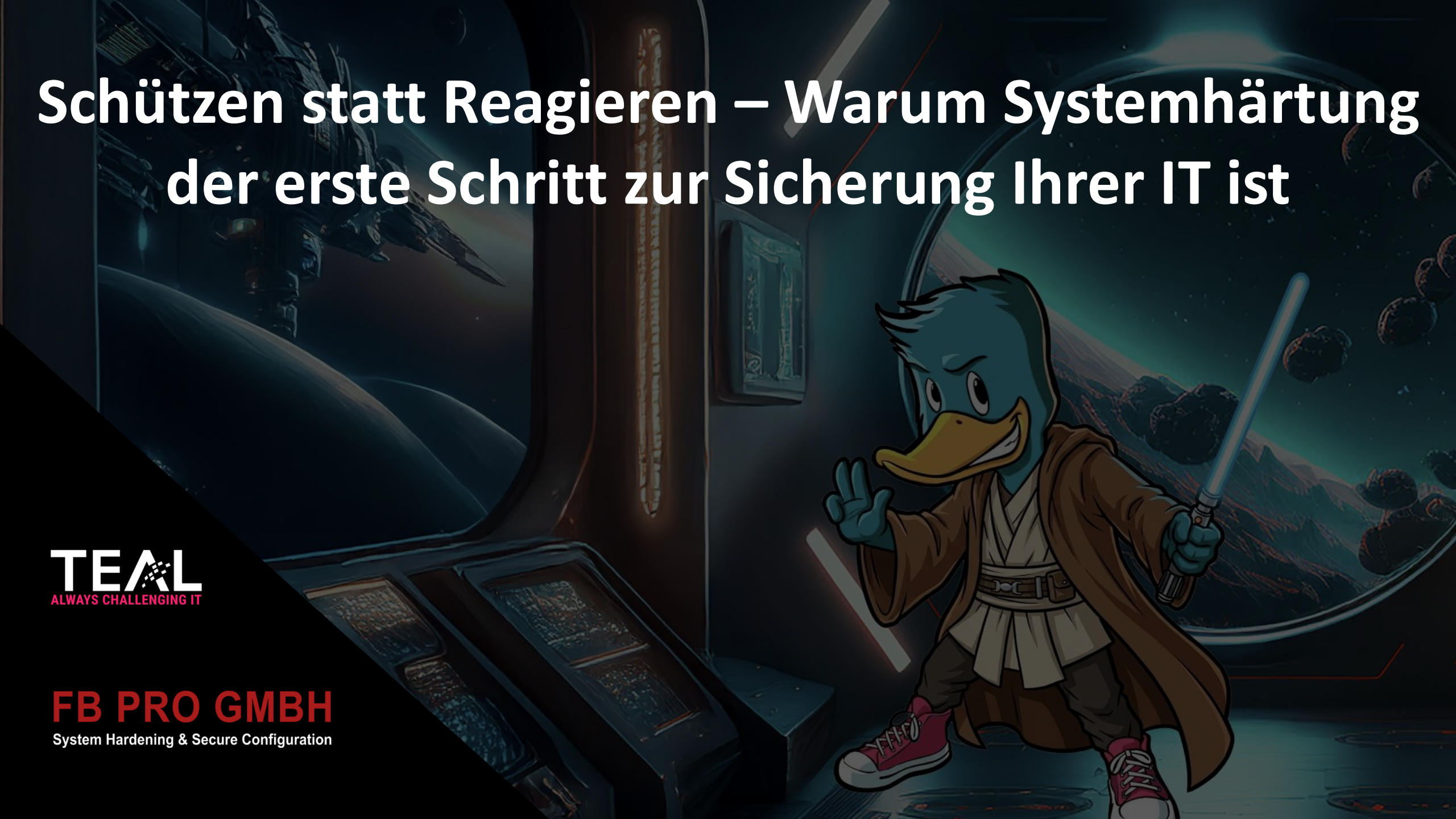
Schützen statt Reagieren – Warum Systemhärtung der erste Schritt zur Sicherung Ihrer IT ist



TEAL
ALWAYS CHALLENGING IT

FB PRO GMBH
System Hardening & Secure Configuration

Florian Bröder

CEO & Founder von FB Pro

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

LinkedIn

Fabian Böhm

CEO & Founder von TEAL

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

LinkedIn

Active Directory

Architecture

TEAL
ALWAYS CHALLENGING IT

Vor Ort auf der secIT 2026

Besuchen Sie uns in der Eilenriedehalle - Stand E40.

Wir freuen uns auf weiteren Austausch nach dem Workshop.

Agenda – Deep Dive Session

1. Kurze Vorstellung Teal & FB Pro
2. Identity is the new perimeter
3. Wie schützen sich Unternehmen heute
4. Was ist eigentlich Systemhärtung?
5. Praxisbewährte Rollout-Ansätze
   - Layered Hardening
   - Rapid Hardening
   - Lifecycle Hardening
6. Q&A / Interaktive Session / RC4 & NTLM

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

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

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

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
13.03.2026	Kerkering, Barberio & Co., Certified Public Accountants	US	Hacker kompromittieren Daten von 4.179 Personen. » Details
13.03.2026	Hypertherm	US	Hacker kompromittieren Daten aufgrund von Sicherheitslücke. » Details
13.03.2026	Grayback Forestry	US	Hacker kompromittieren Daten von 4 Bürgern Maines. » Details
12.03.2026	ID Care	US	Hacker kompromittieren vertrauliche Patientendaten von Praxis. » Details
12.03.2026	Barrio Comprehensive Family Health Care Center (CommuniCare)	US	Hacker kompromittieren Patientendaten von 19.885 Menschen. » Details
12.03.2026	Earthbound Holding	US	Hacker kompromittieren Daten von 6.766 Personen. » Details
11.03.2026	OSI Systems	US	Hacker kompromittieren Daten von 4.910 Personen. » Details
11.03.2026	Health Dimensions Group	US	Hacker kompromittieren Daten von 450 Personen. » Details

