TEAL
ALWAYS CHALLENGING IT

CYBERHYGIENE

die unterschätzte Sicherheitsmaßnahme

Teal Technology Consulting GmbH

Fabian Böhm

CEO & Founder von TEAL

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

LinkedIn

Obwohl viele Unternehmen moderne Sicherheitslösungen einsetzen, bleibt eine Verbesserung aus.

Woran liegt das und wie können Verbesserungen nachhaltig umgesetzt werden?

Datum	Betroffene	Land	Sicherheitsvorfall
10.09.2025	Quadrant Capital	US	Finanzdienstleister meldet Datenleck nach E-Mail-Hack. » Details
10.09.2025	Print Media Association	US	Cyber-Angriff. » Details
10.09.2025	Peregrine Property Management & Peregrine Group	US	Hacker kompromittieren Daten von 1.059 Personen. » Details
09.09.2025	Kreditunternehmen	DE	Ransomware-Angriff: Gruppe droht mit Kundendaten-Leak. » Details
09.09.2025	Noble	IN	Familienbetrieb für Dämmstoff wird auf Opferblog geführt. » Details
09.09.2025	Farmer Brothers Company	US	Hacker kompromittieren Daten von 14.460 Personen. » Details
09.09.2025	Conference USA	US	Hacker kompromittieren Daten von 1.459 Personen. » Details
09.09.2025	Fachanwaltskanzlei	DE	Ransomwaregang exfiltriert angeblich 330 GB von Kanzlei. » Details
09.09.2025	Anchorage Neighborhood Health Clinic	US	Cyberangriff legt Gesundheitszentrum lahm und kompromittiert Daten. . » Details
09.09.2025	Valley Mountain Regional Center	US	Datenpanne bei sozialer Einnrichtung: 529 Klienten betroffen. » Details

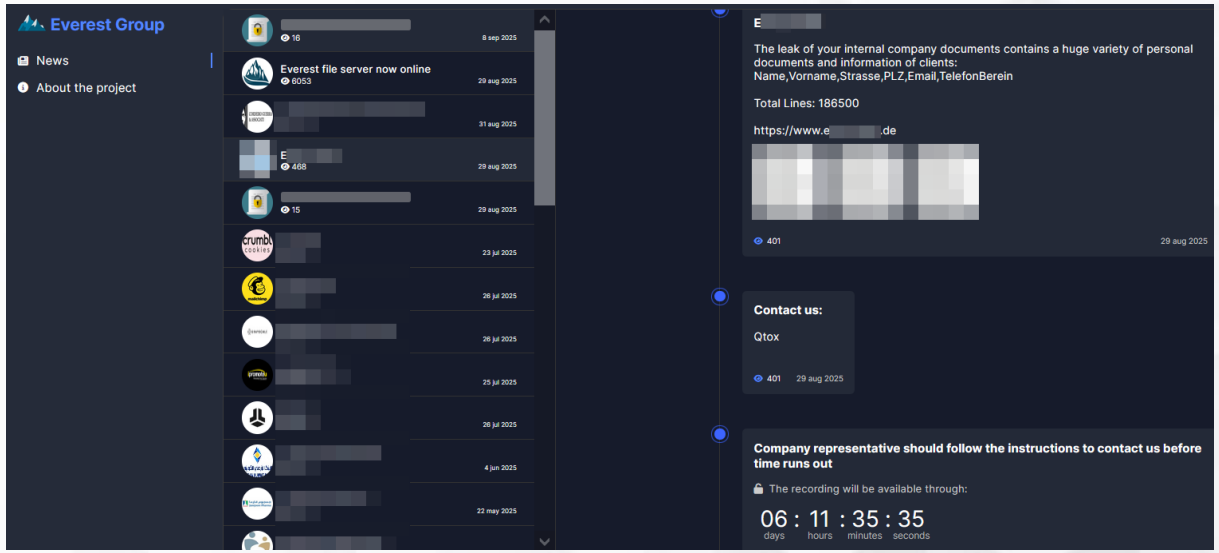
[Sicherheitsvorfall-Datenbank: Datenpannen, Cyber-Atacken und andere Sicherheitsvorfälle | dsgvo-portal.de]

