„Die Spielregeln haben sich geändert!“

#AD-Check
#Schwachstellenanalyse
#Tiering Modell

Vortrag von Manfred Blum

Active Directory

Einführung Server 2000 am 17.02.2000

Für IT-Administratoren ging ein Traum in Erfüllung

Einfache Verwaltung der gesamten Struktur von einer zentralen Stelle aus.

Kerberos mit Single Sign On im gesamten Netzwerk.

Was war speziell neu?

- Verteilte Strukturen, hierarchische Struktur
- Strukturierte Ordnung über OUs
- Granulare Berechtigung im AD möglich
- DNS als zentraler Namensdienst
- Gruppenrichtlinien
- DFS

Was dem Admin lieb, ist dem Hacker recht!

Was damals beim Design nicht bedacht wurde:

- Keine 2-Faktor Authentifizierung vorgesehen
- Kennwort-Hashes werden lokal auf den Systemen zwischengespeichert, um ein SSON im Netz zu ermöglichen
- Kritische System-Benutzer (krbtgt)

→ ☠☠☠ AD ist DIE zentrale Stelle für Angriffe! ☠☠☠

Wie funktionieren üblicherweise Angriffe über AD?

Angriff über zum Beispiel Phishing

- Benutzer (Arbeitsstation) wird kompromittiert
- Hacker hat nun einen direkten Zugang mit den Benutzerdaten
- Recherche im AD z.B. mit Bloodhound.
  AD lesen kann JEDER Benutzer
- Rechteausweitung über CVEs
- Angreifen von (lokalen) Admin-Credentials (Hash) über kompromittierte Programme

Angriff über zum Beispiel Phishing

- Mit lokalen Admin-Rechten ist ein Zugriff auf die LSA als System möglich. Hier liegen weitere Hashes zum Beispiel von Domänen-Admins vor (Mimikatz)

- Mit dem Domänen-Admin steht dann die gesamte Domäne zur Verfügung. Er kann auch verwendet werden um sogenannte „Golden Tickets“ auszustellen, mit denen jederzeit weitere Zugriffstickets über Kerberos ausgestellt werden können, selbst für nicht existierende Benutzer

Exkurse:

Was ist Kerberos?

Was ist Kerberos?

- Authentifizierungssystem
- Bietet Single Sign On
- Kerberos Distribution Center erteilt nach einer Authentifizierung Tickets
  Authentication Server (AS) und Ticket Granting Server (TGS). Läuft auf dem Domaincontroller
- Weitere Authentifizierungen geschehen mit diesen Tickets
- Tickets haben eine Laufzeit von mehreren Stunden, können aber auch länger laufen (10 Jahre „Golden Ticket“)

Was tun?

Was tun?

Hoffen, dass man für Angriffe uninteressant ist!

Hoffen, dass es nur ANDERE trifft!

Agieren anstatt reagieren!

Organisatorische und technische Maßnahmen ergreifen!

Organisatorische Maßnahmen

- Ausmustern nicht mehr aktueller Betriebssysteme
- Löschen unbenutzter Computer- und Benutzer-Accounts
- Administrative Benutzer auf das Minimum beschränken
- „Administrator“ nicht verwenden
- Prinzipiell KEINE administrativen Anmeldungen auf untergeordneten Systemen hinterlassen „Admin-Tier-Modell“

IT ENTLASTER

Organisatorische Maßnahmen

- KEINE lokalen Admin-Rechte normalen Benutzern vergeben (Chef Problem, IT-Admin Problem)
- Regelmäßiges Ändern der Admin-Kennwörter
- Keine Kennwörter im Klartext hinterlegen
- Nur unbedingt nötige Rechte vergeben
- Kontrolle der Maßnahmen

Technische Maßnahmen

- Firewall, die unbefugte oder ungewöhnliche Zugriffe verhindert
- Aktueller Virenscanner und Mailfilter
- Updates, Updates, Updates
- Umsetzung des Admin-Tier Modell
- Individuelle Admin-Kennwörter auf allen Systemen (LAPS)