Datum	Betroffene	Land	Sicherheitsvorfall
10.03.2026	Logistikdienstleister	DE	Ransomware-Gruppe stiehlt 26 GB Firmendaten von Versanddienstleister. » Details
06.03.2026	Industriezulieferer für Kunststoff-Verpackungen	DE	Ransomware-Gruppe exfiltriert 50 GB sensible Firmendaten. » Details
06.03.2026	Arbeiter-Samariter-Bund Landesverband Saarland e.V. (ASB Saarland)	DE	Ransomwaregruppe stiehlt 72 GB Daten von Hilfsorganisation. » Details
06.03.2026	Sozialer Hilfsträger	DE	Hilfsorganisation aus Essen von Ransomware-Gruppe gelistet. » Details
05.03.2026	Green-Tech-Unternehmen	DE	Ransomware-Bande kompromittiert sensible Daten von Clean-Tech-Firma. » Details
05.03.2026	Industriezulieferer	DE	20 GB von deutschem Technologieunternehmen via Ransomware gestohlen. » Details
05.03.2026	Industriezulieferer	DE	Ransomware-Gruppe veröffentlicht sensible Dokumente im Darknet. » Details
05.03.2026	asgoodasnew electronics GmbH	DE	Schwachstelle in Zahlungsmodul erlaubt Datenklau in Online-Shop. » Details

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

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

Identity is the new perimeter - Wer Identity 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.

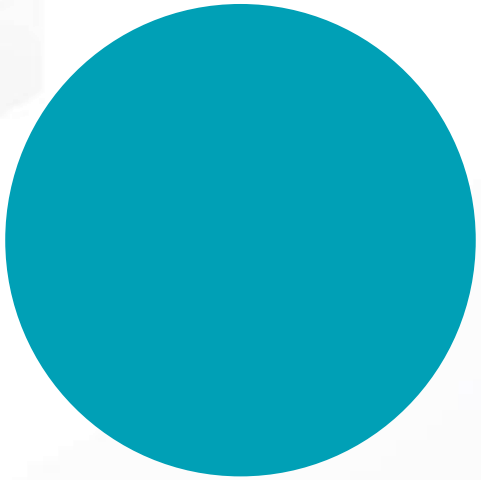
Schutz von AD und Entra ID als strategisches Fundament:
Der Schutz von Active Directory und Entra ID ist kein optionales Sicherheitsfeature. Er bildet das Fundament jeder wirksamen Zero-Trust-Strategie.

TEAL
ALWAYS CHALLENGING IT

FB PRO GMBH
System Hardening & Secure Configuration

Wie schützen sich Unternehmen heute?

Wie schützen sich Unternehmen heute?

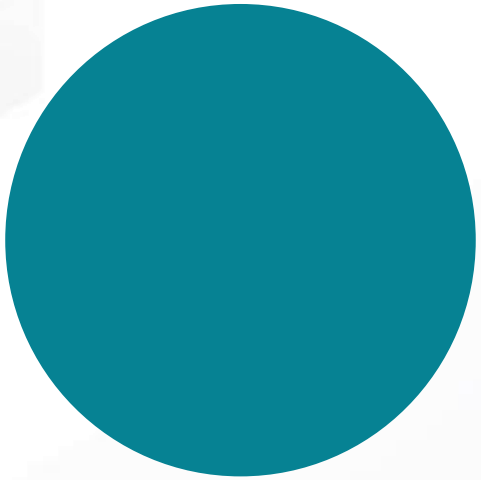


Pentests werden ausgeführt

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

Was ist eigentlich Systemhärtung?

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.

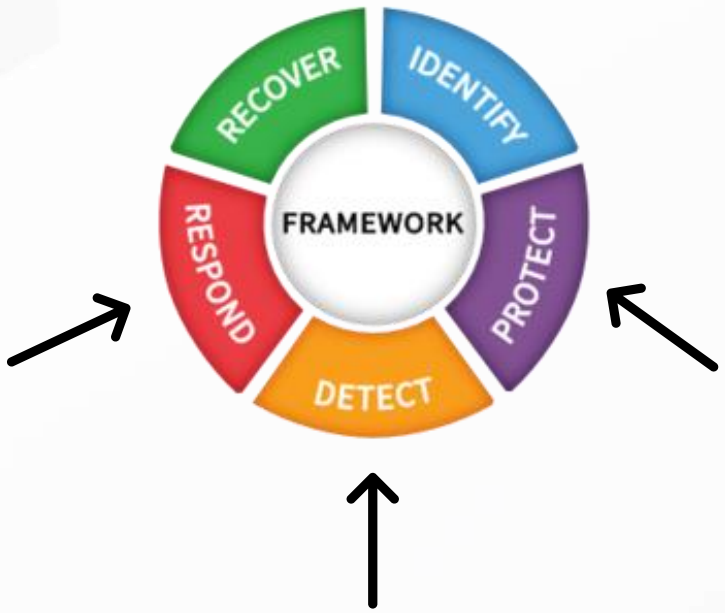
Bei einer professionellen Systemhärtung wird ein IT-System tiefgehend technisch konfiguriert. Eine Anomalieerkennung sorgt dafür, dass Änderungen an Sicherheitskonfiguration erkannt und im Rahmen prozessualer Integration an Security-Teams gemeldet werden. Berichte weisen den Härtungsgrad der Systeme zentral aus, um ein ausreichendes Schutzniveau sicherzustellen, zu halten und transparent zu machen.

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 – kurz erläutert

Es gibt verschiedene Rahmenwerke wie bspw. vom NIST (amerikanische Standardisierungs-organisation), die fünf kritischen Funktionen identifizieren.