Datum	Betroffene	Land	Sicherheitsvorfall
10.09.2025	Quadrant Capital	US	Finanzdienstleister meldet Datenleck nach E-Mail-Hack. » Details
10.09.2025	Print Media Association	US	Cyber-Angriff. » Details
10.09.2025	Peregrine Property Management & Peregrine Group	US	Hacker kompromittieren Daten von 1.059 Personen. » Details
09.09.2025	Kreditunternehmen	DE	Ransomware-Angriff: Gruppe droht mit Kundendaten-Leak. » Details
09.09.2025	Noble	IN	Familienbetrieb für Dämmstoff wird auf Opferblog geführt. » Details
09.09.2025	Farmer Brothers Company	US	Hacker kompromittieren Daten von 14.460 Personen. » Details
09.09.2025	Conference USA	US	Hacker kompromittieren Daten von 1.459 Personen. » Details
09.09.2025	Fachanwaltskanzlei	DE	Ransomwaregang exfiltriert angeblich 330 GB von Kanzlei. » Details
09.09.2025	Anchorage Neighborhood Health Clinic	US	Cyberangriff legt Gesundheitszentrum lahm und kompromittiert Daten. . » Details
09.09.2025	Valley Mountain Regional Center	US	Datenpanne bei sozialer Einnrichtung: 529 Klienten betroffen. » Details

Details zum Sicherheitsvorfall

Ransomware | Datendiebstahl | Erpressung

Betr. (Unternehmen)	Kreditunternehmen
Datum (Veröffent.)	09.09.2025
Land	Deutschland
Vorfall	Am 29. August 2025 listete die "Everest"-Ransomware-Gruppierung ein Kreditunternehmen einer deutschen Bank auf ihrer Darknet-Seite als Opfer. Sie behaupteten, Namen, Adressen, E-Mails, Telefonnummern und potenziell weitere Kundendaten erbeutet zu haben und drohen damit, diese zu veröffentlichen, falls das Unternehmen nicht bis zum 16. September 2025 Kontakt zu ihnen aufnimmt.
Täter	Everest
Quellen	09.09.2025: Everest (Screenshot, Abrufdatum)
Teilen	

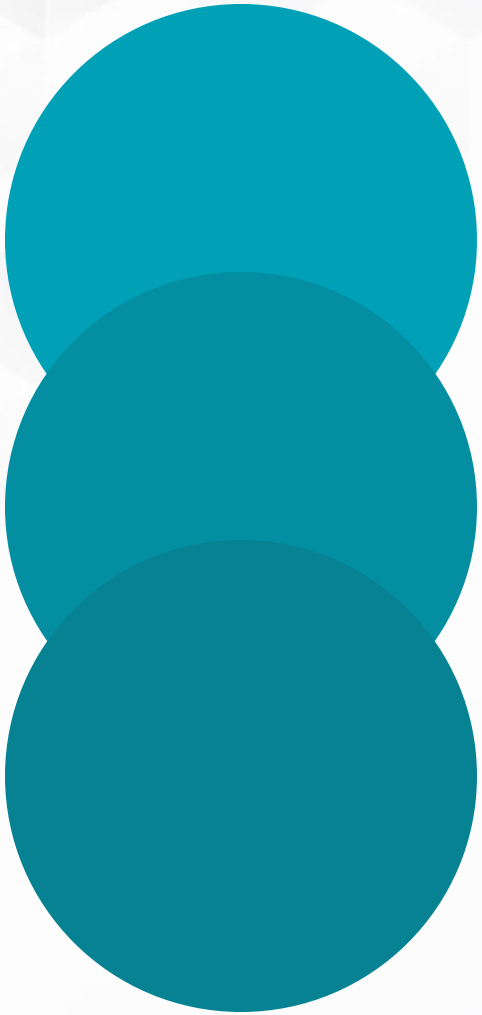


[Sicherheitsvorfall-Datenbank: Datenpannen, Cyber-Atacken und andere Sicherheitsvorfälle | dsgvo-portal.de]

TEAL ALWAYS CHALLENGING IT

Wie schützen sich Unternehmen heute?

Wie schützen sich Unternehmen heute?



Pentests werden ausgeführt

Tools wie XDR, Schwachstellenscans, SOCs etc. werden eingeführt

Firewalls und klassische Antivirus-Software

… und das reicht aus?

NEIN!

Wieso funktioniert das nicht?

1. **Pentest-Ergebnisse werden nur teilweise angegangen.** Danach landet der Bericht wieder in der Schublade.

2. **Meldungen in Security Tools** werden nicht bearbeitet.

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 Produktionsmaschinen. Das alte ERP-System kann nicht abgeschaltet werden etc.