IT ENTLASTER

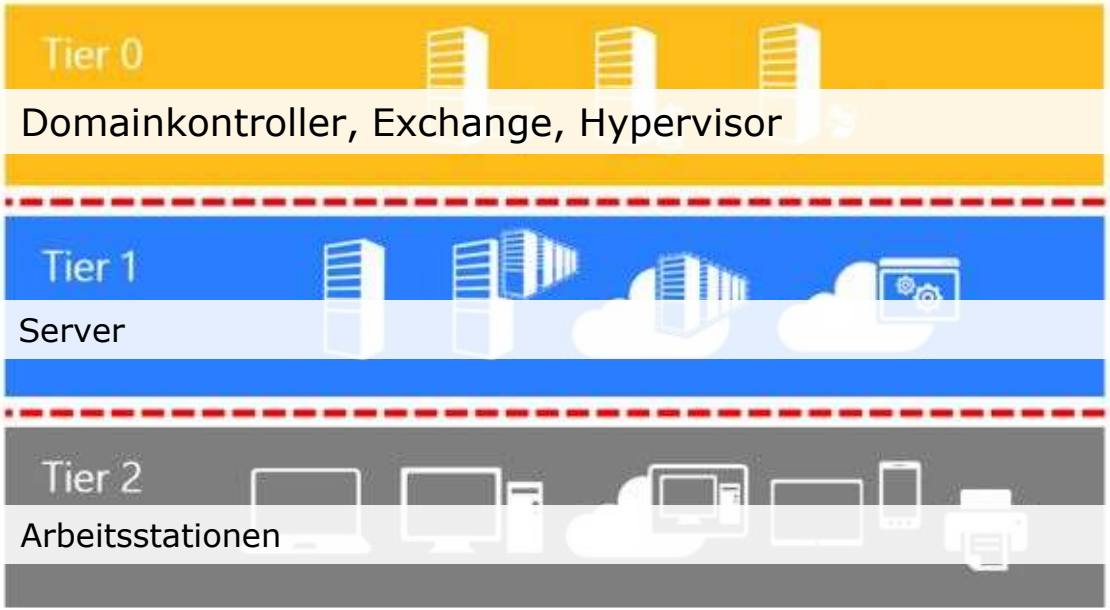
Technische Maßnahmen

- Backups mit Kontrolle *(Kein Backup, kein Mitleid)*
- Regelmäßige Änderung des KRBTGT Kennworts
- AD-Audits regelmäßig durchführen
- Prüfen der Systeme auf CVEs und Netzwerke auf ungewöhnliche Vorgänge
- Netzwerksegmentierung über Firewalls (nicht nur Router /Switche)

Das Admin Tier Modell

Admin Tier Modell

Auftrennung der Computer im AD in administrative Bereiche



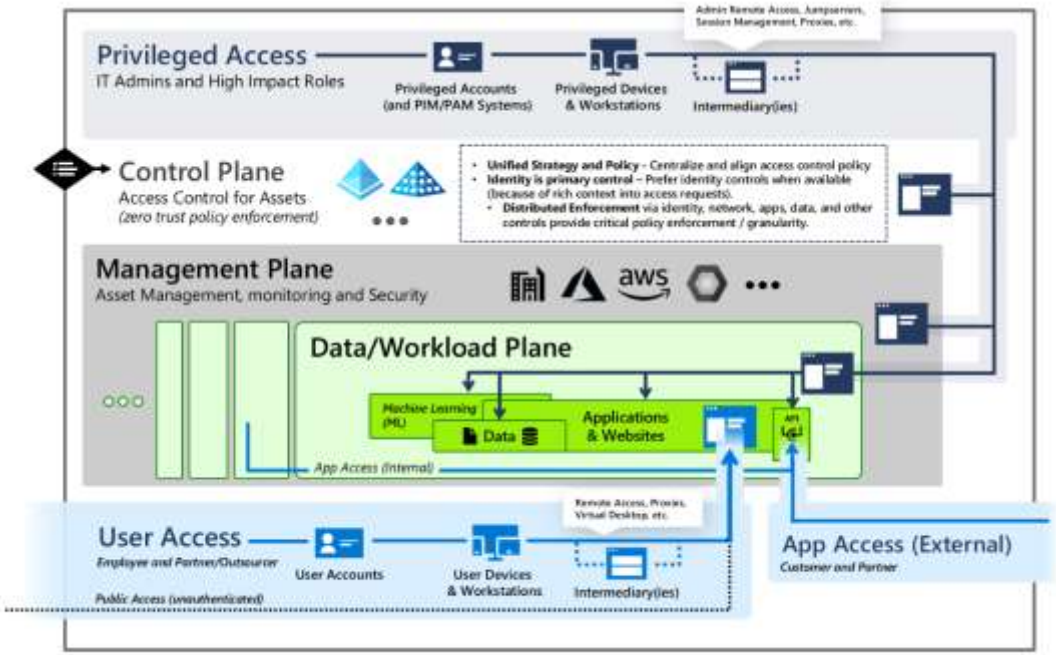
Hilfsmittel:

Unterstützung der Maßnahmen über GPOs

PAW(Privilegierte Administrator Workstation)

⚠ Keine Anmeldung von Tier 0 berechtigten Personen auf einer untergeordneten Ebene, damit diese Zugangsdaten dort nicht abgegriffen werden können!

Erweiterung des Admin-Tier Modell



https://learn.microsoft.com/de-de/security/privileged-access-workstations/privileged-access-access-model

Fazit

Fazit

Sicherheit ist kein Selbstläufer, der Schaden bei einer Kompromittierung ist extrem groß

Zero Trust – Hinterfragen Sie alle benötigten Rechte in Ihrem System

IT-Sicherheit ist nicht bequem und kostet Geld

IT-Sicherheit muss im Budget berücksichtigt werden

Machen Sie Ihre IT-Sicherheit zur

CHEFSACHE

Vielen Dank