



20. Mai 2026

17. Bechtle
IT-Forum
Thüringen
Steigerwald Stadion Erfurt

20
26

AD Tiering geknackt: Audit-Albträume entlarvt

Wie aus Strukturfehlern echte
Geschäftsrisiken werden

Pascal Bliedung &
Jannis Weigand

20.05.2026



Pascal Bliedung

Zertifizierungen / relevante Trainings :

- ✓ 2017 **ISO/IEC 27001** Foundation | Zertifizierung
- ✓ 2020 **OWASP TOP 10** Exploit Training
- ✓ 2020 **Greenbone** Vulnerability Management Training
- ✓ 2021 **PenTesting** & Netzwerkhacking FAU Erlangen
- ✓ 2022 **Computerstrafrecht** FAU Erlangen
- ✓ 2023 **CSP** Cyber Security Practitioner ISACA e.V. | Zertifizierung
- ✓ 2025 **BSI** Grundschutz-Praktiker & BSI Grundschutz-Berater
- ✓ 2025 **NIS2** Lead Implementer



Jannis Weigand

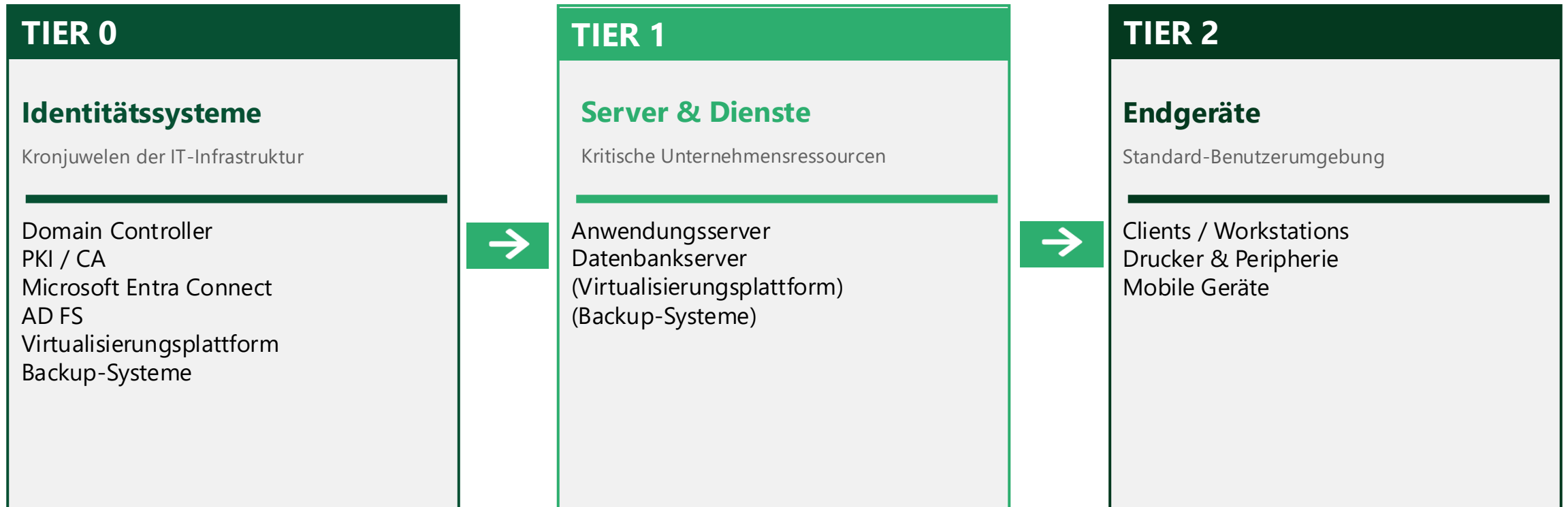
Zertifizierungen / relevante Trainings :

- ✓ 2025 **Sophos** Firewall Certified Engineer | Zertifizierung
- ✓ 2025 **CSP** Cyber Security Practitioner ISACA e.V. | Zertifizierung



Was ist AD-Tiering?

AD-Tiering ist ein Sicherheitsmodell, das alle Systeme und Administrator-Konten in Ihrem Active Directory in drei strikt getrennte Sicherheitsebenen (Tiers) unterteilt – um die laterale Ausbreitung von Angreifern zu stoppen.