Kontinuität

Wissensaufbau

Angriffsfläche verkleinern

Wie schütze ich mich richtig?

technische Schulden beseitigen

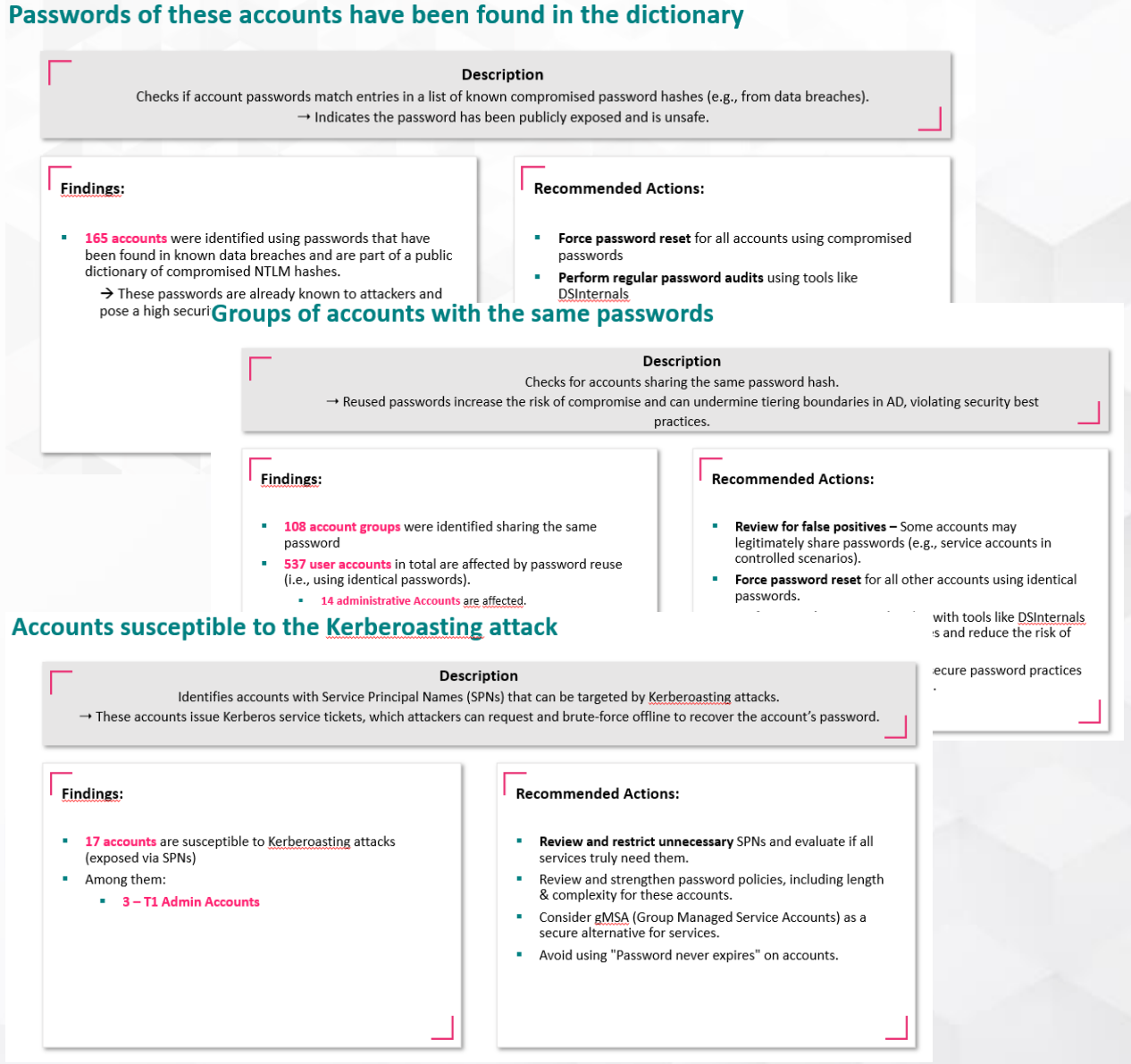
Basishygiene

1.

Regelmäßige Passwort Überprüfungen

NTLM-Hashes werden aus der AD-DB extrahiert und mit bekannten kompromittierten Passwörtern abgeglichen. So lassen sich schwache, wiederverwendete oder bereits kompromittierte Kennwörter identifizieren.