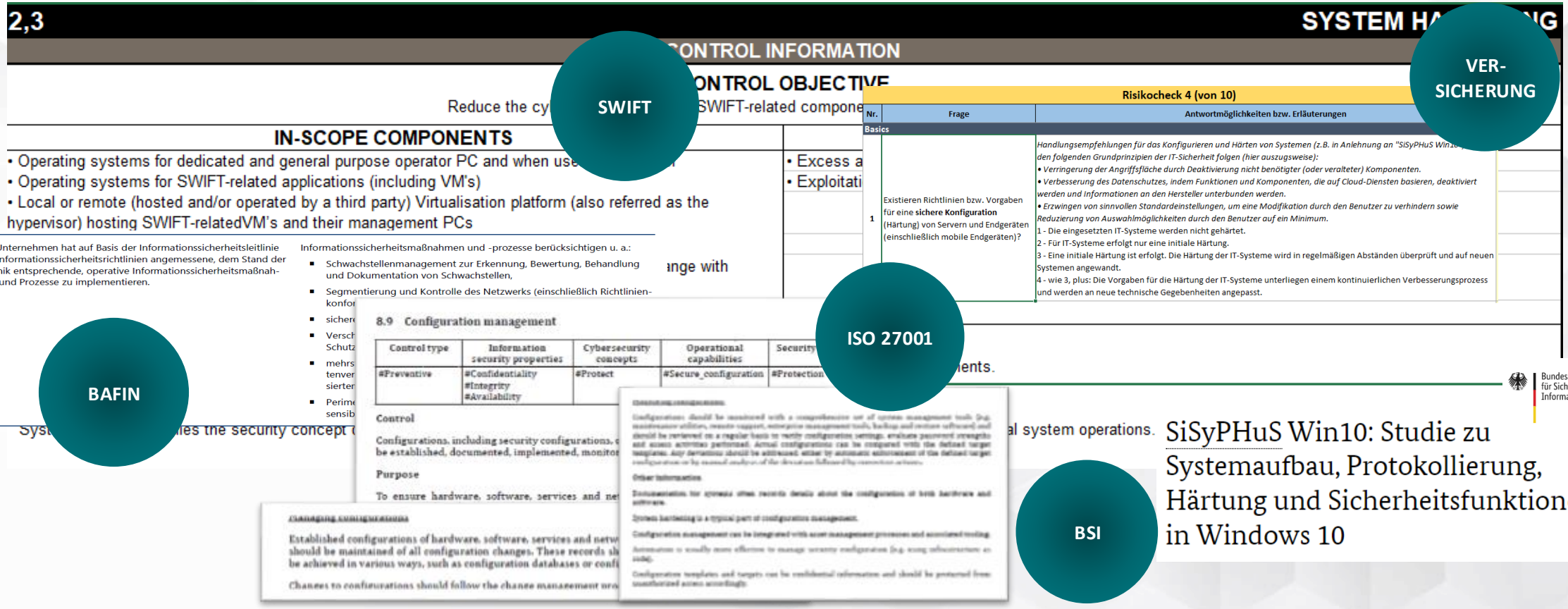


Technology	PROTECT	DETECT	RESPOND
Anti-Malware solutions		X	X
Threat-Intel solutions		X	X
EDR/XDR solutions		X	X
MDR solutions		X	X
Vulnerability scanner		X	
SIEM solutions		X	X (SOC, IM process)
Compromise Assessment		X	X
Hardening	X		
Enforce Administrator	X	X	IM process

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

Systemhärtung – Security-Frameworks

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



TEAL ALWAYS CHALLENGING IT

FB PRO GMBH System Hardening & Secure Configuration

Systemhärtung – in neuen Trends

Hilft Systemhärtung eigentlich auch bei neuen Angriffswegen?

Google says hackers abuse Gemini AI to empower their attacks

By Bill Toulas

February 1, 2025 12:14 PM

Multiple state-sponsored groups are experimenting with the AI-powered Gemini assistant from Google to increase productivity and to conduct research on potential infrastructure for attacks or for reconnaissance on targets.

Google's Threat Intelligence Group (GTIG) detected government-linked advanced persistent threat (APT) groups using Gemini primarily for productivity gains rather than to develop or conduct novel AI-enabled cyberattacks that can bypass traditional defenses.

Threat actors have been trying to leverage AI tools for their attack purposes to various degrees of success as those utilities can at least shorten the preparation period.

https://www.bleepingcomputer.com/news/security/google-says-hackers-abuse-gemini-ai-to-empower-their-attacks

ChatGPT Creates Polymorphic Malware

Alessandro Mascellino

Freelance Journalist

Email Alessandro Follow @a_mascellino

OpenAI's ChatGPT has reportedly created a new strand of polymorphic malware following text-based interactions with cybersecurity researchers at CyberArk.

According to a technical write-up recently shared by the company with *Infosecurity*, the malware created using ChatGPT could "easily evade security products and make mitigation cumbersome with very little effort or investment by the adversary."

The report, written by CyberArk security researchers Eran Shimony and Omer Tsarfati, explains that the first step to creating the malware was to bypass the content filters preventing ChatGPT from creating malicious tools.

To do so, the CyberArk researchers simply insisted, posing the same question more authoritatively.

"Interestingly, by asking ChatGPT to do the same thing using multiple constraints and asking it to obey, we received a functional code," Shimony and Tsarfati said.

Further, the researchers noted that when using the API version of ChatGPT (as opposed to the web version), the system reportedly does not seem to utilize its content filter.

"It is unclear why this is the case, but it makes our task much easier as the web

https://www.infosecurity-magazine.com/news/chatgpt-creates-polymorphic-malware

Systemhärtung – in neuen Trends

Systemhärtung als Präventivmaßnahme ist auch in “trendy” Angriffsszenarien eine wirkungsvolle Maßnahme…

“Polymorphe Malware”*

KI-/AI-basierten Angriffsmethoden*

*Es geht nicht darum, jede neue Methode (Mail, Pattern, Verhalten, etc.) zu erkennen und zu reagieren – die Türe (“der Angriffsvektor”) ist einfach geschlossen.

NEWS

The #1 Skill on OpenClaw's Marketplace Was Malware: Inside the ClawHub Supply Chain Attack

1,184 malicious skills were found on OpenClaw's ClawHub marketplace - stealing SSH keys, crypto wallets, browser passwords, and opening reverse shells. One attacker uploaded 677 packages alone. The #1 ranked skill had 9 vulnerabilities and was downloaded thousands of times.

BY ELENA MARCHETTI · FEBRUARY 19, 2026 · 7 MIN READ

[redacted]
IT Security Operations and Compliance Consu...
Visit my website
3h

Wenn jeder technische Laie in die Lage versetzt wird komplexe Angriffe fahren zu können, dann haben wir es nicht nur mit APTs zutun, sonder mit einer ganz neuen permanenten Angriffskultur.

Ich leite davon folgendes ab, was ich bisher nicht auf dem Radar hatte:

Im SOC sinkt die Signal-to-Noise Ratio (SNR) massiv da durch KI-gestützte Tools eine Flut von automatisierten, teils amateurhaften Angriffen ein enormes Grundrauschen („Noise") erzeugt.

Das ist deshalb schlecht, weil hochgradig gefährliche, gezielte Angriffe in dieser Alert-Flut untergehen ...more

Show translation

Axel Rengstorf and 14 others 10 comments

Like Comment Repost Send

Add a comment...