Warum ist AD-Tiering wichtig?



Schutz der Kronjuwelen

Kompromittierung eines Tier-2-Clients öffnet NICHT das Tor zu Domain Controllern
Laterale Bewegungen oder Privilege Escalation (Pass-the-Hash oder Kerberoasting) werden blockiert.



Compliance & Regulatorik

NIS2, ISO 27001 und BSI IT-Grundschutz fordern Privileged Access Management
-> AD-Tiering ist der technische Nachweis und reduziert Haftungsrisiken.



Least Privilege

Jedes Admin-Konto erhält ausschließlich die Rechte für seine jeweilige Ebene
Kein Konto hat überall Zugriff!



Risikominimierung für die Geschäftsführung

Geringeres Risiko von Betriebsausfällen, Datenverlust, Reputationsschäden und Bußgeldern durch Datenschutzverletzungen.

Finding #1 – Server falsch zugeordnet

Ein Domain-Admin-Konto ist nur so gut geschützt wie das Gerät, auf dem es benutzt wird.

Was ist zu beachten?

Systeme nach Risiko und Verwaltungswirkung einstufen

Citrix- und Terminalserver sind z.B. Tier-2
(Benutzerarbeit)

Administrative Anmeldungen höherer Tiers konsequent verhindern

Managementsysteme: Wer Tier 0 verwaltet, ist Tier 0

SCCM / WSUS / Deployment-Systeme dürfen keine unkontrollierte Brücke zwischen Tiers bilden

Auswirkungen auf Management / Organisation

Ein einzelner kompromittierter Benutzerarbeitsplatz kann zur Serverkompromittierung führen

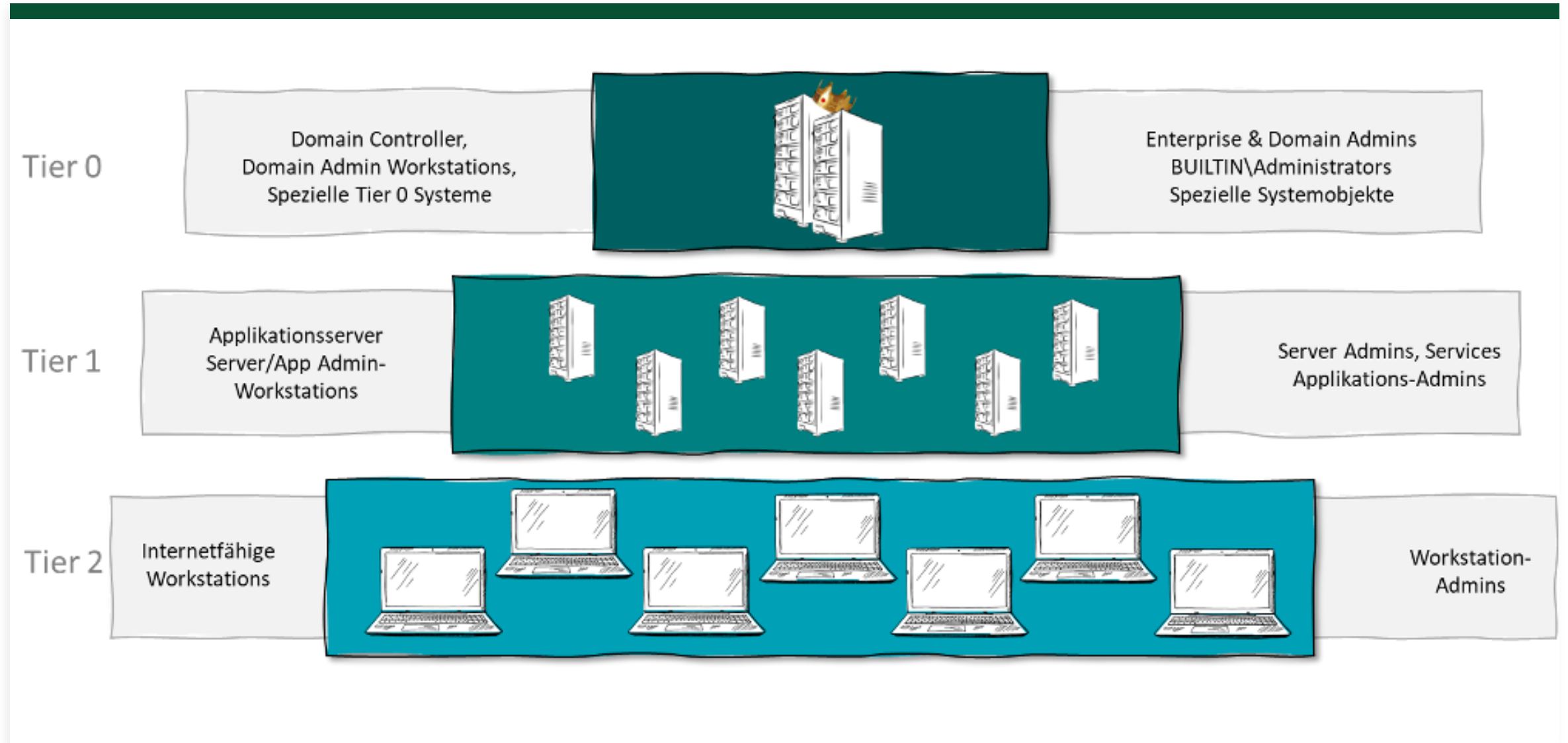
Das Tiering wirkt auf dem Papier sauber, wird technisch aber durch falsche Systemklassifizierung ausgehebelt