Dieser proaktive Ansatz stärkt die Sicherheit unserer Domäne gezielt und effektiv.



TEAL ALWAYS CHALLENGING IT

Passwords of these accounts have been found in the dictionary

Description

Checks if account passwords match entries in a list of known compromised password hashes (e.g., from data breaches).

→ Indicates the password has been publicly exposed and is unsafe.

Findings:

- **165 accounts** were identified using passwords that have been found in known data breaches and are part of a public dictionary of compromised NTLM hashes.

  → These passwords are already known to attackers and pose a high security risk.

Recommended Actions:

- **Force password reset** for all accounts using compromised passwords
- **Perform regular password audits** using tools like DSInternals
- Implement **password blacklist filtering** (e.g., with Azure AD Password Protection)

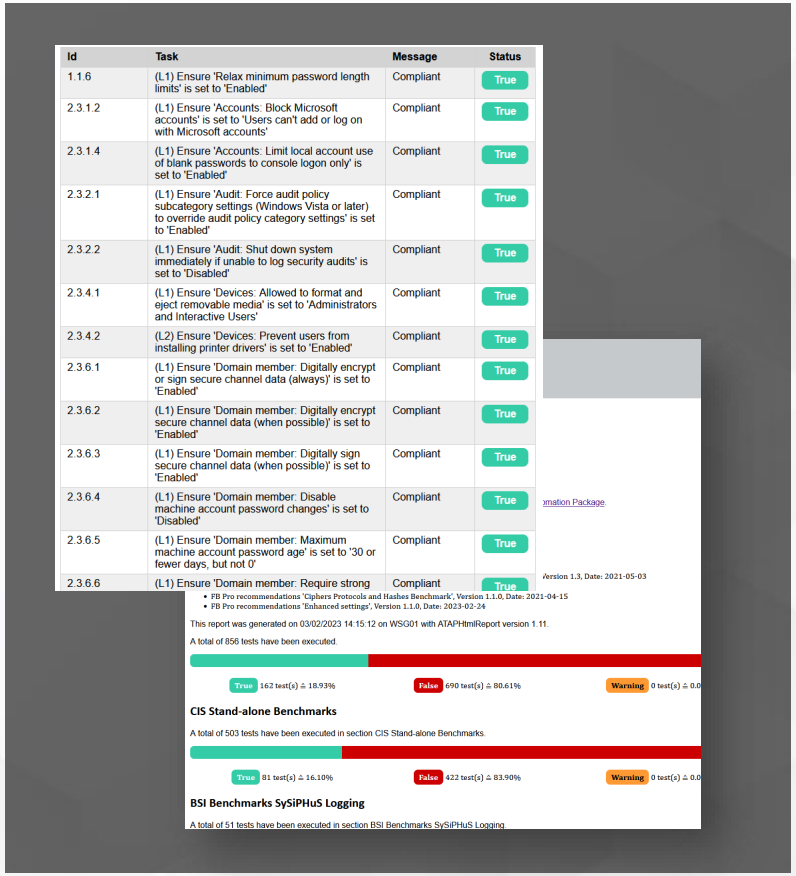
Basishygiene

2.

Systemhärtung

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

Gängige Industriestandards sind z.B. die Empfehlungen von CIS oder BSI



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

ormation Package.

Version 1.3, Date: 2021-05-03

- 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 503 tests have been executed in section CIS Stand-alone Benchmarks.