Most relevant

Florian Bröder • You 3h
Preventive protection. System hardening.

Angriffsvektoren tatsächlich schließen und nicht nur monitoren könnte helfen...nach Systemhärtung googlen könnte dann der erste Schritt sein, um Informationen zu sammeln...

Show translation

Like · 2 | Reply · 1 reply | 68 impressions

https://www.linkedin.com/posts/johanneskresse_wenn-jeder-technische-laie-in-die-lage-versetzt-activity-7430505240522616832-gyWh?utm_source=share&utm_medium=member_desktop&rcm=ACoAAAGq2O0BNAenOcJwQkxeDMgebqys5q1s8EQ

Maßnahmen im Umfeld „Erkennung und Reaktion“ (detection and response) reichen alleine nicht mehr aus, um eine angemessene Informationssicherheit zu gewährleisten.

Warum ist Systemhärtung eigentlich so komplex?

Konkrete Tasks im Rahmen der Einführung von Systemhärtung im Unternehmen

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

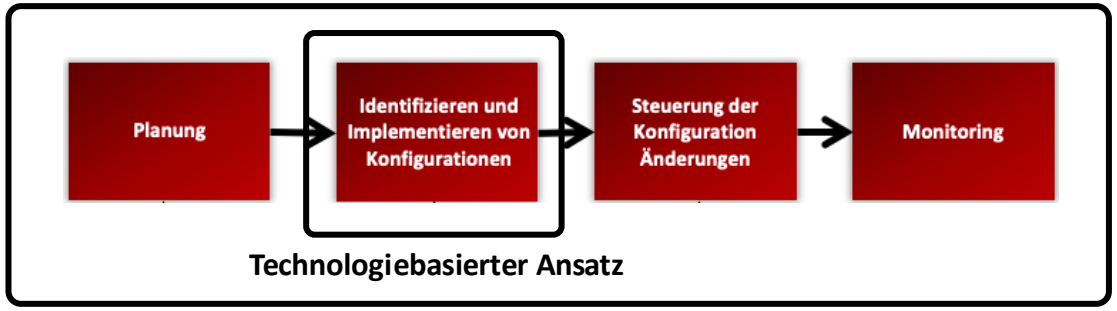
In der Praxis gibt es mehrere technologische Ansätze:

- 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?

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

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"

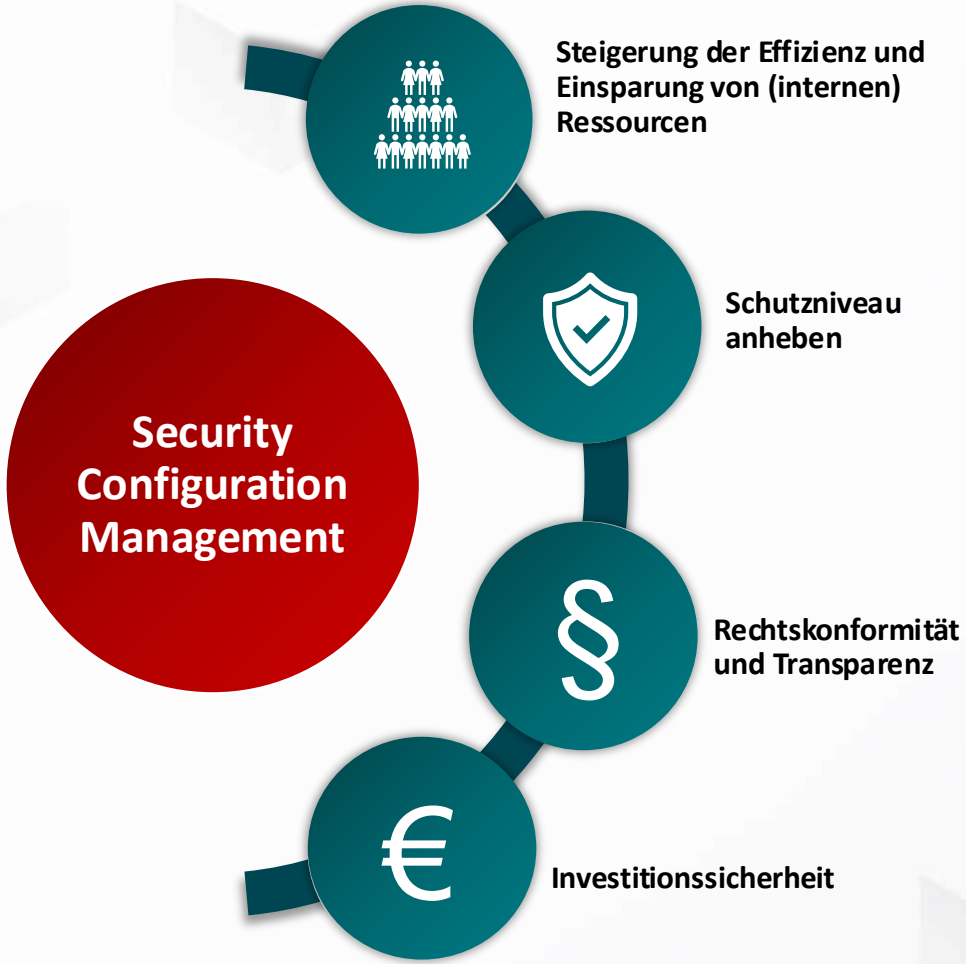


TEAL ALWAYS CHALLENGING IT
FB PRO GMBH System Hardening & Secure Configuration

Warum nicht über "Gruppenrichtlinienobjekte"?

1. Wie schnell sind mehrere hundert Härtungseinstellungen implementiert? Wir sind nach der Installation sofort einsatzbereit.
2. Wie wird kontrolliert, dass alle Einstellungen auf den Zielsystemen ankommen?
3. Wie erfolgt eine "Wiederherstellung" der Einstellungen, wenn eine Anwendung aufgrund von Härtungskonfigurationen nicht mehr funktionsfähig ist?
4. Wie wird das IT-Team benachrichtigt, wenn IT-Systeme plötzlich nicht mehr "konform" zu den vorgegebenen Einstellungen sind?
5. Wie findet eine sinnvolle Prozessintegration (Incident Management, ConfigMgmt) statt?

Systemhärtung hat viele Vorteile



Eine neue Erkenntnis?