Aus einem isolierten Client-Vorfall kann ein unternehmensweiter Sicherheitsvorfall entstehen

Kritische Dienste wie AD, Fileservices, Fachanwendungen oder zentrale Infrastruktur können betroffen sein

**Nicht „Server oder Client“ entscheidet über das Tier, sondern die Frage:
Wer arbeitet dort, wer meldet sich dort an und welche Systeme können von dort aus beeinflusst werden?**

Finding #1 – Server falsch zugeordnet



Finding #2 – Nur Admins und DCs im Scope

Was ist zu beachten?

Tier 0 umfasst mehr als Domain Admins und DCs:

- GPO-Rechte
- OU-Delegationen
- AD CS
- Backup
- Hypervisor
- Entra Connect
- PAM und Jumpserver
- PAWs

Effektive Berechtigungen prüfen

-> nicht nur Gruppenmitgliedschaften

Auswirkungen auf Management / Organisation

Die Liste der Domain Admins kann sauber aussehen, obwohl weiterhin kritische Angriffspfade bestehen

Ein Konto ohne offensichtliche Hochprivilegierung kann trotzdem Tier-0-Wirkung entfalten

Audits finden nicht nur „zu viele Admins“, sondern versteckte Kontrollmöglichkeiten

Ein Angreifer muss nicht Domain-Admin heißen, wenn er Domain-Admin-Wirkung erreichen kann

Nicht der Gruppenname entscheidet über das Risiko, sondern die tatsächliche Wirkung einer Berechtigung auf: Identitäten, Richtlinien und kritische Systeme.

Finding #3 – Nutzung bestehender Konten

Was ist zu beachten?

Alte Admin-Konten nicht ungeprüft in neues Tiering übernehmen

Neue Tier-Konten sauber erstellen: eigener Zweck, eigene OU, eigene GPOs, klare Namenskonvention

Historie alter Konten prüfen: Logons, lokale Gruppen, Dienste, Tasks, Skripte, Zertifikate

Alte Admin-Konten kontrolliert ent-privilegieren, deaktivieren oder entfernen

Parallelbetrieb alter und neuer Admin-Konten zeitlich begrenzen und überwachen

Auswirkungen auf Management / Organisation

Das neue Sicherheitsmodell übernimmt sonst alte, unbekannte Risiken

Alte Konten können somit als Bypass am neuen Tiering vorbei genutzt werden

Im Incident ist schwer nachvollziehbar, welche Altlasten noch aktiv waren

Investitionen in Tiering verlieren Wirkung, wenn alte Generalschlüssel weiter funktionieren

Ein neues Tiering-Modell mit alten Admin-Konten ist oft nur ein neues Etikett auf alten Angriffspfaden.

Finding #4 – LAPS nicht (korrekt) umgesetzt

Was ist zu beachten?