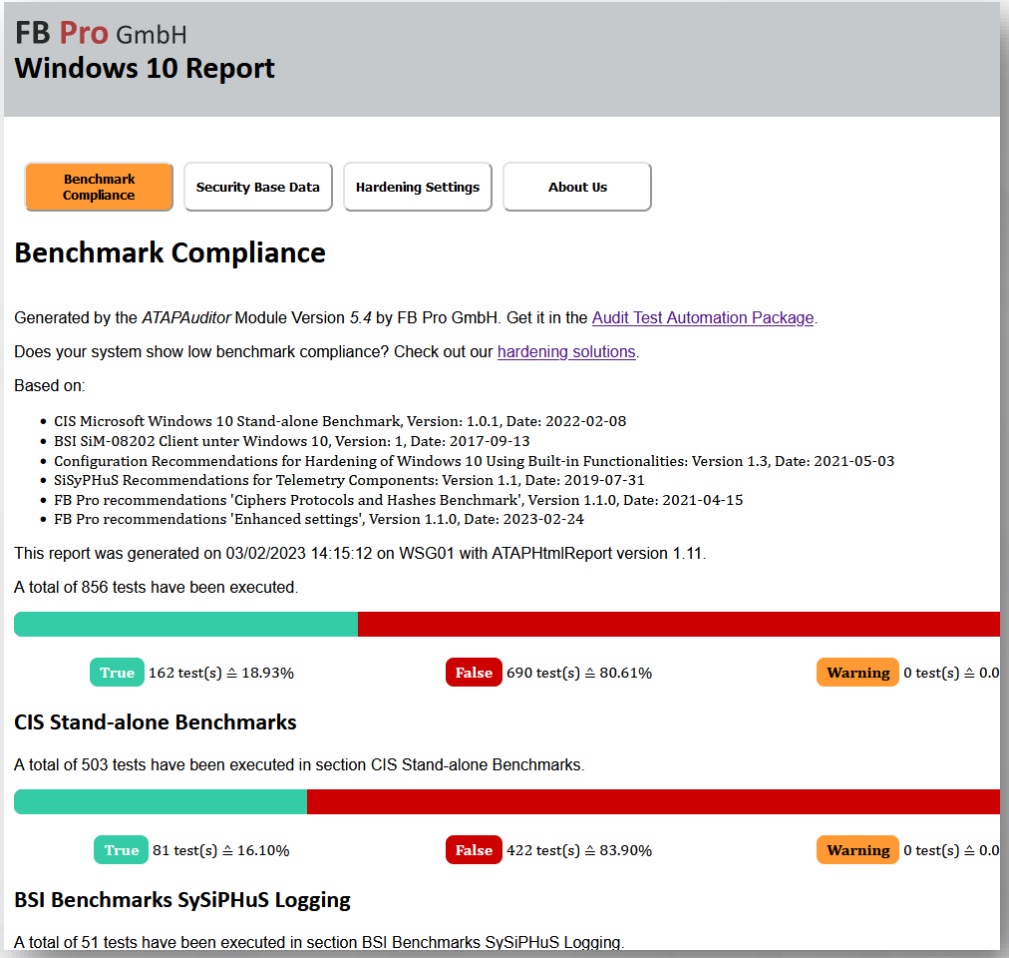
True 81 test(s) ≙ 16.10% False 422 test(s) ≙ 83.90% Warning 0 test(s) ≙ 0.0

BSI Benchmarks SySiPHuS Logging

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

Basishygiene

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



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 503 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.

Kostenlose Analyse: https://github.com/fbprogmbh/Audit-Test-Automation

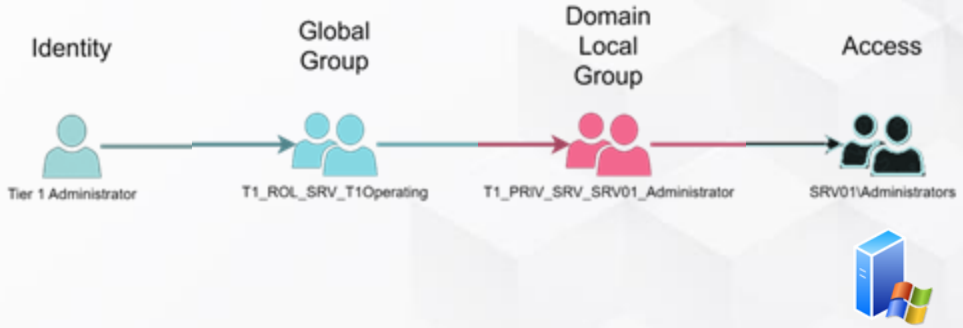
Basishygiene

3.

