung eines Next-Generation-SIEM-Systems für eine automatisierte Analyse großer Datenmengen.
- **Schwachstellen-Management:** Regelmäßige Schwachstellenscans in allen Netzbereichen, unabhängig von deren Zonierung.

SIT_Incident_Response_v1.1.pdf

TEAL
ALWAYS CHALLENGING IT

FB PRO GMBH
System Hardening & Secure Configuration

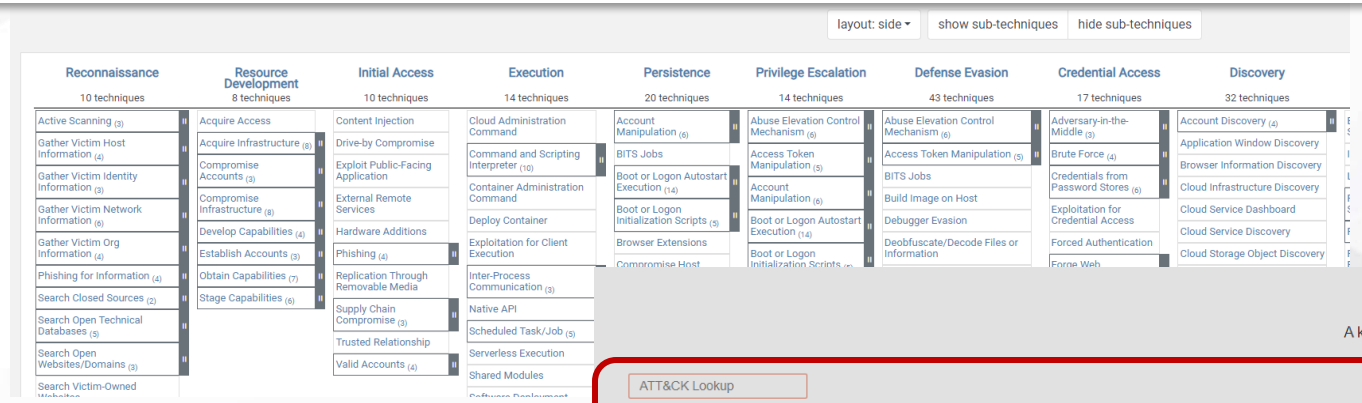
# Wo findet man Systemhärtung in der Regulatorik?

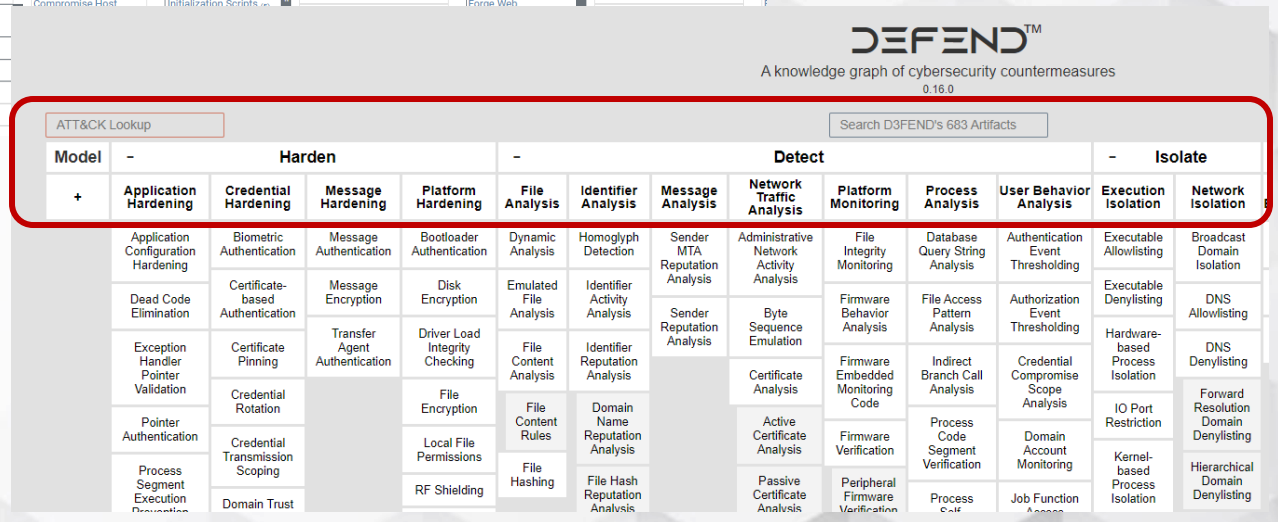
# Systemhärtung – Security-Frameworks und Regulatorik

Das MITRE D3FEND Framework setzt "Hardening" (secure configuration/Systemhärtung) als Basismaßnahme voraus.

MITRE ATTACK

MITRE DEFEND




**Was macht mehr Sinn**? Erst mit dem Auto zur HU fahren oder doch lieber vorher die Dinge reparieren, die dort geprüft werden?

# Systemhärtung – Security-Frameworks und Regulatorik

Das Center for Internet Security (CIS) definiert in seinen "CIS Controls" 18 Maßnahmen, sortiert nach Priorität. Systemhärtung findet sich dort auf Platz 4 – das hat seinen Grund. Aktuell "gehypte" Maßnahmen sind (nicht nur bei CIS) deutlich weiter hinten angesiedelt.

## CIS Critical Security Controls


**Control 1: Inventory and Control of Enterprise Assets**
Why is this Control critical?
Procedures and tools
Safeguards

**Control 2: Inventory and Control of Software Assets**
Why is this Control critical?
Procedures and tools
Safeguards

**Control 3: Data Protection**
Why is this Control critical?
Procedures and tools
Safeguards

**Control 4: Secure Configuration of Enterprise Assets and Software**
Why is this Control critical?
Procedures and tools
Safeguards

**Control 5: Account Management** 32
Why is this Control critical? 32
Procedures and tools 32
Safeguards 33

**Control 6: Access Control Management** 35
Why is this Control critical? 35
Procedures and tools 36
Safeguards 37

**Control 7: Continuous Vulnerability Management** 39
Why is this Control critical? 39
Procedures and tools 40
Safeguards 41

**Control 8: Audit Log Management** 43
Why is this Control critical? 43
Procedures and tools 43
Safeguards 44

**Control 14: Security Awareness and Skills Training**
Why is this Control critical?
Procedures and tools
Safeguards

**Control 15: Service Provider Management**
Why is this Control critical?
Procedures and tools
Safeguards

**Control 16: Application Software Security**
Why is this Control critical?
Procedures and tools
Safeguards

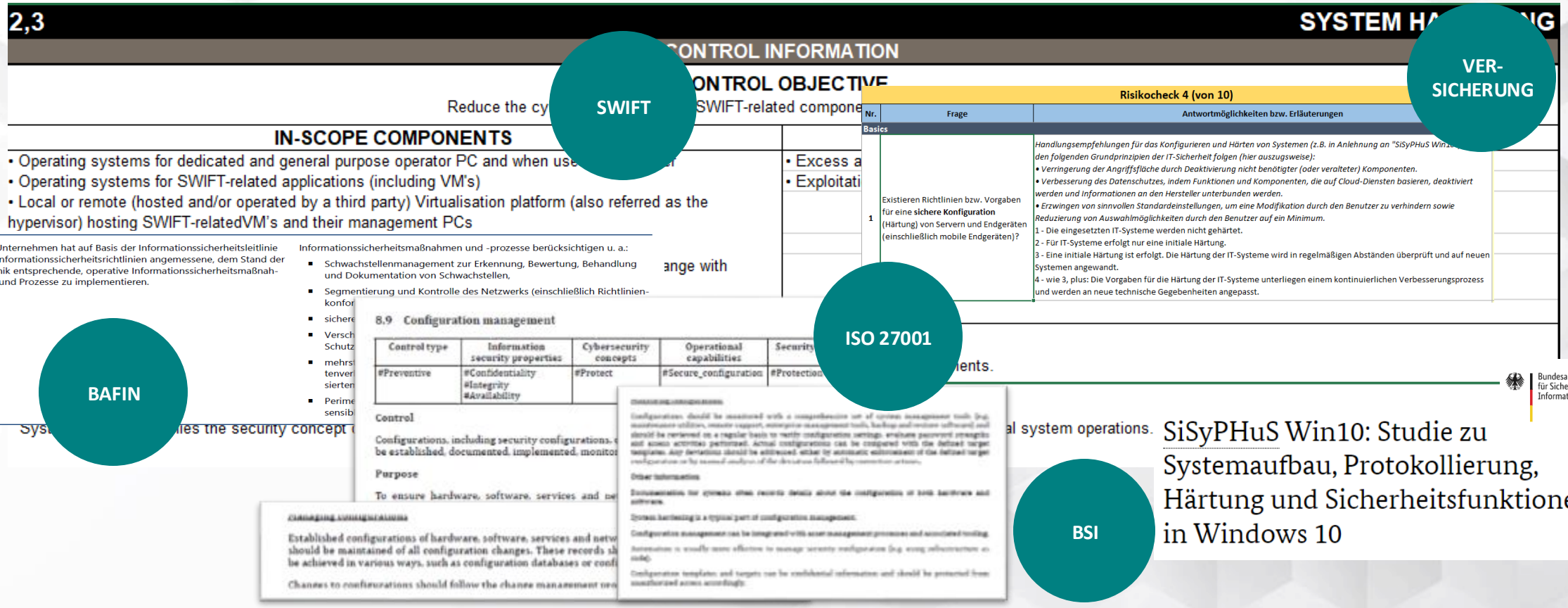
**Control 17: Incident Response Management**
Why is this Control critical?
Procedures and tools
Safeguards

**Control 18: Penetration Testing**
Why is this Control critical?
Procedures and tools
Safeguards


**Was macht mehr Sinn**? Erst mit dem Auto zur HU fahren oder doch lieber vorher die Dinge reparieren, die dort geprüft werden?