Frühzeitig erkannte und behobene Fehler in einer Kette reduzieren den Aufwand und sparen am Ende Geld.

Schlussfolgerung: Härtung ist kosteneffizient!

Praxisbewährte Rollout-Ansätze

Wie kann ich denn jetzt sicher konfigurieren?

Häufige "Fallstricke" bei Härtungsprojekten

Hardening-Projekte helfen bei der Schaffung einer besseren Cyber-Abwehrstrategie! Mögliche ausgenutzte Angriffsvektoren werden deaktiviert. Einiges kann automatisiert werden, manches muss getestet/evaluiert werden. In den meisten Fällen helfen Härtungsprojekte also dabei, die eigene Infrastruktur besser kennenzulernen als man denkt sie zu kennen:

- Welche Dienste sind aktiviert, werden aber nie genutzt?
- Welcher Server (oder welche geschäftskritische Anwendung) läuft noch auf einem alten Betriebssystem?
- Verwenden die Administratoren immer noch ein Konto/einen Rechner für das Surfen im Internet und die Verwaltung?
- Sind “built in accounts" noch aktiv und/oder werden noch kritischere Accounts verwendet?
- Und vieles mehr...

Die häufigsten Fallstricke sind unter anderem die folgenden:

- Fehlende Kenntnis der eigenen Infrastruktur
- Fehlende Dokumentation und Übersicht über die Systeme
- Fehlende Dokumentation und Übersicht über die Anwendung
- Fehlendes Wissen darüber, wie z.B. Administratoren Systeme warten
- "Altmodische" (aka unsichere) Methoden zur Wartung/Verwaltung von IT-Systemen

Hardening Rollout Strategien

Layered Hardening

- Härtung erfolgt stufenweise im Rahmen eines Sicherheitsprojekts. Klassifizierung der Systeme als Tier 0 / Tier 1 / Tier 2.
- Start mit den kritischsten Systemen (Tier 0).
- Die anderen Layer werden nach T0 durchgeführt.

Anwendung:

- Nach einer Sicherheitsverletzung oder proaktiv, um Angriffsfläche zu verringern.
- Wenn Schwerpunkt auf hoher Sicherheit liegt.

Security Level	★★★★★
Komplexität	★★☆☆☆
Aufwand	★★☆☆☆
Dauer	★★★☆☆

Rapid Hardening

- Wellenbasierte Einführung eines einheitlichen Hardening-Sets, für schnell messbare Sicherheitsgewinne.
- Je nach Standardisierung kann das Base- oder das Secure-Hardening-Set verwendet werden
- Weitere iterative Erhöhung der Sicherheitsstufe je Kritikalität möglich.

Anwendung:

- Einhaltung von Audits – TISAX, ISO
- Beginn von Härtungsaktivitäten & Aufbau von Vertrauen in eine Lösung.
- Schneller Rollout.

Security Level*	★★☆☆☆
Komplexität	★★★★☆
Aufwand	★★★☆☆
Dauer	★★★★☆

Lifecycle Hardening

- Hardening wird fest in ein Lifecycle-Projekt integriert (z.B. Einführung von Windows 11, Hardware Refresh).
- Systeme werden bereits bei Erstbereitstellung gehärtet -> hohe Effizienz & Konsistenz.
- Solider Benchmark (CIS-Level 2).

Anwendung:

- Geringerer Aufwand für Applikationstests.

Security Level	★★★★☆
Komplexität	★★★☆☆
Aufwand	★★★★★
Dauer	★★★☆☆

*Bewertung basiert auf den Base Hardening Set

Vorschlag Projektablauf

Projektsetup

- Aufbau Enforce Administrator durch Teal.
- [Kunde] begleitet optional zum Wissensaufbau.

Rolloutstrategie – Server (Anzahl: 500)

Annahme:

- Aufteilung der Server in zwei Kategorien:
  - **Base Hardening** (~90%) -> effiziente, schnelle Basisicherung – 50% CIS L1 comliance.
  - **Secure Hardening** (~10%) -> maximale Sicherheit für besonders kritische Systeme – 80% Cis L2 compliance.

Vorgehen:

- Base Hardening (Rollout in Wellen): Beispiel ist grafisch rechts dargestellt.
- Secure Hardening (Parallel zum Rollout): System für System Vorgehen.

Rolloutstrategie – Clients (Anzahl: 6.500)

Annahme: Hochstandardisierte Clients → Secure Hardening:

- Laborprüfung, anschließender Friendly-user Test und ein schrittweiser Rollout in wachsenden Wellen bis 300 Clients pro Woche. Maximal jedoch 26 Wellen.

Annahme: Nichtstandardisierte Clients:

- Fallback auf Base Hardening, identische Rollout Methode.