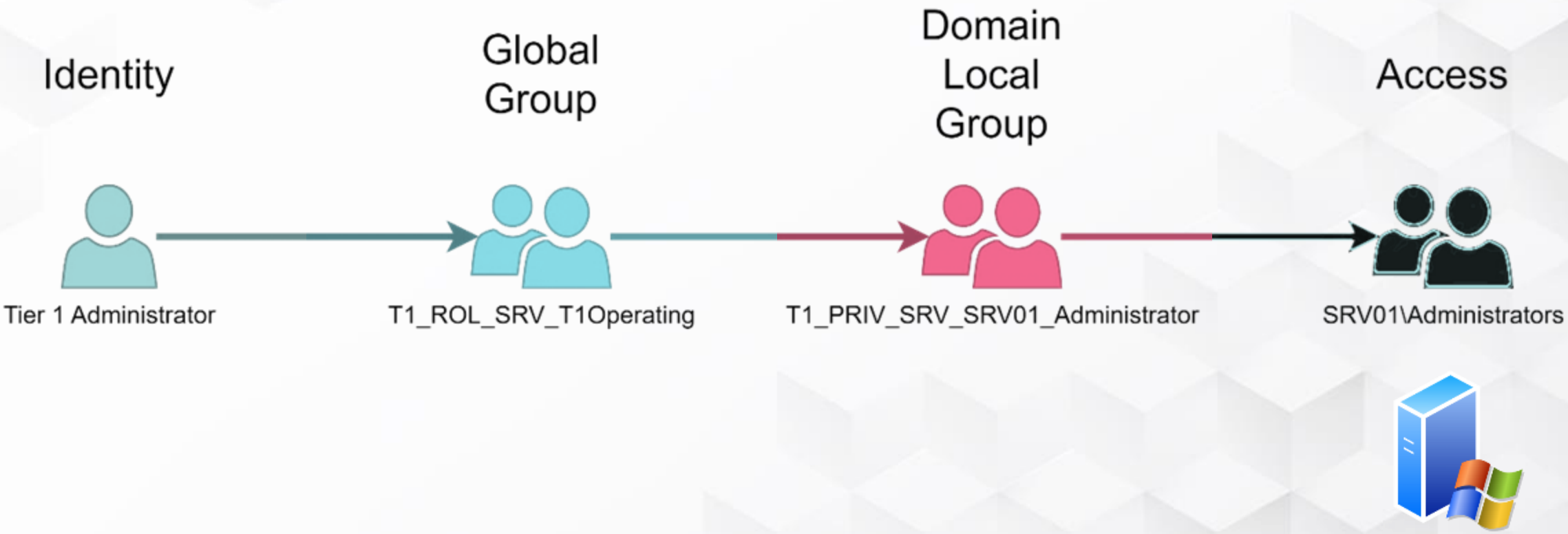
RBAC / least privileges

RBAC (Role-Based Access Control) und das Prinzip der minimalen Rechtevergabe (Least Privilege) sind essenziell für eine sichere IT-Umgebung.

- RBAC sorgt dafür, dass Benutzer nur Zugriff auf die Ressourcen erhalten, die ihrer Rolle entsprechen.
- Least Privilege verhindert, dass Benutzer unnötige Berechtigungen haben, wodurch potenzielle Angriffsflächen deutlich minimiert werden.



Basishygiene

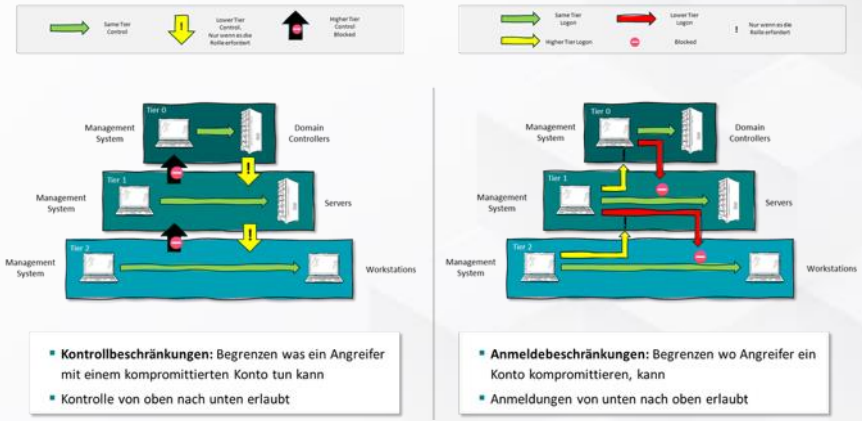


Basishygiene

4.