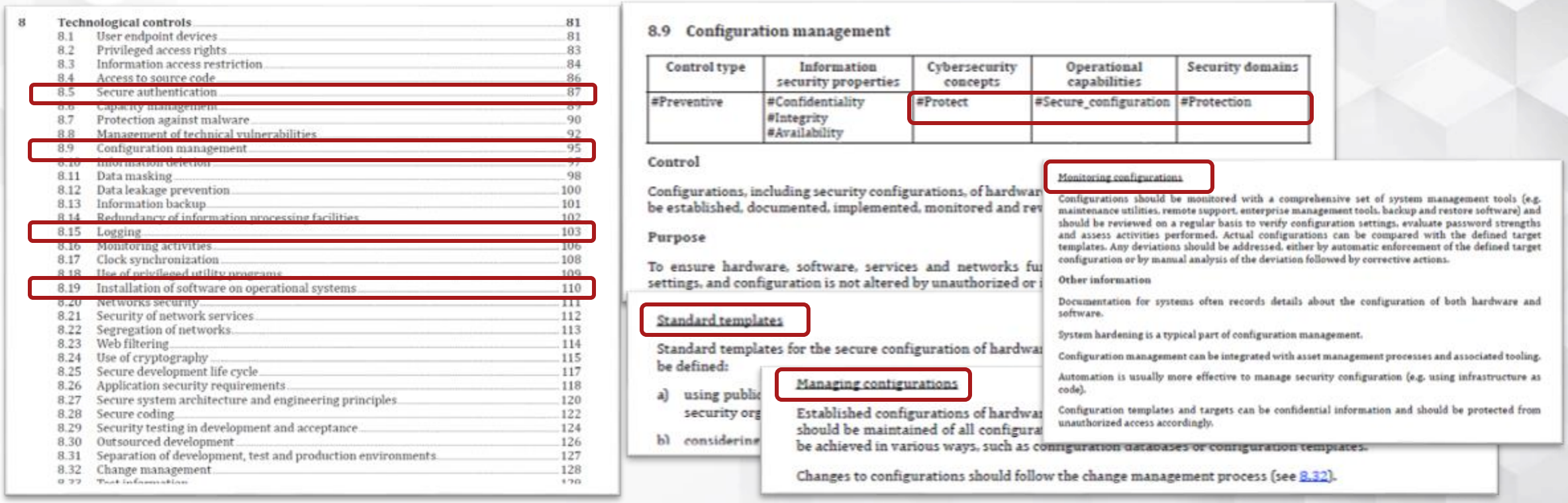
# Systemhärtung – Security-Frameworks und Regulatorik

„Secure Configuration“ / Hardening wird inzwischen in allen relevanten Security-Frameworks, Branchen-Regularien als auch Fragebögen von (Cyber-) Versicherungen gefordert.



# Systemhärtung – Security-Frameworks und Regulatorik

**In aktuellen ISO-Zertifizierungen ist Systemhärtung (konkret “secure configuration”) zertifizierungsrelevant.**
**Die Norm im Stand von 2022 (deutsche Norm 27001:2024) schreibt das Control vor!**



8 Technological controls 81
8.1 User endpoint devices 81
8.2 Privileged access rights 83
8.3 Information access restriction 84
8.4 Access to source code 86
8.5 Secure authentication 87
8.6 Capacity management 89
8.7 Protection against malware 90
8.8 Management of technical vulnerabilities 92
8.9 Configuration management 95
8.10 Information deletion 97
8.11 Data masking 98
8.12 Data leakage prevention 100
8.13 Information backup 101
8.14 Redundancy of information processing facilities 102
8.15 Logging 103
8.16 Monitoring activities 106
8.17 Clock synchronization 108
8.18 Use of privileged utility programs 109
8.19 Installation of software on operational systems 110
8.20 Networks security 111
8.21 Security of network services 112
8.22 Segregation of networks 113
8.23 Web filtering 114
8.24 Use of cryptography 115
8.25 Secure development life cycle 117
8.26 Application security requirements 118
8.27 Secure system architecture and engineering principles 120
8.28 Secure coding 122
8.29 Security testing in development and acceptance 124
8.30 Outsourced development 126
8.31 Separation of development, test and production environments 127
8.32 Change management 128
8.33 Test information 129

8.9 Configuration management

| Control type | Information security properties | Cybersecurity concepts | Operational capabilities | Security domains |
|---|---|---|---|---|
| #Preventive | #Confidentiality<br>#Integrity<br>#Availability | #Protect | #Secure_configuration | #Protection |

Control

Configurations, including security configurations, of hardwar
be established, documented, implemented, monitored and rev

Purpose

To ensure hardware, software, services and networks fu
settings, and configuration is not altered by unauthorized or i

Standard templates

Standard templates for the secure configuration of hardwa
be defined:

a) using publi
security org

b) considerin

Managing configurations

Established configurations of hardwa
should be maintained of all configura
be achieved in various ways, such as configuration databases or configuration templates.

Changes to configurations should follow the change management process (see 8.32).

Monitoring configurations

Configurations should be monitored with a comprehensive set of system management tools (e.g. maintenance utilities, remote support, enterprise management tools, backup and restore software) and should be reviewed on a regular basis to verify configuration settings, evaluate password strengths and assess activities performed. Actual configurations can be compared with the defined target templates. Any deviations should be addressed, either by automatic enforcement of the defined target configuration or by manual analysis of the deviation followed by corrective actions.

Other information

Documentation for systems often records details about the configuration of both hardware and software.

System hardening is a typical part of configuration management.

Configuration management can be integrated with asset management processes and associated tooling.

Automation is usually more effective to manage security configuration (e.g. using infrastructure as code).

Configuration templates and targets can be confidential information and should be protected from unauthorized access accordingly.

# Systemhärtung – Security-Frameworks und Regulatorik

**In der kommenden (teilweise bereits geltenden!) NIS2 EU-Verordnung wird es sehr konkret.**

## 6.3 CONFIGURATION MANAGEMENT

6.3.1. The relevant entities shall take the appropriate measures to establish, document, implement and monitor configurations, including security configurations of hardware, software, services and networks.

**GUIDANCE**

- Establish documented processes based on best practices and information security standards ([52])
- Maintain and document detailed configuration settings for the following operating procedures ( exhaustive list):
- Employ automated mechanisms to centrally manage, apply and verify configuration settings for so hardware, including mobile devices and the entity's connected vehicles.
  - Where appropriate, implement a configuration management database to catalogue and classify all configuration items (CIs), including their security attributes (e.g. patch level, firewall rules and encryption status)
- Ensure that all network, software and system configurations adhere to established security and operational standards for functions, ports, protocols and services.
- Monitor and control changes to the configuration settings in accordance with the entity's policy on the security of network and information systems and topic-specific policies and procedures.

NIS2

6.3.2. For the purpose of point 6.3.1., the relevant entities shall:

(a) lay down and ensure security in configurations for their hardware, software, services and networks;

(b) lay down and implement processes and tools to enforce the laid down secure configurations for hardware, software, services and networks, for newly installed systems as well as for systems in operation over their lifetime.

**GUIDANCE**

- Consider hardening guides/best practices and general cybersecurity principles (e.g. least functionality and least privilege) as a basis for deriving the defined security configurations.
- Establish, document and maintain configuration settings respecting the access control policy.
- Where applicable, test the configuration before implementation.

6.3.3. The relevant entities shall review and, where appropriate, update configurations at planned intervals or when significant incidents or significant changes to operations or risks occur.

**GUIDANCE**

- Review and, where appropriate update ([53]) configurations at least monthly to ensure that patches have been applied, that the backup has been executed according to the plan and that monitoring is in place to identify and alert to fatal server/device/disk errors without delay.
- Regularly produce, keep and review change logs regarding the security configuration of information systems.
- Review and update the configurations after major changes (e.g. software updates) and past incidents.
- Where feasible, obtain baseline configuration files for key systems and devices to compare against current configurations.

ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf

NIS 2, ISO 27001 und Systemhärtung: Ein Dreiklang, an den immer mehr Unternehmen denken müssen - FB Pro GmbH

# Systemhärtung – Regulatorik

„Secure Configuration“ / Hardening wird inzwischen in allen relevanten Security-Frameworks, Branchen-Regularien als auch Fragebögen von (Cyber-) Versicherungen gefordert.

| | | |
|---|---|---|
| 25. | **Umgang mit Schwachstellen, Störungen und Fehlern – System-Härtung**<br>Systemkomponenten, welche für die Erbringung der kritischen Dienstleistung verwendet werden, sind gemäß allgemein etablierter und akzeptierter Industriestandards gehärtet. Die herangezogenen Härtungsanleitungen werden ebenso wie der Umsetzungsstatus dokumentiert. | RB-22 |

KRITIS

Konkretisierung der Anforderungen an die gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen (bund.de)

## DORA-Beispiel 2: Article 11 RTS RMF – Data and System Security

Dieser Bereich ist besonders spannend, da hier nicht nur auf die einmalige Anwendung, sondern auch auf die regelmäßige Kontrolle von führenden Standards hingewiesen wird. Im Wortlaut heißt es:

> *“The data and ICT system security procedure referred to in paragraph 1 shall include all of the following elements related to data and ICT system security, in accordance with the classification performed pursuant to Article 8(1) of Regulation (EU) 2022/2554:*
>
> *(a) the access restrictions, in line with Article 21, supporting the protection requirements for each level of classification;*
> *(b) identification of secure configuration baseline for ICT assets that will minimise their exposure to cyber threats and measures to verify regularly that these baselines are those that are effectively deployed. The secure configuration baseline shall take into account leading practices and appropriate techniques referred to in standards (..)”*

DORA

DORA: Was hat die EU-Verordnung mit Systemhärtung zu tun? [Update] - FB Pro GmbH (fb-pro.com)

# Systemhärtung – Security-Frameworks und Regulatorik

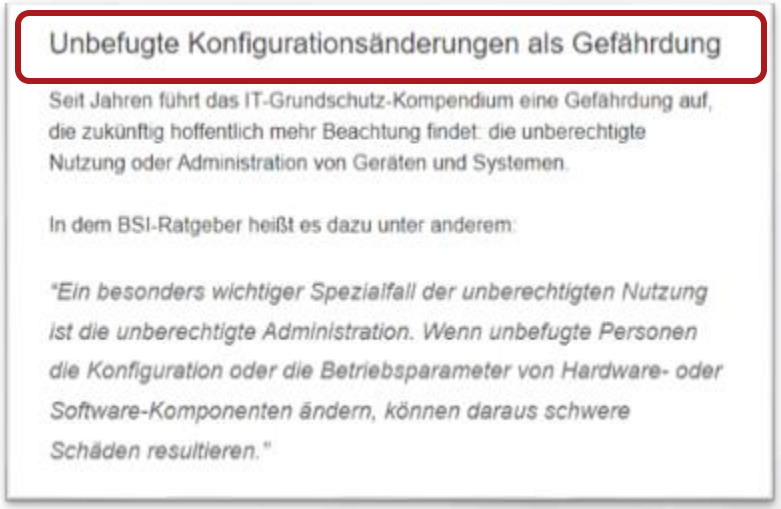
**Für das Bundesamt für Sicherheit in der Informationstechnik ist Systemhärtung die Antwort auf die Gefährdung "Unbefugte Konfigurationsänderung" und damit eine sogenannte geschäftskritische Maßnahme.**

## Die essentielle Erkenntnis: Ohne Systemhärtung geht es nicht mehr

In der neuen Edition des BSI IT-Grundschutzes spielt Systemhärtung eine deutlich wichtigere Rolle als bisher. Das zeigt sich zum Beispiel in der Häufigkeit, wie oft die IT-Sicherheitsmaßnahme erwähnt wird: In der 2023er-Fassung werden 55 Mal die Begriffe "härten" oder "Härtung" (und Abwandlungen davon) verwendet. In der Edition 2018 kommen die Worte nur 27 Mal vor.