LAPS nicht nur aktivieren, sondern nach Tiers sauber delegieren

Client-Helpdesk darf nur Client-Kennwörter lesen

Server-LAPS-Zugriff getrennt und nur für zuständige Serveradministratoren vergeben

Tier-0-LAPS-Zugriff besonders restriktiv behandeln

Effektive Leserechte regelmäßig prüfen: OU-Vererbung, alte Delegationen, „All Extended Rights“

Auswirkungen auf Management / Organisation

Ein kompromittiertes Helpdesk-Konto kann sonst zum Server-Angriffspfad werden

Eine eigentlich gute Schutzmaßnahme wird durch falsche Berechtigungen zum Risiko

Laterale Bewegung wird nicht verhindert, sondern nur anders ermöglicht

Supportprozesse können ungewollt Zugriff auf geschäftskritische Systeme eröffnen

LAPS schützt nur dann vor Flächenbrand, wenn nicht jeder Bereich die Schlüssel zum nächsten Brandabschnitt lesen kann.

Finding #5 – Kein Tiering im Backup

Ein funktionierendes Backup ist die Lebensversicherung eines jeden Unternehmens.

Was ist zu beachten?

Zugriff auf ein Backup = Zugriff auf das System selbst.

Backupkonsole generell sichern

Nur Tier-0-Admins dürfen z.B. Backups der Domain Controller einsehen → Wiederherstellung von Passwort-Hashes

Explizite Freigabe nur für Backup-Sets des gleichen Tiers: granulare Rechteverwaltung in der Backup-Lösung

Auswirkungen auf Management / Organisation

Ein einziger kompromittierter Benutzer mit Backup-Zugriff kann die gesamte AD-Infrastruktur übernehmen

Unkontrollierter Backup-Zugriff verletzt NIS2, DSGVO und BSI IT-Grundschutz (CON.10)

Backup-Konsolen-Zugriff revisionssicher protokollieren und regelmäßig auditieren

Prozessanpassung notwendig: geringer Konfigurationsaufwand, aber regelmäßige Prüfung der dedizierten Konten

Ein Tiering-Konzept ohne Backup-Einbindung ist unvollständig und gefährlich.

Finding #6 – PKI im falschen Tier

Die PKI ist der Vertrauensanker der gesamten Infrastruktur.

Was ist zu beachten?

Zugriff auf die PKI= Kontrolle über das AD

ADCS Server generell ins Tier 0 (Zertifikate nutzbar für Anmeldungen [802.1X, VPN, Smartcard])

Keine Schreibrechte/Template-Besitzer von Tier-1-Konten auf Zertifikatstemplates → eröffnet Eskalationspfade zur AD-Übernahme

Templates, die beliebige Subject Alternate Name (SAN) erlauben, zwingend Tier-0 (Bspw. MDM)

Auswirkungen auf Management / Organisation

Eine einzige ADCS-Fehlkonfiguration kann zur vollständigen Übernahme des gesamten ADs führen.

NIS2 und BSI IT-Grundschutz (APP.1.2, OPS.1.1.7) fordern expliziten Schutz kryptographischer Infrastruktur.

dedizierte Tier-0-Admin-Konten und klare Zuständigkeiten

Fehlkonfigurationen der PKI sind gleichbedeutend mit einer offenen Tür zum Domain Controller.