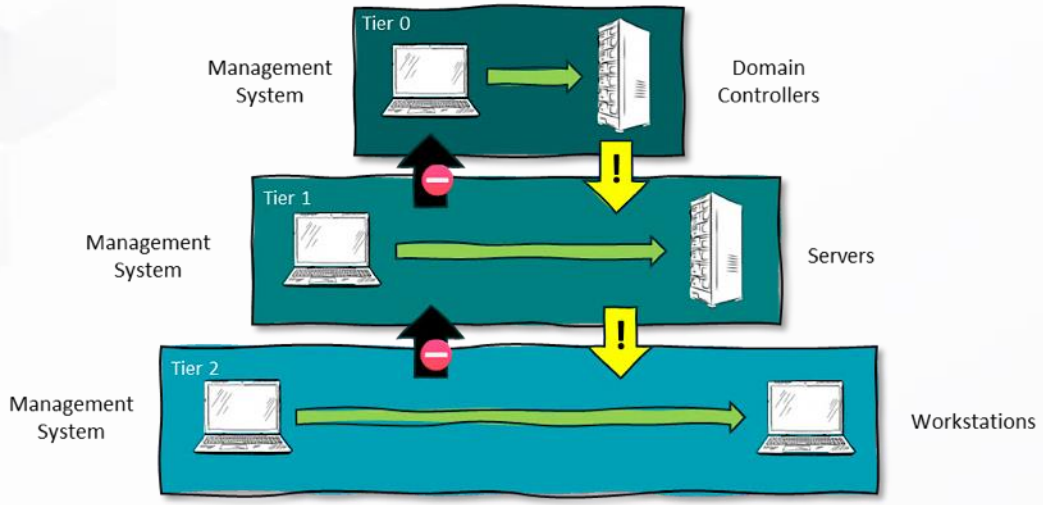
Tiering

die Aufteilung von IT-Systemen und Identitäten in Sicherheitsstufen, meist Tier 0, Tier 1 und Tier 2. Dadurch wird verhindert, dass ein kompromittiertes Konto mit niedriger Berechtigung Zugriff auf kritische Systeme erhält, was die Angriffsfläche deutlich reduziert.

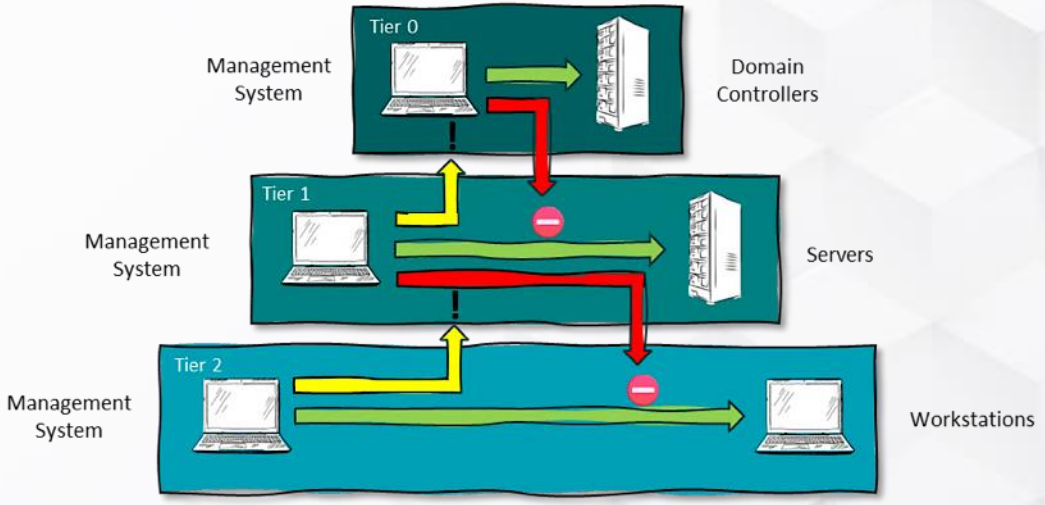


TEAL ALWAYS CHALLENGING IT

Basishygiene



- **Kontrollbeschränkungen:** Begrenzen was ein Angreifer mit einem kompromittierten Konto tun kann
- Kontrolle von oben nach unten erlaubt



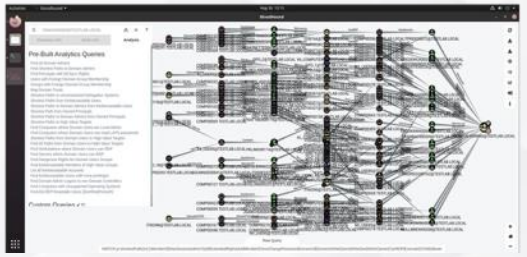
- **Anmeldebeschränkungen:** Begrenzen wo Angreifer ein Konto kompromittieren, kann
- Anmeldungen von unten nach oben erlaubt

Basishygiene

5.