Die Erwähnung der Maßnahme hat sich also in den letzten Jahren mehr als verdoppelt und findet sich beinahe in jeder Disziplin wieder. Bevor wir auf die Details des neuesten IT-Grundschutz-Kompendiums eingehen, hier eine Zusammenfassung:

- Härtung gilt als geschäftskritische Maßnahme
- Das Kompendium empfiehlt Härtung in verschiedenen Bereichen und Systemen, zum Beispiel bei:
  - Terminal-Servern
  - Virtualisierungsinfrastrukturen
  - Virtuelle Desktops (VDI)
  - Standard Workstations (Laptops, Notebooks etc.)
  - Datenbank-Management-Systeme
  - Administrations-Servern (Privileged Admin Workstations)
- Härtung wird ebenfalls als dringende Maßnahme nach einem APT-Angriff (Advanced Persistent Thread) empfohlen.
- Um Gefährdungen aus dem Gefährdungskatalog zu mitigieren, ist die Integritätsüberwachung der System-Konfiguration eine effektive Maßnahme



## Unbefugte Konfigurationsänderungen als Gefährdung

Seit Jahren führt das IT-Grundschutz-Kompendium eine Gefährdung auf, die zukünftig hoffentlich mehr Beachtung findet: die unberechtigte Nutzung oder Administration von Geräten und Systemen.

In dem BSI-Ratgeber heißt es dazu unter anderem:

*"Ein besonders wichtiger Spezialfall der unberechtigten Nutzung ist die unberechtigte Administration. Wenn unbefugte Personen die Konfiguration oder die Betriebsparameter von Hardware- oder Software-Komponenten ändern, können daraus schwere Schäden resultieren."*

## Härtung als geschäftskritische Maßnahme

Was als erstes ins Auge fällt: Relativ am Anfang (Kapitel 2.2) verweist das BSI darauf, dass verschiedene Faktoren eine eingeschränkte Verfügbarkeit auslösen können. Neben den "alten Bekannten", zu denen beispielsweise fehlende Redundanzen gehören, führt das Bundesamt in seinem Kompendium inzwischen auch das Thema Härtung als geschäftskritische Basismaßnahme an.

So heißt es:

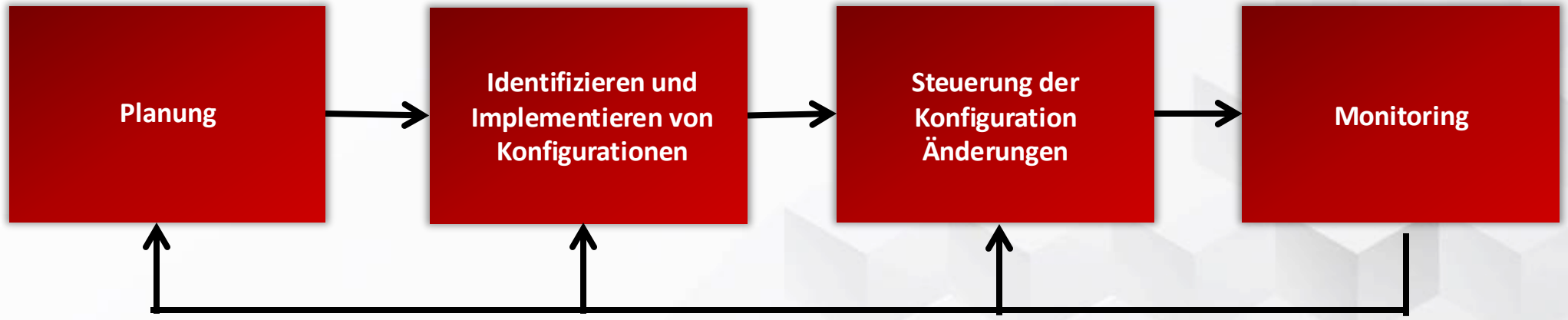
*"Sind die Betriebsmittel unzureichend redundant ausgelegt, nur eingeschränkt gehärtet oder überlastet, kann hierdurch die Verfügbarkeit eingeschränkt sein."*

Conclusio: Eine auf Standards basierende Systemhärtung wirkt sich mittel- bis langfristig positiv auf die Verfügbarkeit aus.

# Systemhärtung – prozessintegriert

**NIST definiert es als:**
"Die Verwaltung und Kontrolle der Konfigurationen eines Informationssystems, um die Sicherheit zu gewährleisten und das Risikomanagement zu erleichtern." Guide for Security-Focused Configuration Management of Information Systems | NIST

**Vier Phasen sind relevant:**




**Phasen des sicherheitsorientierten Konfigurationsmanagements**

TEAL
ALWAYS CHALLENGING IT

FB PRO GMBH
System Hardening & Secure Configuration

# Konkrete Vorgaben im Rahmen von Richtlinien

Vorgaben aus der Governance-Einheit helfen ungemein.

# Konkrete Vorgaben für die IT helfen bei der Umsetzung

Die Anforderungen aus der Regulatorik an die technische Maßnahme „Systemhärtung“ sind klar definiert.

Sie basieren auf **industrieerprobten Empfehlungen** (NIST, CIS, DISA, ISO 27001:2022, etc.)

Die **Effektivität von Härtungskonfigurationen** ist zu prüfen

Die **tatsächliche Anwendung** ist zu überwachen (“Regelmäßige Maßnahmen”)

**Abweichungen** (“misconfigurations”) sind zu **erkennen** (Prozess)

**Abweichungen** (“misconfigurations”) sind zu **behandeln** (Prozess)

Es ist eine **umfassende Dokumentation** zu erstellen (Nachweispflicht)

# Konkrete Vorgaben für die IT helfen bei der Umsetzung

Die Realität ist aber eher…

**… auf Anforderungsebene**

Wir brauchen „Systemhärtung“.

ODER

„Wendet die CIS Benchmarks an!“

**… auf Umsetzungsebene**

Wie sollen wir das jetzt kombinieren? Umsetzen? Monitoren? Kontrollieren? Dokumentieren?

**Praxistipp**

In dieser Situation mit den Stakeholdern (ISO, CISO, etc.) über die Konkretisierung der Anforderungen sprechen. Auch eine 50% Compliance (vgl. “rapid hardening”-Ansatz”) zu einem Standard hilft in der Realität mehr als ideologische / dogmatische Diskussionen. Beispiele folgen…

# Konkrete Vorgaben für die IT helfen bei der Umsetzung

**Im besten Fall macht der/die Informationssicherheitsbeauftragte, die Governance-Organisation oder eine adäquate Einheit entsprechende konkrete Vorgaben (bspw. im Rahmen einer "Richtlinie"):**

- Basis sind CIS Benchmark in der aktuellen Version für Windows Server 2022 (oder anderes Betriebssystem)
  - CIS L1 ist zwingend zu nutzen für Systeme mit "normalem" Schutzbedarf
  - CIS L2 in Kombination mit CIS L1 für Systeme mit "hohem" Schutzbedarf [kritische Systeme]

- Für Systeme mit "hohem Schutzbedarf" sind zusätzlich die **MS Security Baseline** anzuwenden – bei Konflikten ist die "sichere (härtere)" Einstellung zu bevorzugen

- Ergänzend ist für alle Systeme der **BSI Mindeststandard zur Verwendung von Transport Layer Security** zu verwenden

- **Browser** sind auf Basis von Herstellervorgaben, der Microsoft Baselines (Edge) und / oder der CIS Empfehlungen zu konfigurieren

# Konkrete Vorgaben für die IT helfen bei der Umsetzung

- Im ersten Schritt sind mindestens 50% CIS Compliance [CIS L1 Compliance] zu erreichen. Sukzessive Verbesserung ist Bestandteil des ISMS und entsprechend nachzuweisen; in den Folgejahren ist das Compliance-Niveau auf über 80% anzuheben

- Die CIS-Empfehlungen sind gegen die Empfehlungen des “Bundesamts für Sicherheit in der Informationstechnik” zu prüfen; bei Konflikten wird eine Risikobewertung zusammen mit der Informationssicherheit durchgeführt

- Notwendige Abweichungen / Ausnahmen von verwendeten Industriestandards sind begründet zu dokumentieren, die Freigabe erteilt die Abteilung / das Referat Informationssicherheit [der ISO/CISO etc.]