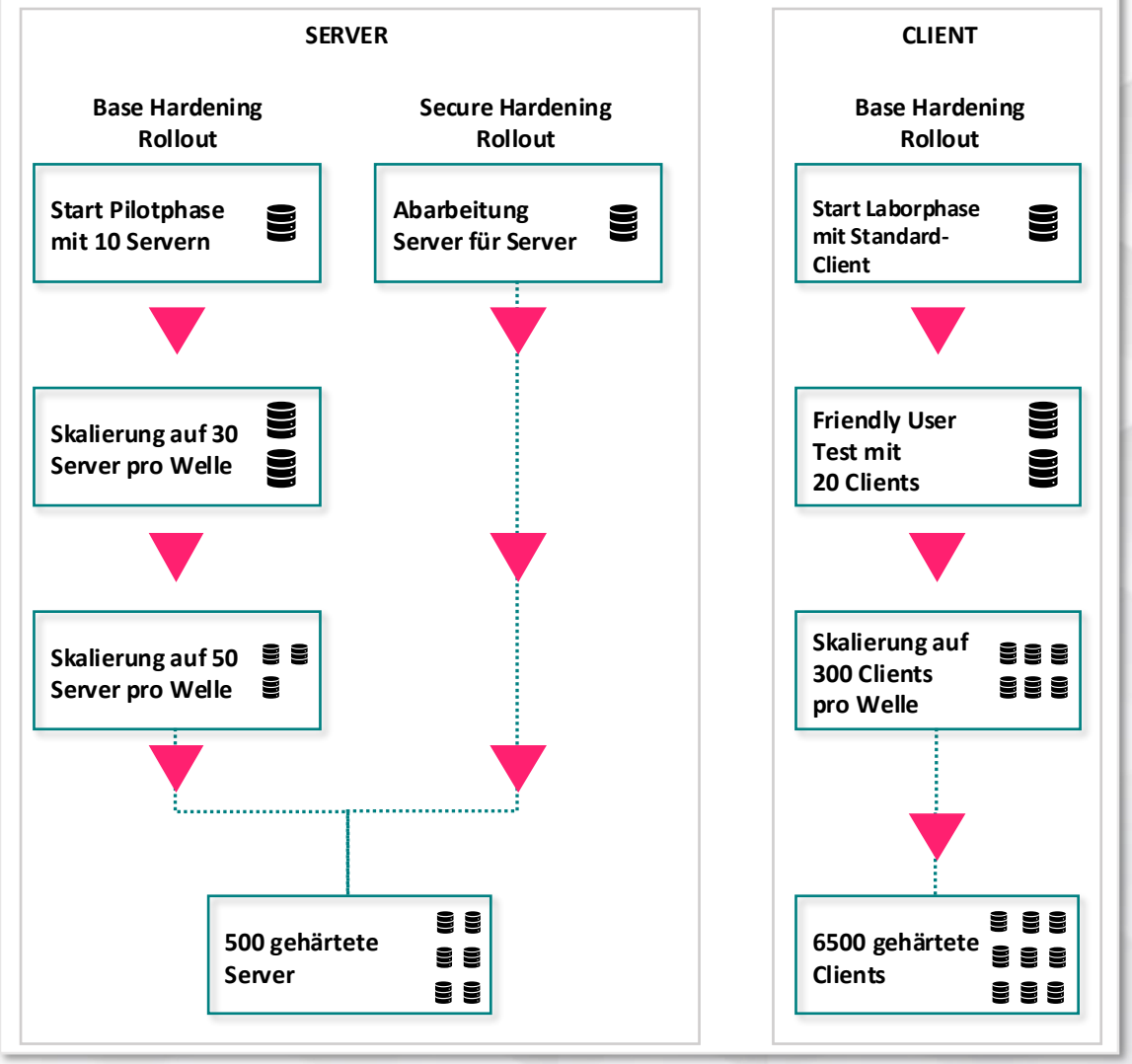
Must-Have

Ab Projektstart:

- Alle neuen Systeme müssen zwingend **vollständig Secure-gehärtet** sein.
- **Vollautomatisches Onboarding** in den Enforce Administrator.

Betrieb

- Betrieb des Enforce Administrators erfolgt durch **[Kunde]** oder **Teal.**



TEAL ALWAYS CHALLENGING IT

Interaktive Session

Echte Geschichten / Herausforderungen / Ihre Anfragen

„war story“

1. **Konkrete Kundensituation**
   - Gehärtetes Windows-System macht (laut Logfile) einen Fallback auf NTLMv2 (und nicht Kerberos)
   - Ungehärtetes Standard-Windows-System macht keinen Fallback und nutzt Kerberos

2. **Analyse**
   - Im Rahmen der Härtung "alte Algorithmen" abgeschaltet (RC4, DES, etc.)
   - Da DomainController und auch der Service "FileShare" (basierend auf einer NETAPP APpliance) aber für Kerberos ausschließlich alte Algorithmen zulassen für Kerberos Encryption, war auf Kerberos-Ebene keine Kommunikation machbar (Remember: Client hat kein RC4 und kein DES mehr zugelassen)
   - Also Fallback auf NTLMv2
   - Erstmal paradox, aber dann gut nachvollziehbar

3. **Fazit**
   - Das Thema ist nicht nur ein informationssicherheitstechnisches Thema
   - Auch Datenschutz (Stand der Technik)
   - Und auch Compliance denn wenn man aus dem regulierten Finanzsektor kommt, gelten noch folgende Dinge:
     a) PCI-DSS fordert den Einsatz starker kryptografischer Verfahren [kleiner Spoiler: DES und RC4 gehören nicht mehr dazu
     b) Das BSI empfiehlt in seiner Technische Richtlinie zu kryptografischen Verfahren bei der Verwendung von TLS nur noch auf AES basierende Verschlüsselung (auch hier sind DES und RC4 nicht mehr dabei)

RC4

HERAUSFORDERUNG

RC4 gilt seit langem als schwacher Cipher. Bei der Verwendung mit Kerberos gibt es einen bekannten Angriff namens Kerberoasting, bei dem das Knacken etwa 800 Mal schneller ist als bei der Verwendung von AES. Wenn RC4 für den Sessionkey verwendet wird, kann die Sicherheitslücke CVE-2022-37966 - Windows Kerberos RC4-HMAC Elevation of Privilege Vulnerability ausgenutzt werden.

BEKANNTE ATTACKEN

CVE-2026-20833

Steal or Forge Kerberos Tickets: Kerberoasting, Sub-technique T1558.003 - Enterprise | MITRE ATT&CK®

January 2026

Windows updates released on and after January 13, 2026, contain protections for a vulnerability with the Kerberos authentication protocol. The Windows updates address an information disclosure vulnerability in CVE-2026-20833 that might allow an attacker to obtain service tickets with weak or legacy encryption types such as RC4 to perform offline attacks to recover a service account password.

April 2026

Enforcement mode will be automatically enabled by installing Windows Updates released on or after April 2026 on all Windows domain controllers and will block vulnerable connections from non-compliant devices. At that time, you will not be able to disable the auditing but may move back to the Audit mode setting.

July 2026

Enforcement Phase

The Windows updates released in or after July 2026 will remove support for the registry subkey **RC4DefaultDisablementPhase**.

NTLM

Microsoft will NTLM v1 und v2 loswerden

Phase 1

Phase 2

Phase 3

Building visibility and control

Available now, enhanced NTLM auditing helps your organization understand exactly where and why NTLM is still being used in your environment. This is the foundation of any NTLM migration effort.

You can use it today with Windows Server 2025 and Windows 11, versions 24H2 and later. For additional guidance, see Disabling NTLM.