Finding #7 – NTLMv1 bricht das Tiering

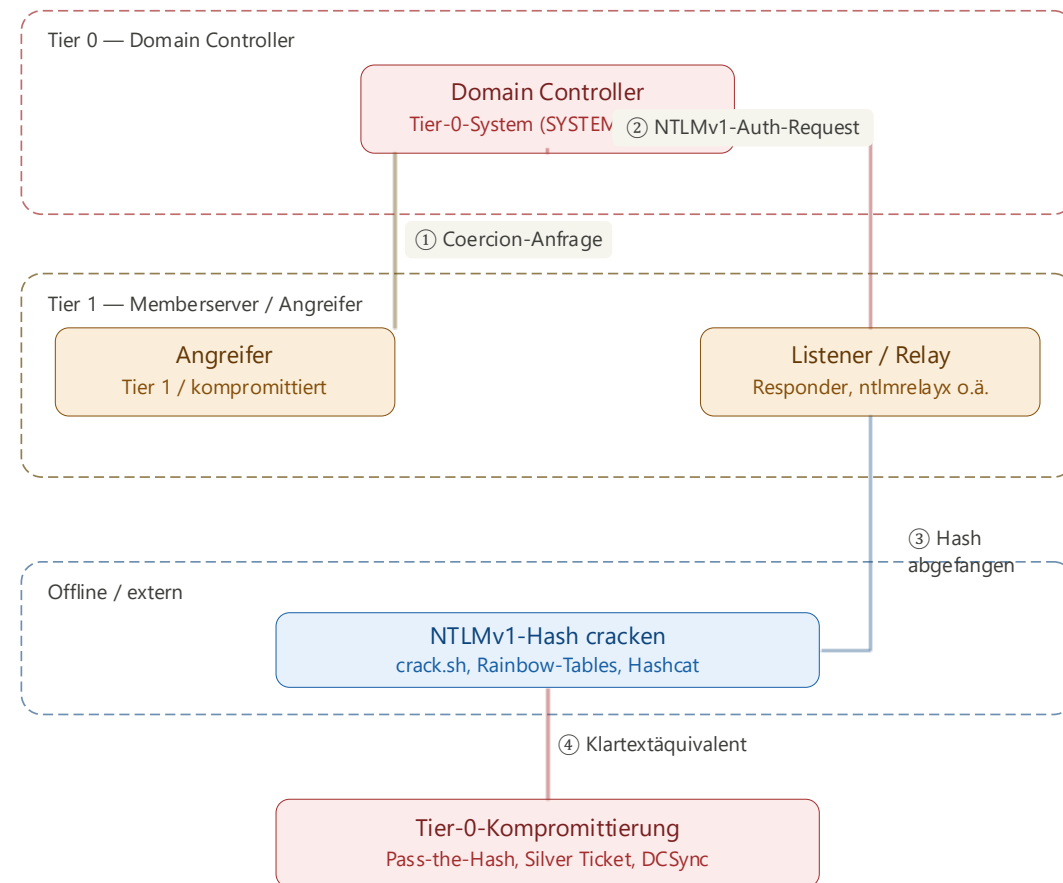
Windows-Systeme vertrauen sich innerhalb einer Domäne ...

Coercion- / NTLM-Relay-Angriff

1. Spezieller RPC-Aufruf zwingt / nötigt den DC zur Authentifizierung bei einer kontrollierter (z.B. Druckerspuler)

2. & 3. NTLM-Hash-Information (v1) wird abgefangen → Missbrauch möglich (Hash-Tabellen oder direkter Relay)

4. Missbrauch möglich (Hash-Tabellen oder direkter Relay z.B. an Webservices für DC-Zertifikat oder Hash-Synchronisation Benutzer Hashes)



Finding #7 – NTLMv1 kann das Tiering brechen

Windows-Systeme vertrauen sich innerhalb einer Domäne ...

Was ist zu beachten?

NTLMv1 vollständig deaktivieren

LDAP & SMB Signing erzwingen
→ verhindert NTLM-Relay-Angriffe

Unnötige Dienste auf DCs deaktivieren
→ z.B. WebClient, Druckspooler

Tiering mit Authentication Policies absichern
→ Verhindert die Authentifizierung von Tier-0-Konten gegenüber Tier-1-Systemen

Alarmierung für Anmeldeereignisse in Verbindung mit unsicheren Authentifizierungsprotokollen einrichten

Auswirkungen auf Management / Organisation

kein Patching möglich

kein Produkt, keine Lizenz notwendig, reine Konfiguration

vorherige Auditphase notwendig (2-4 Wochen)

Regulatorik fordert Abschaltung:
BSI IT-Grundschutz (SYS.1.2, NET.1.1) und NIS2 fordern den Einsatz aktueller, sichere Authentifizierungsprotokolle

Ein Angreifer mit beliebigem Netzwerkzugang kann ohne gültige Credentials via Coercing + Relay die gesamte AD-Infrastruktur übernehmen

Finding #8 – kein Review, kein Mitleid

Strukturiertes Review ist gleichzeitig Sicherheitsmaßnahme, Compliance-Nachweis und Kostenhebel.

Was ist zu beachten?