- Die Sicherheitseinstellungen dürfen nur im Rahmen von technischen Root-Cause-Analysen mit erfasstem Ticket [Incident/Event/…] angepasst / editiert / verändert werden und sind nach Abschluss der Analyse wieder auf den geforderten SOLL-Zustand zu konfigurieren

# Konkrete Vorgaben für die IT helfen bei der Umsetzung

- Die Einhaltung ist einmal pro Tag (pro Woche/stündlich) automatisiert zu kontrollieren; es erfolgt eine Prozessintegration in vorhandene Prozesse:
  - Jedes neue System wird nur gehärtet ausgeliefert (Provisionierung / Bereitstellung / **ServiceReq.Ful.**)
  - Härtungsänderung / Konfigurationsänderungen sind in der CMDB hinterlegt (**ConfigMgmt**.)
  - Abweichungen sind zu behandeln und an das Betriebs-Team oder das IT-Sec-Team (Ticketing, Mail, etc.) zu eskalieren (Ticket- / Event - / **Incident-Management**)

- Jedes neu installierte System ist (im Gegensatz zu Bestandssystemen) umfassend sicher zu konfigurieren

- Aktuelle Dokumentation ist vorzuhalten und auf Nachfrage innerhalb von zwei Arbeitstagen (zwei Wochen / monatlich) zu liefern

  - SOLL-Zustand
  - Aktueller Zustand der Implementierung
  - „Ad hoc reporting“ für einzelne Systeme

- Änderungen an den Standards sind anlassbezogen mindestens einmal pro Jahr zu prüfen

TEAL
ALWAYS CHALLENGING IT

15:00

FB PRO GMBH
System Hardening & Data Protection

# PAUSE (15 Minuten)

Hier geht‘s zum Quiz ›

TEAL
ALWAYS CHALLENGING IT

FB PRO GMBH
System Hardening & Data Protection

# Systemhärtung

## Die Praxis

# Anforderungen aus der Regulatorik

Schauen wir uns die Anforderungen nochmal an.

Sie basieren auf **industrieerprobten Empfehlungen** (NIST, CIS, DISA, ISO 27001:2022, etc.)

Die **Effektivität von Härtungskonfigurationen** ist zu prüfen

Die **tatsächliche Anwendung** ist zu überwachen (“Regelmäßige Maßnahmen”)

**Abweichungen** (“misconfigurations”) sind zu **erkennen** (Prozess)

**Abweichungen** (“misconfigurations”) sind zu **behandeln** (Prozess)

Es ist eine **umfassende Dokumentation** zu erstellen (Nachweispflicht)

# Härtung in der Praxis

Schauen wir uns die konkrete Umsetzung mal genauer an.

| | | | | |
|---|---|---|---|---|
| **Härtungsempfehlungen** auswählen | **Härtungskonfigurationen konzeptionieren** (für verschiedene OS, Rollen, Client/Server, etc) | **Duplikate** zwischen Standards **erkennen** und bereinigen | **Konflikte zwischen Standards erkennen** und bereinigen | **Konflikte mit eigener Infrastruktur** erkennen und entscheiden (GPO, Image, etc.) |
| **Härtung (meist) manuell konfigurieren** | Mit **Ausnahmen** für bestimmte Rollen / Apps umgehen (technisch/Doku) | **Dokumentation (SOLL/IST/Ausnahmen) manuell erstellen** (meist Excel) für alle Rollen | **Härtungen monitoren** | **Abweichungen erkennen** und aktiv informieren (Prozess) |
| **Härtungskonfigurationen versioniert aktualisieren** | **Härtung und Doku aktuell halten** | **„Non domain“-integrierte Systeme härten** | **Linux-Systeme härten** | **…** |

# Systemhärtung ist nicht nur Scripting und Technologie

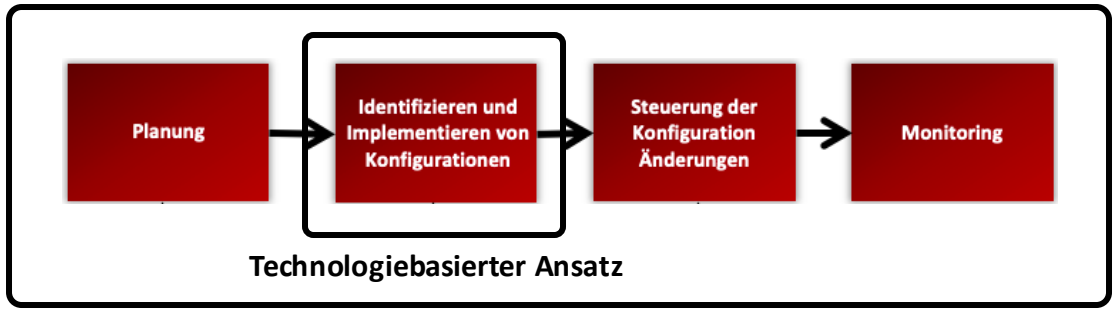

## Es gibt verschiedene Ansätze zum "Härten" von Systemen

In der Praxis gibt es mehrere technologische Ansätze:

- Mehrere Magazine liefern “Security Tools" | Wer will diese im professionellen Bereich einsetzen?
- Github-Repositories mit Tausenden von Codezeilen | Wer will das Risiko eingehen, sie in einem KMU-Unternehmen einzusetzen?
- Beratungsanbieter liefern "Härtung" auf Zeit- und Materialbasis | Was passiert, wenn der Anbieter geht, aber etwas nicht wie erwartet funktioniert?

## Ihre Vorteile eines toolbasierten Ansatzes

- Automatisierte Optimierung Ihrer Systemkonfiguration
- Kontinuierliche Überwachung Ihrer Sicherheit
- Umfassende und aktuelle Systemheilungspakete
- Reduzierte Betriebskosten durch Auto-Optimierung
- Professioneller Betrieb über "Managed Services"




**Suchen Sie einfach nach "hardening tools oder „Systemhärtung" in Ihrer bevorzugten Suchmaschine**



TEAL ALWAYS CHALLENGING IT
FB PRO GMBH System Hardening & Secure Configuration

TEAL
ALWAYS CHALLENGING IT

FB PRO GMBH
System Hardening & Secure Configuration

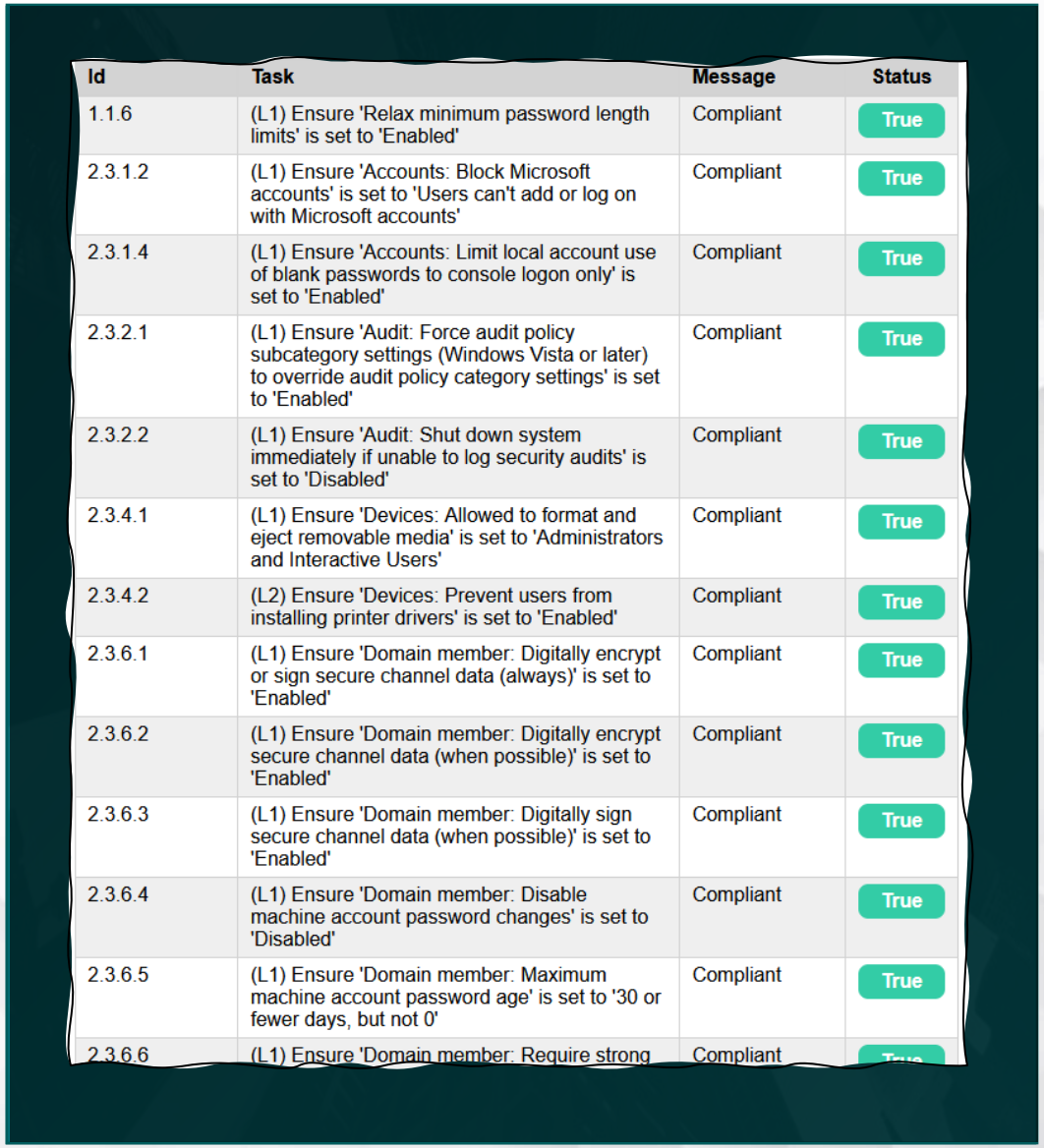
# Systemhärtung messbar machen mit dem open source Tool „AuditTAP“.