Addressing the top NTLM pain points

Here is how we can address some of the biggest blockers you may face when trying to eliminate NTLM:

- **No line of sight to the domain controller:** Features such as IAKerb and local Key Distribution Center (KDC) (pre-release) allow Kerberos authentication to succeed in scenarios where domain controller (DC) connectivity previously forced NTLM fallback.
- **Local accounts authentication:** Local KDC (pre-release) helps ensure that local account authentication no longer forces NTLM fallback on modern systems.
- **Hardcoded NTLM usage:** Core Windows components will be upgraded to negotiate Kerberos first, reducing instances on NTLM usage.
- The solutions to these pain points will be available in the second half of 2026 for devices running Windows Server 2025 or Windows 11, version 24H2 and later.

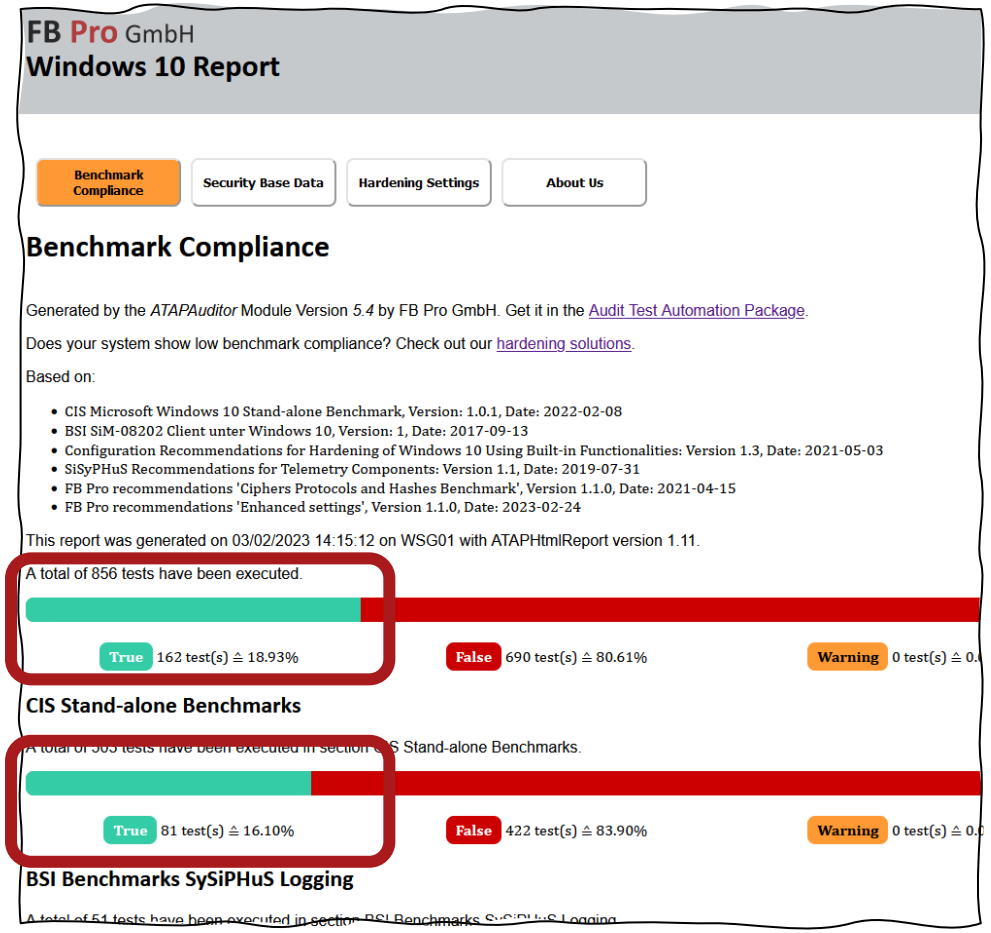
NTLM disabled by default

In the next major Windows Server release and associated Windows client releases:

- Network NTLM will be disabled by default.
- NTLM usage will require explicit re-enablement through new policy controls.
- Support for handling NTLM only cases will be built-in, reducing application breakage. Examples include accessing targets with unknown SPNs, authentication requests made using IP addresses, local accounts on domain joined machines, and new NTLM blocking policies.

Systemhärtungstatus einfach mal messen

Systemhärtung mit dem AuditTAP messen – gegen aktuelle Standards



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

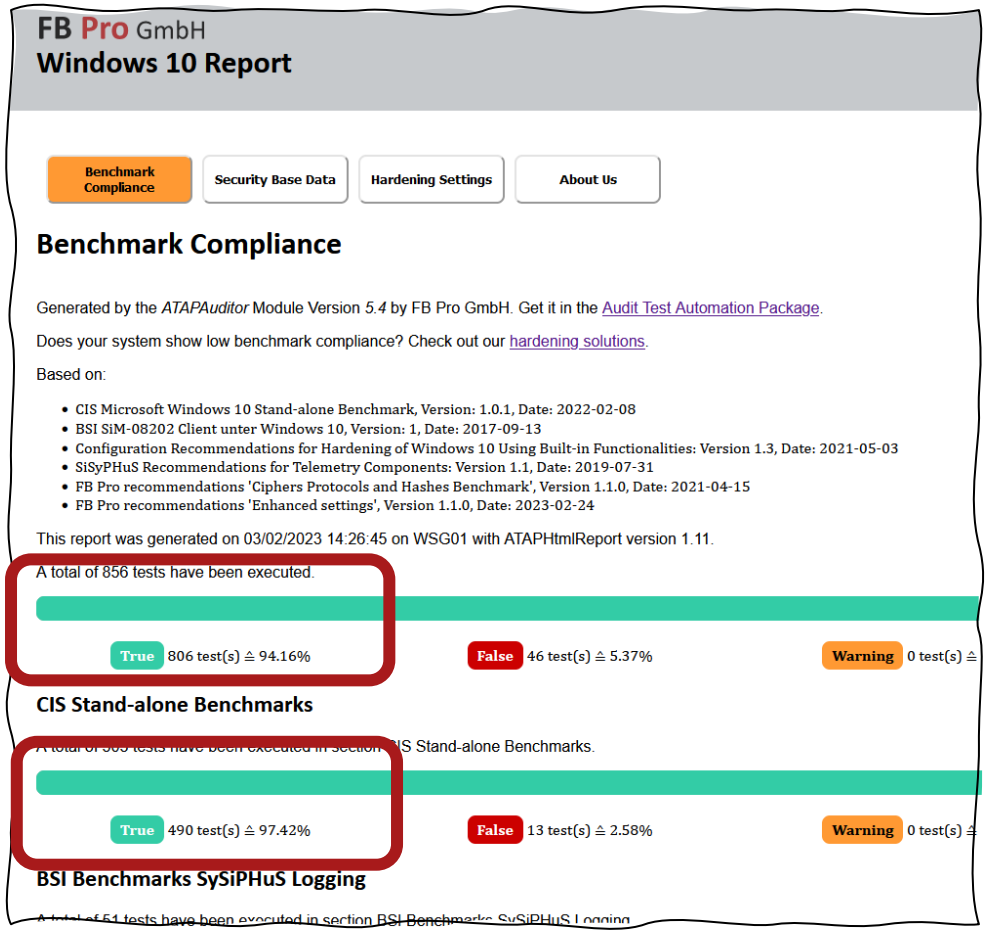
CIS Stand-alone Benchmarks

A total of 505 tests have been executed in section CIS 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