Quartalsweise strukturierte Reviews für T0- und T1-Konten

Automatisiertes Alerting für bestimmte Usergruppen bei einer definierten Zeitspanne der Inaktivität

Dokumentierter Owner, Zweck und Gültigkeitsdatum für Service-Accounts

Regelmäßige Berechtigungsscans: ACL-basierte Eskalationspfade schließen
→ Shadow-Admins finden

Auswirkungen auf Management / Organisation

Cyber-Kriminelle suchen gezielt nach inaktiven privilegierten Konten
→ Zugriff ohne Erregung von Verdacht

Shadow-Admins tauchen nicht in Reports auf

Regulatorik fordert Review:
ISO 27001 (A.8.2), NIS2 Art. 21 und BSI ORP4.A14 fordern dokumentierte Zugriffsrechte
→ Abweichung ist Major Finding im Audit

Verwaiste Accounts kosten Geld
→ binden Lizenzen

Ein Tiering-Konzept ohne regelmäßiges Account-Review ist wie ein Hochsicherheitsschloss mit unbekannter Anzahl verlorener Schlüssel

Finding #9 – PIM als Tiering-Ansatz in Entra ID / M365

Nicht „Brauchen wir PIM?“ – Sondern: „In welchen Tier gehört diese Rolle?“

<p>TIER 0</p> <p>Control Plane</p>	<p>Identitäts- & Sicherheitsebene</p> <p><i>Volle Kontrolle über Identitäten, Conditional Access & Rollenarchitektur</i></p> <p>Global Admin Privileged Role Admin Security Admin Conditional Access Admin Privileged Auth Admin Authentication Policy Admin</p>	<p>SCHUTZMECHANISMEN</p> <ul style="list-style-type: none"> FIDO2 / Windows Hello – phishing-resistente MFA Pflicht Dedizierte Admin-Workstation – gehärtetes PAW-Gerät Approval erforderlich – 4-Augen-Genehmigung via PIM Max. Aktivierungsdauer: 2 Stunden
<p>TIER 1</p> <p>Workload Admins</p>	<p>Dienst- & Workload-Ebene</p> <p><i>Administration von M365-Diensten – kein Zugriff auf Identitätsebene</i></p> <p>Exchange Admin Teams Admin SharePoint Admin Intune Admin Compliance Admin Application Admin</p>	<p>SCHUTZMECHANISMEN</p> <ul style="list-style-type: none"> MFA – Standard Authenticator App Justification – Begründung bei Aktivierung erforderlich Kein Approval – Self-Service-Aktivierung Max. Aktivierungsdauer: 8 Stunden
<p>TIER 2</p> <p>Helpdesk & Support</p>	<p>Operative Support-Ebene</p> <p><i>Tagesbetrieb – Scope via Administrative Units auf Standard-User begrenzt</i></p> <p>User Admin Helpdesk Admin Password Admin Operative Supportrollen</p>	<p>SCHUTZMECHANISMEN</p> <ul style="list-style-type: none"> MFA Pflicht – keine Ausnahmen PIM optional – permanent bei streng begrenztem Scope Administrative Units – kein Reset von Tier-0/1-Konten möglich

Undifferenziertes „alles in Approval“ ist kein Sicherheitsgewinn, es hemmt aktiv die Produktivität.

Fazit

Tiering ist kein Projekt – es ist eine Dauerdisziplin

TOPs der technischen Umsetzung

Kontentrennung

→ Strikte Tier-Separation – kein Crossing

Tier-0-Härtung

→ DC, PKI, Backup, Patchmanagement, Entra (Connect)

Kontinuierliches Review

→ Accounts, Shadow-Admins und PKI-Scans prüfen

Angriffsfläche minimieren

→ bekannte Vektoren schließen

TOPs für das Management

Compliance stärken

→ nachweisbare NIS2, ISO27001, BSI erfüllen

Wirtschaftlichkeit und Versicherungsschutz sichern

→ Nachweisbare Maßnahmen zur Risikominimierung

Betriebsstabilität stärken

→ erschwert die Ausweitung einzelner Angriffe

AD-Tiering ist die wichtigste Einzelinvestition in die IT-Sicherheitsarchitektur – mit direktem Compliance-Wert, messbarer Risikoreduktion und ohne zusätzliche Lizenzkosten.

360° Blick auf Ihre IT-Sicherheit