# Live-Präsentation – „Secure Configuration Assessment“

**Systemhärtung messbar machen**

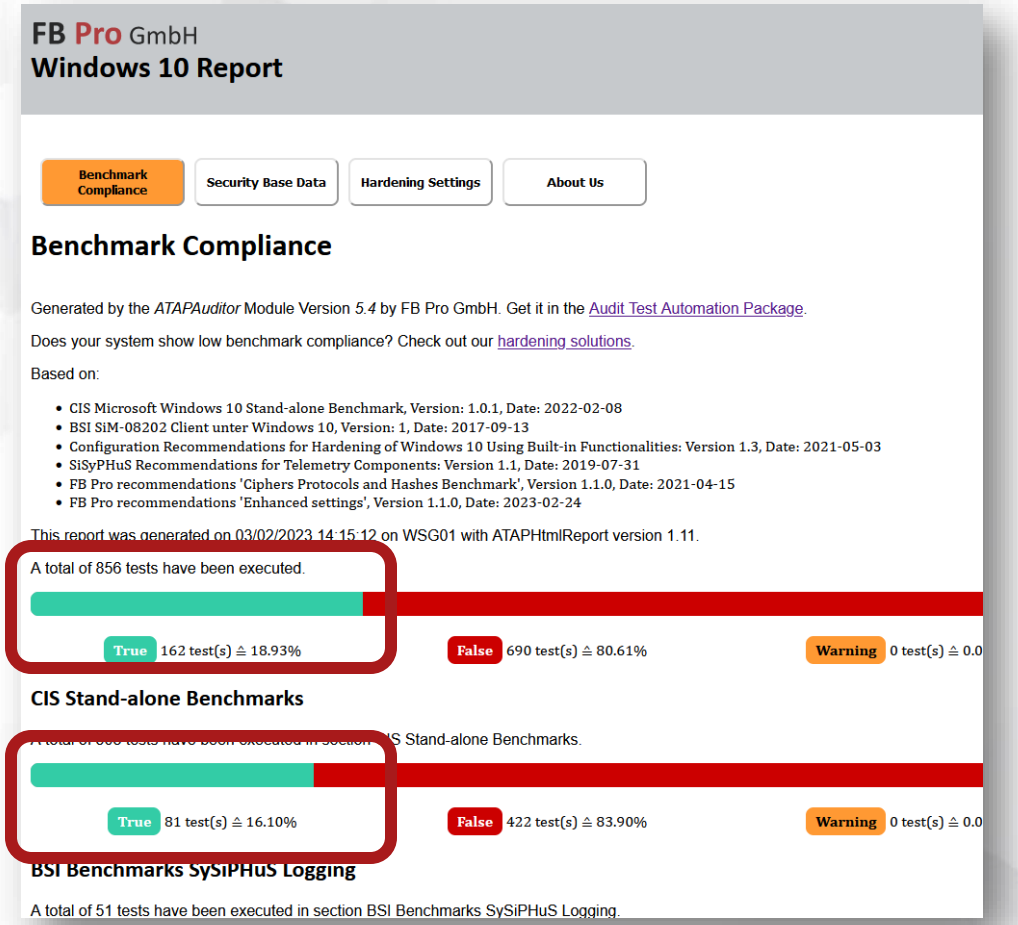
- Warum sind die XBOX-Dienste an?
- Warum kann jeder Drucker-Treiber installieren?
- Warum kann der DC drucken?
- Warum sind alte Protokolle (SMBv1, RC4, etc.) angeschaltet?
- Warum werden nur „Basisdinge“ protokolliert (Forensik?)
- Passworteinstellungen? Multifaktor-Authentisierung?
- Warum Bluetooth und Kamera auf einem Admin- / Jump-Server?
- Müssen Server vom Office-Rechner aus administriert werden?
- ….

LIVE-Präsentation



| Id | Task | Message | Status |
|---|---|---|---|
| 1.1.6 | (L1) Ensure 'Relax minimum password length limits' is set to 'Enabled' | Compliant | True |
| 2.3.1.2 | (L1) Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts' | Compliant | True |
| 2.3.1.4 | (L1) Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' | Compliant | True |
| 2.3.2.1 | (L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled' | Compliant | True |
| 2.3.2.2 | (L1) Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' | Compliant | True |
| 2.3.4.1 | (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators and Interactive Users' | Compliant | True |
| 2.3.4.2 | (L2) Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled' | Compliant | True |
| 2.3.6.1 | (L1) Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' | Compliant | True |
| 2.3.6.2 | (L1) Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled' | Compliant | True |
| 2.3.6.3 | (L1) Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled' | Compliant | True |
| 2.3.6.4 | (L1) Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled' | Compliant | True |
| 2.3.6.5 | (L1) Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0' | Compliant | True |
| 2.3.6.6 | (L1) Ensure 'Domain member: Require strong | Compliant | True |

# Vergleich „Standard“ – „Gehärtet“



FB Pro GmbH
Windows 10 Report

Benchmark Compliance | Security Base Data | Hardening Settings | About Us

## Benchmark Compliance

Generated by the *ATAPAuditor* Module Version *5.4* by FB Pro GmbH. Get it in the Audit Test Automation Package.

Does your system show low benchmark compliance? Check out our hardening solutions.

Based on:

- CIS Microsoft Windows 10 Stand-alone Benchmark, Version: 1.0.1, Date: 2022-02-08
- BSI SiM-08202 Client unter Windows 10, Version: 1, Date: 2017-09-13
- Configuration Recommendations for Hardening of Windows 10 Using Built-in Functionalities: Version 1.3, Date: 2021-05-03
- SiSyPHuS Recommendations for Telemetry Components: Version 1.1, Date: 2019-07-31
- FB Pro recommendations 'Ciphers Protocols and Hashes Benchmark', Version 1.1.0, Date: 2021-04-15
- FB Pro recommendations 'Enhanced settings', Version 1.1.0, Date: 2023-02-24

This report was generated on 03/02/2023 14:15:12 on WSG01 with ATAPHtmlReport version 1.11.

A total of 856 tests have been executed.

True 162 test(s) ≙ 18.93% | False 690 test(s) ≙ 80.61% | Warning 0 test(s) ≙ 0.0

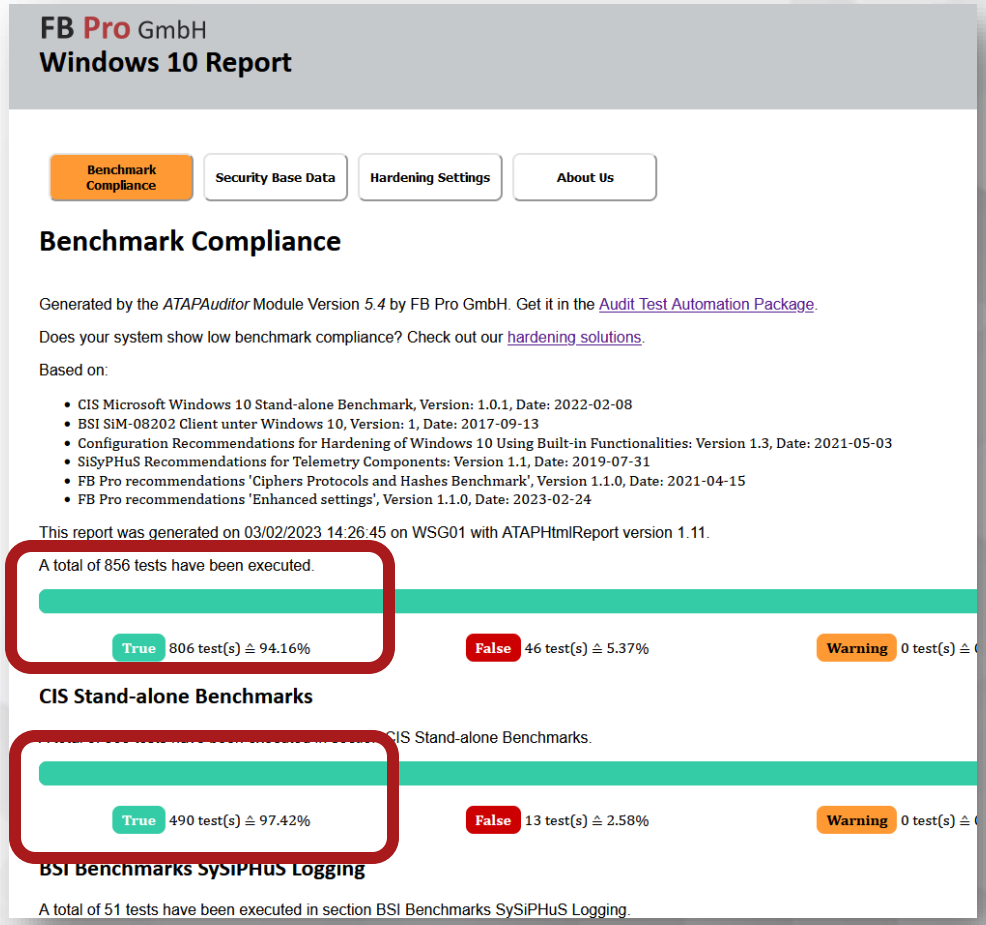
### CIS Stand-alone Benchmarks

S Stand-alone Benchmarks.

True 81 test(s) ≙ 16.10% | False 422 test(s) ≙ 83.90% | Warning 0 test(s) ≙ 0.0

### BSI Benchmarks SySIPHuS Logging

A total of 51 tests have been executed in section BSI Benchmarks SySiPHuS Logging.



FB Pro GmbH
Windows 10 Report

Benchmark Compliance | Security Base Data | Hardening Settings | About Us

## Benchmark Compliance

Generated by the *ATAPAuditor* Module Version *5.4* by FB Pro GmbH. Get it in the Audit Test Automation Package.

Does your system show low benchmark compliance? Check out our hardening solutions.

Based on:

- CIS Microsoft Windows 10 Stand-alone Benchmark, Version: 1.0.1, Date: 2022-02-08
- BSI SiM-08202 Client unter Windows 10, Version: 1, Date: 2017-09-13
- Configuration Recommendations for Hardening of Windows 10 Using Built-in Functionalities: Version 1.3, Date: 2021-05-03
- SiSyPHuS Recommendations for Telemetry Components: Version 1.1, Date: 2019-07-31
- FB Pro recommendations 'Ciphers Protocols and Hashes Benchmark', Version 1.1.0, Date: 2021-04-15
- FB Pro recommendations 'Enhanced settings', Version 1.1.0, Date: 2023-02-24

This report was generated on 03/02/2023 14:26:45 on WSG01 with ATAPHtmlReport version 1.11.

A total of 856 tests have been executed.

True 806 test(s) ≙ 94.16% | False 46 test(s) ≙ 5.37% | Warning 0 test(s) ≙

### CIS Stand-alone Benchmarks

CIS Stand-alone Benchmarks.

True 490 test(s) ≙ 97.42% | False 13 test(s) ≙ 2.58% | Warning 0 test(s) ≙

### BSI Benchmarks SySIPHuS Logging

A total of 51 tests have been executed in section BSI Benchmarks SySiPHuS Logging.