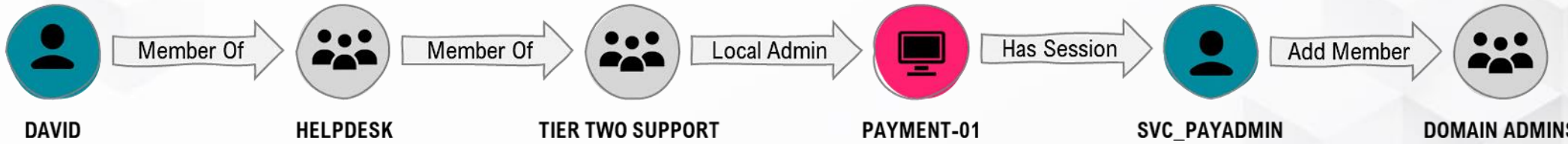
Attack Path Management

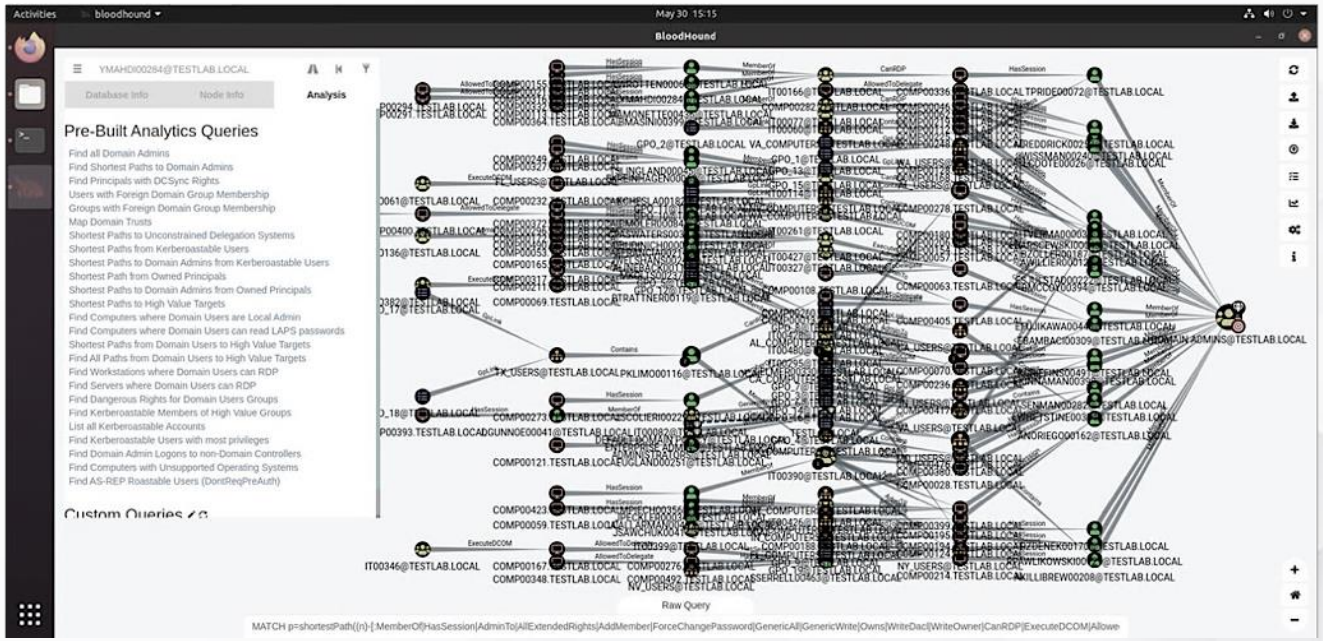
bezeichnet die systematische Identifikation und Beseitigung von potenziellen Angriffswegen innerhalb einer IT-Infrastruktur. Ziel ist es, die Möglichkeiten für Angreifer, sich lateral durch das Netzwerk zu bewegen, frühzeitig zu erkennen und gezielt zu unterbrechen.



TEAL ALWAYS CHALLENGING IT

Basishygiene





TEAL ALWAYS CHALLENGING IT

Teste dein Security-Niveau

Starte jetzt selbst den kostenlosen Identity Check.
Gerne helfen wir dir bei der Analyse deiner Ergebnisse.

Self Assessment

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

Live - Webinar
24.09. um 12-13 Uhr

„Die 5 kritischsten Pentest-Findings, die du sofort beheben solltest“

Sei dabei!

https://www.itideen.de/hackerfrei-webinar

Vielen Dank!

TEAL ALWAYS CHALLENGING IT