A total of 505 tests have been executed in section 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

AuditTAP Ergebnis – Hilfe zur Einordnung

< 30% Compliance

Das Betriebssystem ist mehr oder weniger in der Standard-Konfiguration im Einsatz.

Statements:

- Starten mit Systemhärtung auf Basis anerkannter Empfehlungen wie CIS, DISA oder anderer
- Stand der Technik erreichen, im ersten Schritt sind ~50% Compliance sinnvoll
- Nachweisbarkeit erreichen

< 50% Compliance

Erste Härtungskonfigurationen sind angewendet.

Statements:

- Erster Schritt gemacht, iterativ besser werden, 80% Compliance machbar
- Einstellungen überwachen und prozessual integrieren
- Dokumentation aktuell halten

> 80% Compliance

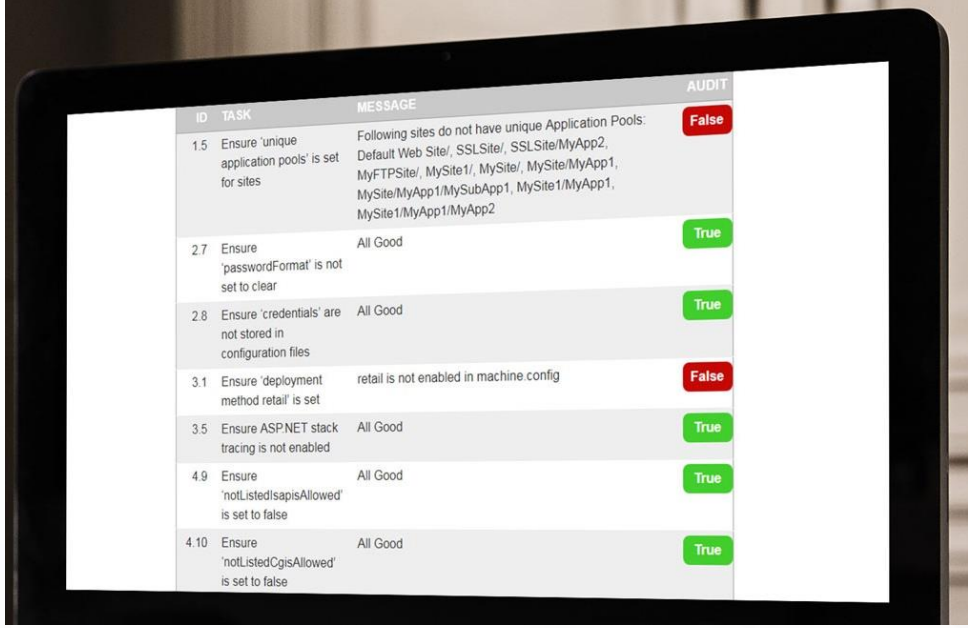
Härtung auf Basis von Standards ist angewendet.

Statements:

- Die letzten Schritte gehen und besser werden
- Besonderes Augenmerk auf kritische Einstellungen legen
- Ausnahmen für Legacy-Applikationen zurückfahren

Wir können konkret helfen, wenn…

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



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

TEAL
ALWAYS CHALLENGING IT

FB PRO GMBH
System Hardening & Secure Configuration

Standprogramm Eilenriedehalle E40

Mi, 18.03.2026

Uhrzeit	Ort	Thema	Weitere Informationen
10:00 – 10:30	Stand E40	Showcase *Systemhärtung live erleben*	
11:00 – 11:20	Stand E40	Q&A-Session *Fragen Sie unsere Kunden*	mit Christopher Loch / Deutsche Energy Terminal
11:30 – 12:00	Stand E40	Showcase *Systemhärtung live erleben*	
13:00 – 13:30	Stand E40	Showcase *SMBv1-Lücke schließen*	
14:30 – 15:30	Deep-Dive Raum 18	Deep-Dive *Schützen statt Reagieren**	Kostenloser Workshop / mit Fabian Böhm
16:00 – 16:20	Stand E40	Q&A-Session *Fragen Sie unsere Kunden*	mit Andreas Hübner / Landkreis Spree-Neiße
16:30 – 17:00	Stand E40	Showcase *Bye, bye, PrintNightmare!*	
17:15 – 17:45	Stand E40	Showcase *Systemhärtung live erleben*	

Do, 19.03.2026

Uhrzeit	Ort	Thema	Weitere Informationen
09:30 – 09:50	Stand E40	Q&A-Session *Fragen Sie unsere Kunden*	mit Bert Peters / T.I.K. GmbH
10:00 – 10:30	Stand E40	Showcase *Systemhärtung live erleben*	
10:00 – 11:00	Deep-Dive Raum 17	Deep-Dive *Schützen statt Reagieren**	Kostenloser Workshop / mit Fabian Böhm
10:30 – 11:00	Stand E40	Showcase *SMBv1-Lücke schließen*	
13:30 – 14:00	Stand E40	Showcase *Systemhärtung live erleben*	
15:00 – 15:30	Stand E40	Showcase *Systemhärtung live erleben*	

TEAL
ALWAYS CHALLENGING IT

FB PRO GMBH
System Hardening & Secure Configuration

Vielen Dank!

Weitere Informationen

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

… und ab in die Eilenriedehalle zu Stand E40

(unser Gewinnspiel und Live-Demo-Showcases warten auf dich)

Kontaktdaten

TEAL

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

Telefon: 0211/93675225

FB PRO

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

Telefon: 06721/4009999