TEAL
ALWAYS CHALLENGING IT

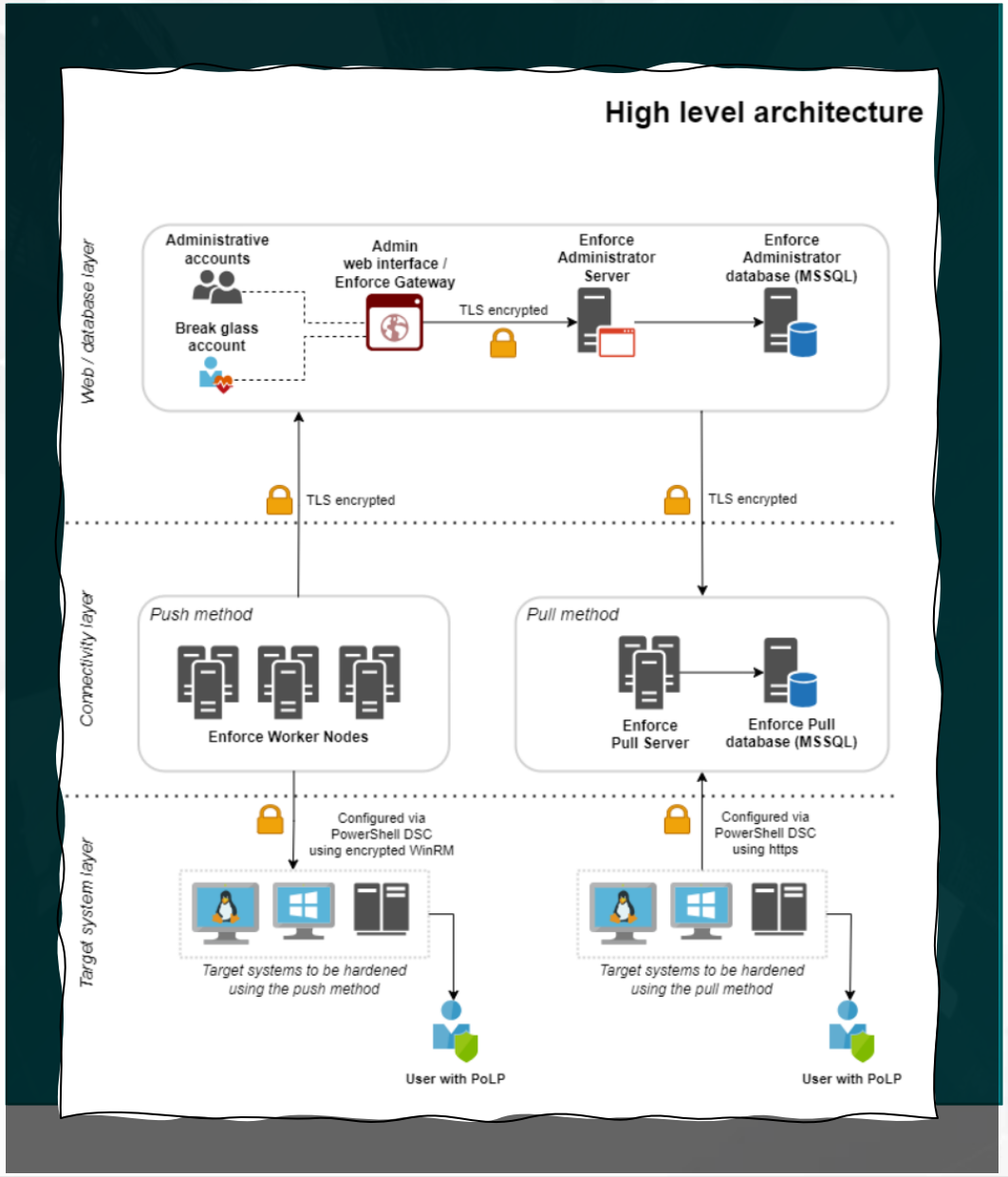
FB PRO GMBH
System Hardening & Secure Configuration

# Ihre regulatorischen Anforderungen im Umfeld Systemhärtung mit Enforce Administrator erfüllen

# Härtung in der Praxis

Wir erinnern uns…

- **Härtungsempfehlungen** auswählen
- **Härtungskonfigurationen konzeptionieren** (für verschiedene OS, Rollen, Client/Server, etc)
- **Duplikate** zwischen Standards **erkennen** und bereinigen
- **Konflikte zwischen Standards erkennen** und bereinigen
- **Konflikte mit eigener Infrastruktur** erkennen und entscheiden (GPO, Image, etc.)
- **Härtung (meist) manuell konfigurieren**
- Mit **Ausnahmen** für bestimmte Rollen / Apps umgehen (technisch/Doku)
- **Dokumentation (SOLL/IST/Ausnahmen) manuell erstellen** (meist Excel) für alle Rollen
- **Härtungen monitoren**
- **Abweichungen erkennen** und aktiv informieren (Prozess)
- **Härtungskonfigurationen versioniert aktualisieren**
- **Härtung und Doku aktuell halten**
- **„Non domain“-integrierte Systeme härten**
- **Linux-Systeme härten**
- **…**




# LIVE-Präsentation – Systemhärtung umsetzen

**Praxisfall 1:**
Eine auf Industrie-Standards basierende Härtungs-konfiguration mit rund 600 Einstellungen in wenigen Minuten zusammenbauen.

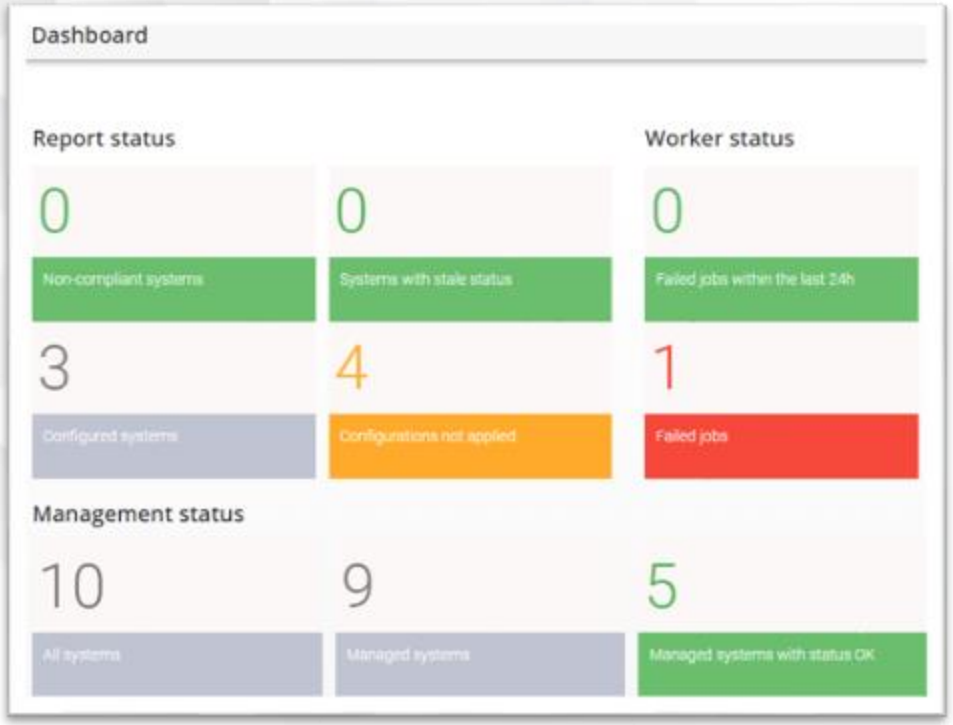
**Praxisfall 2:**
Dokumentation dieser Härtungskonfiguration mit einem Mausklick erzeugen.

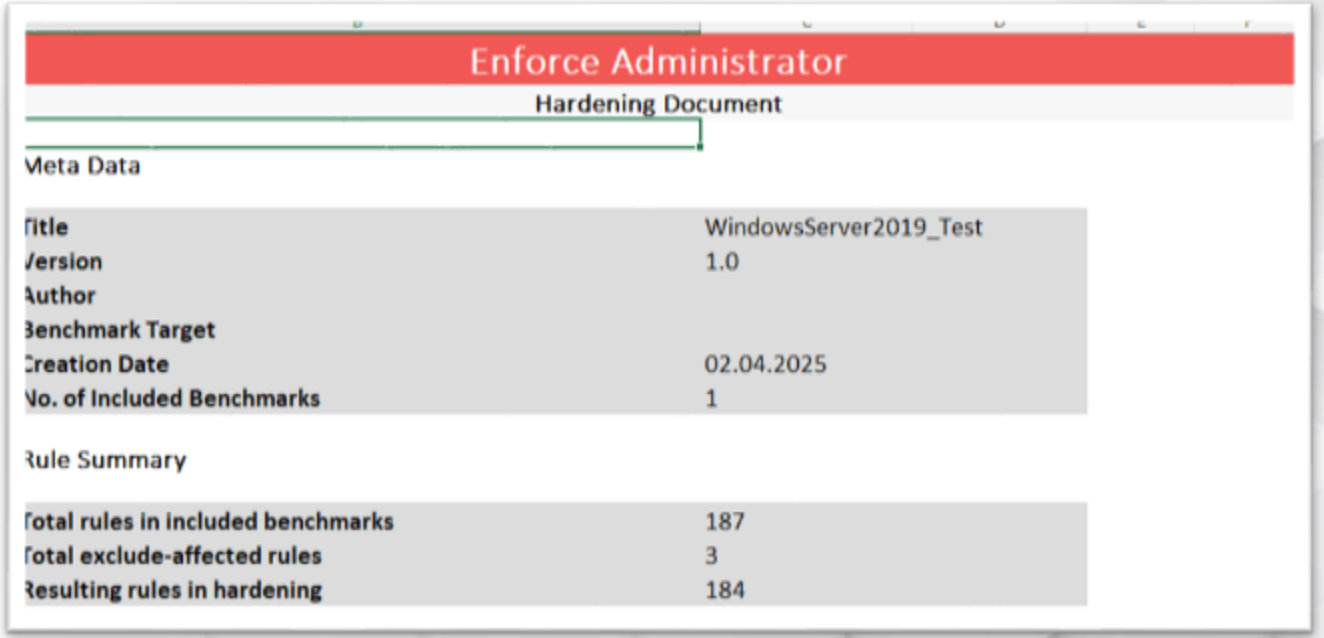
**Praxisfall 3:**
Die Härtungskonfiguration in einem Dashboard überwachen und Dokumentation des IST-Zustandes der Infrastruktur erstellen.

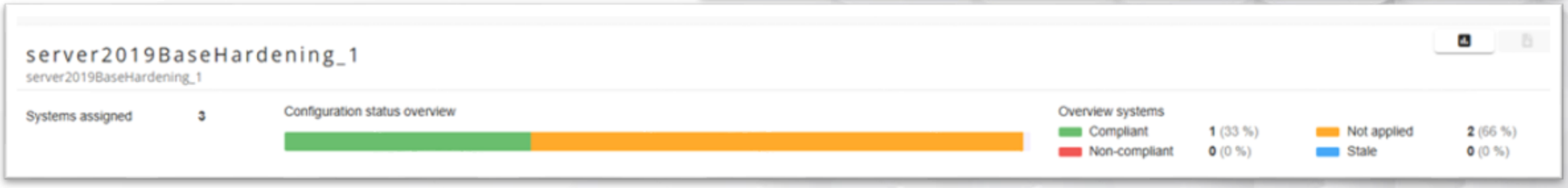
**Praxisfall 4:**
Im Fall einer Abweichung vom SOLL-Zustand / Anomalie eine aktive Push-Nachricht erhalten – **am Messestand**

**Praxisfall 5:**
IT-Systeme, die nicht compliant sind, den Zugriff auf Unternehmens-Ressourcen verbieten (über Azure Conditional Access Policies) - **am Messestand**

# LIVE-Präsentation – Systemhärtung umsetzen



TEAL
ALWAYS CHALLENGING IT

FB PRO GMBH
System Hardening & Secure Configuration

# Herangehensweisen im Bereich Windows Server hardening

## Rollout Modelle

# Nützliche Ansätze

**Option 1**

## layered hardening

Härtung als Teil eines Sicherheitsprojekts. Klassifizierung der Systeme als T0/T1/T2 und Beginn der Härtung von T0 so weit wie möglich. Die anderen Layer werden nach T0 durchgeführt.

**Option 2**

## rapid hardening

Führen Sie ein Basis-Hardening-Set ein, um schnell Ergebnisse zu erzielen. Erhöhen Sie anschließend iterativ die Sicherheitsstufe.

**Option 3**

## lifecycle hardening

Rollout-Härtungssatz während eines Lifecycle-Projekts (z. B. Rollout von Windows 11).

# Nützliche Ansätze

**Option 1**

## layered hardening

Härtung als Teil eines Sicherheitsprojekts. Klassifizierung der Systeme als T0/T1/T2 und Beginn der Härtung von T0 so weit wie möglich. Die anderen Schichten werden nach T0 durchgeführt.

| | |
|---|---|
| Security Level | ★★★★★ |
| Komplexität | ★★☆☆☆ |
| Aufwand | ★★☆☆☆ |
| Dauer | ★★★☆☆ |

**Option 2**

## rapid hardening

Führen Sie ein Basis-Hardening-Set ein, um schnell Ergebnisse zu erzielen. Erhöhen Sie anschließend iterativ die Sicherheitsstufe.

| | |
|---|---|
| Security Level | ★★☆☆☆ |
| Komplexität | ★★★★☆ |
| Aufwand | ★★★☆☆ |
| Dauer | ★★★★☆ |

**Option 3**

## lifecycle hardening

Rollout-Härtungssatz während eines Lifecycle-Projekts (z. B. Rollout von Windows 11).

| | |
|---|---|
| Security Level | ★★★★☆ |
| Komplexität | ★★★☆☆ |
| Aufwand | ★★★★★ |
| Dauer | ★★★☆☆ |



Sehr gut ★★★★★ Gut ★★★★☆ Befriedigend ★★★☆☆ Ausreichend ★★☆☆☆ Sehr gering ★☆☆☆☆

# Praxisbeispiel

## Härtungssätze

- Rapid Hardening ~190 Einstellungen (Basis: CIS L1)
- Secure Hardening ~530 Einstellungen (Basis: CIS L1 + L2, Cipher, Teal Recommendations)

## Planung

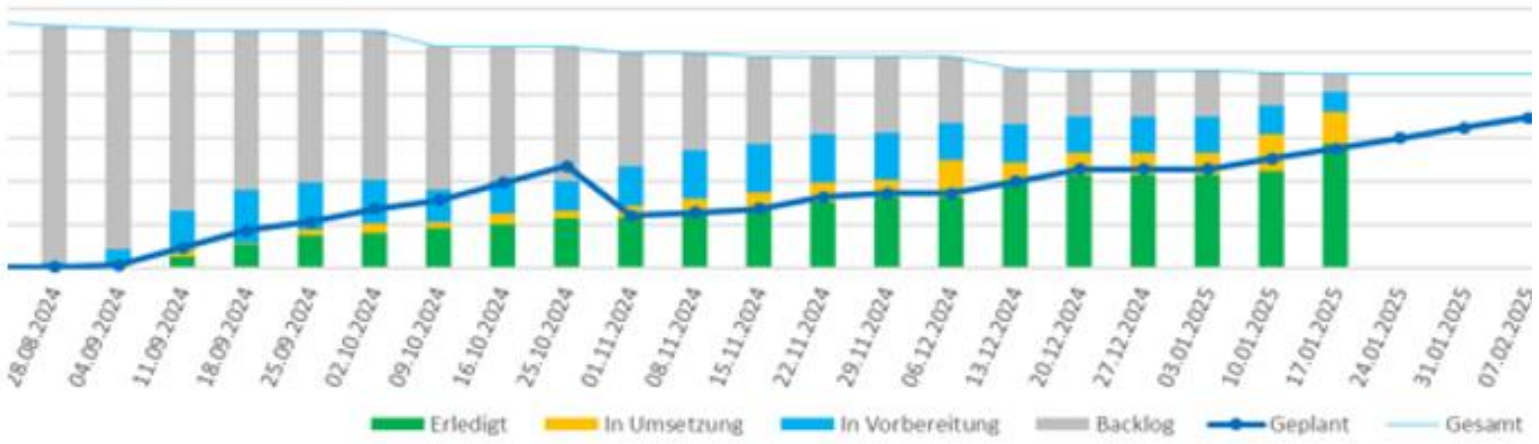
- Klassifizierung der IT-Systeme (Rapid/Secure) → 80/20 % empfohlen
- Identifizierung von Pilotsystemen
- Vorbereitung Kommunikation

## Rollout

- Rollout Pilotgruppe
- Rollout Rapid Wave 1 – X
- Rollout Secure Hardening

## Steuerung + Reporting

- Regelmäßiges Fortschrittstracking
- Vorgehen nach festen Rollen:
  - Planung
  - Vorbereitung + initial Rollout
  - Ggf. Troubleshooting parallel






TEAL ALWAYS CHALLENGING IT

FB PRO GMBH
System Hardening & Secure Configuration

TEAL
ALWAYS CHALLENGING IT

FB PRO GMBH
System Hardening & Secure Configuration

# Nachhaltigkeit und Wissensaufbau mit der TEAL Expertise Community

TEAL
ALWAYS CHALLENGING IT

FB PRO GMBH
System Hardening & Secure Configuration

Kontinuität

Angriffsfläche verkleinern

Wissensaufbau

# Wie schütze ich mich richtig?

technische Schulden beseitigen

# Expertise Community

**In einer Welt voller Tools…**
müssen IT-Abteilungen jeden Tag neue Herausforderungen meistern: mehr Systeme, mehr Sicherheitsanforderungen, mehr Abhängigkeiten und Regulatorik.
**Die Realität: zu viele Tools, zu viele Prozesse, zu wenig Klarheit und keine Zeit.**

**Wir bei TEAL wissen: Machen ist wie wollen, nur besser!**

Wir legen den Schwerpunkt auf Wissensvermittlung und tragen gemeinsam den Berg an technischen Schulden ab.

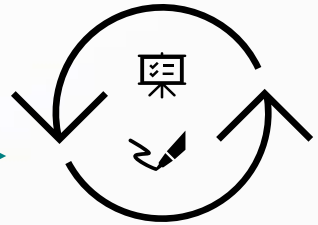
**Dein Unternehmen ist *nicht besser geschützt*, wenn du noch ein Tool kaufst, das du nur zu 20% nutzt!**
**Wir sorgen dafür, dass du aus dem, was du hast, den maximalen Schutz rausholst.**

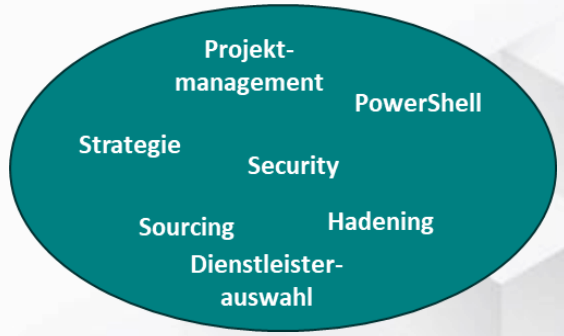
Mit unserer **Expertise Community** hast du jederzeit die richtigen Köpfe zur Hand. Ob Sicherheitsvorfall, Audit-Finding, Betriebsengpass oder strategische Planung, wir helfen dir, technische Schulden abzutragen, Lücken zu schließen und nachhaltiges Know-how aufzubauen.
**Der regelmäßige Austausch mit unseren Experten hilft dir in der Praxis!**

# Expertise Community

**Urgent Requests !!!**

**Regel-Jour-Fixes**






**Neue Anforderungen**

- Offene Anforderungen werden im Jour-Fix **vom Kunden** platziert
- Qualifizierung der Anforderung, um die **richtigen TEAL-Spezialisten** hinzuzuziehen

**Arbeitsgruppen**

- Arbeitsgruppe 1: PowerShell Script
- Arbeitsgruppe 2: Tiering
- Arbeitsgruppe „n“: Hardening

**Status- und Performance Report**

- Überblick über laufende Anforderungen und deren Status
- Richtungsweisungen von laufenden Maßnahmen
- Status-Tracking und Veränderung von Maßnahmen

DU

TEAL

# TEAL Expertise Community im Detail

**TEAL Expertise Community**

| Thema | Beispiele |
|---|---|
| **Scripting in PowerShell** | • Unterstützung bei der Anpassung und/oder Troubleshooting bestehender Scripts |
| **Hardening & Tiering** | • Unterstützung bei der Anwendung von Hardening Standards<br>• Support beim Troubleshooting, falls Apps auf gehärteten Systemen nicht funktionieren<br>• Tier-Zuordnung neuer Services im Unternehmen |
| **Architecture Reviews** | • Review und Beratung<br>• Überprüfung von Dokumenten nach Security- oder Tiering-Standards |
| **Bewertung dedizierter Schwachstellen** | • Analyse von Schwachstellen und möglichen Mitigationen<br>• Kritikalitätsbewertung von Schwachstellen für spezifische Services |
| **Rollenmodelle / RBAC / ORG Abbildung im AD** | • Aufnahme von Tätigkeiten und entsprechender Abbildung im AD<br>• „Good Practices“ für die Dokumentation des ORG-Modells im AD |
| **Knowledge Transfer Tiering** | • Maßnahmen zur Akzeptanzerhöhung von Sicherheitsstandards<br>• Team-Building Maßnahmen<br>• Regelmäßige Coaching-Termine für das Vertiefen von ESAE-Wissen in der Organisation |

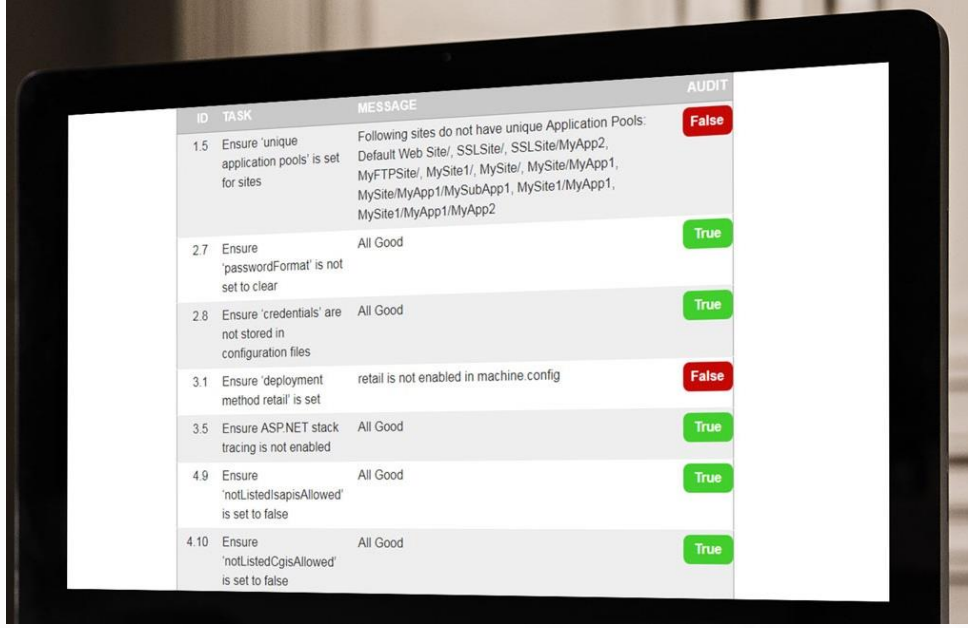
# TEAL Expertise Community im Detail

**TEAL Expertise Community**

| Thema | Beispiele |
|---|---|
| **Strategische Ausrichtungen** | • Kostenvergleiche, Ausschreibungen oder Dienstleisterauswahl<br>• Tool-Vergleiche (z.B. Cloud vs. On-Premises)<br>• Service-Portfolio-Analysen (z.B. Ablösbare Services durch Azure Nutzung) |
| **Betriebsmodell** | • Unterstützung bei Re-Organisation und Arbeitsoptimierung<br>• Strukturierung von Aufgaben (3rd -> 2nd -> 1st Level), um Freiräume zu schaffen<br>• Identifikation von "Zeit- und Aufwandsfressern" |
| **Infrastruktur Prozesse** | • Optimierung bestehender Betriebsprozesse<br>• Prozessaufnahme und Dokumentation |
| **Projektmanagement Basics / Templates** | • Coaching von Projektleitern<br>• Aufbau von QA-Prozessen bzw. Projektüberprüfungen<br>• Template Erstellung für PM-Artefakte |
| **Fortschrittskontrolle und Darstellung** | • Report-Strukturen entwickeln und pflegen / aktualisieren, um Fortschritte zu messen<br>• JF-Strukturen aufbauen und trainieren, um Fortschritte dauerhaft im Betrieb umzusetzen |

# Wir können konkret helfen, wenn…

- … Sie die **Angriffsfläche Ihrer IT-Systeme maximal reduzieren** wollen
- … wenn Ihre **Cyber-Versicherung** Sie nicht (weiter) versichern will oder sogar aktiv kündigt / die Kündigung androht (neuester Fall aus der Praxis)
- … Sie sich auf ein **externes Audit (Nachweispflicht)** vorbereiten wollen/müssen
- … Sie **regulatorische Anforderungen** erfüllen müssen
- … Sie Ihr **Haftungsrisiko minimieren**, bzw. reduzieren wollen
- … Sie umfänglich ein **Business Continuity Management planen**, Beispiel: NIS 2
- … **Schwachstellen nicht nur verwaltet, sondern wirklich verringert werden sollen**
- … Sie **nach einem Cyber-Angriff** noch laufende Systeme **maximal absichern** wollen



| ID | TASK | MESSAGE | AUDIT |
|---|---|---|---|
| 1.5 | Ensure 'unique application pools' is set for sites | Following sites do not have unique Application Pools: Default Web Site/, SSLSite/, SSLSite/MyApp2, MyFTPSite/, MySite1/, MySite/, MySite/MyApp1, MySite/MyApp1/MySubApp1, MySite1/MyApp1, MySite1/MyApp1/MyApp2 | False |
| 2.7 | Ensure 'passwordFormat' is not set to clear | All Good | True |
| 2.8 | Ensure 'credentials' are not stored in configuration files | All Good | True |
| 3.1 | Ensure 'deployment method retail' is set | retail is not enabled in machine.config | False |
| 3.5 | Ensure ASP.NET stack tracing is not enabled | All Good | True |
| 4.9 | Ensure 'notListedIsapisAllowed' is set to false | All Good | True |
| 4.10 | Ensure 'notListedCgisAllowed' is set to false | All Good | True |

https://github.com/fbprogmbh/Hardening-Audit-Tool-AuditTAP

# Siegerehrung & Q&A

## AuditTAP

https://github.com/fbprogmbh/Hardening-Audit-Tool-AuditTAP

## Kontaktdaten


**TEAL**

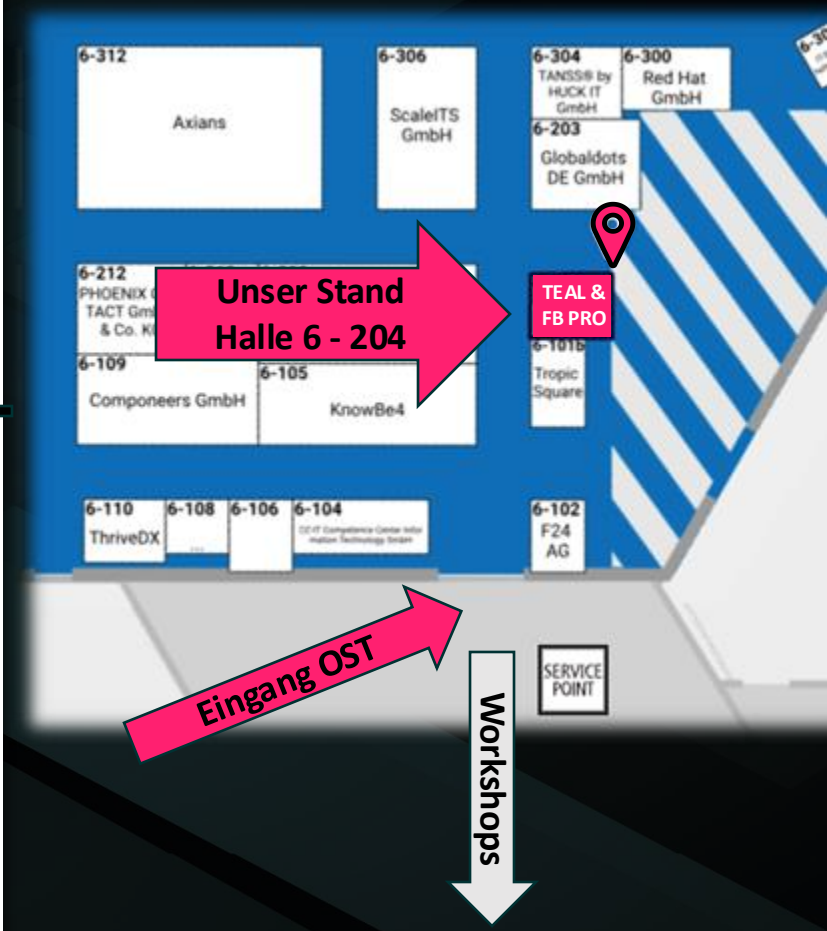
E-Mail: fabian.boehm@teal-consulting.de

Telefon: 0211/93675225

**FB PRO**

E-Mail: florian.broeder@fb-pro.com

Telefon: 06727/7559039


## iX heise academy Trainings, Informationen & Vortragsfolien

Wir freuen uns, dass Teal und FB Pro dieses Jahr mehrere **exklusive Workshops** über die iX heise academy zum Thema „Windows Server absichern und härten“ anbieten.

**Termine:**

- 19. + 20. November 2025 (09:00 – 17:00 Uhr)
- 01. + 02. Dezember 2025 (vor Ort in Frankfurt am Main)
- 12. + 13.01.2026 (09:00 – 17:00 Uhr)
- 24. + 25.02.2026 (09:00 – 17:00 Uhr)
- 21. + 22.04.2026 (09:00 – 17:00 Uhr)
- 10. + 11.06.2026 (09:00 – 17:00 Uhr)

https://www.teal-consulting.de/messeinfos/