Active Directory / Azure

Zum Leiden aller trägt jedes Unternehmen irgendwo ein Microsoft AD mit sich herum.
Seit etwa 2018 sollte dies Azure AD / Exchange Online heißen, je nachdem wie fähig ein Betriebsrat ist...
Seit etwa 2022 sollte dies Entra ID heißen, je nachdem ob man 2018 aufgepasst hat oder nicht.

- BSI-Modell 3-tier-Admins
- ExecutionPolicy bei Domänenscripts
- Azure Brainstorming

BSI-Modell 3-tier-Admins

Das BSI empfiehlt, den globalen Administrator abzuschaffen und durch eine 3-Tier-Variante zu ersetzen.
Also Domänenadmin rechtemäßig von Client-Admin und Server-Admin zu trennen.

Das klingt erst mal recht nett und hilfreich. Ist es sicher auch, ich sehe da aber einige Probleme bei.

1. Man muss das Konstrukt konsequent durchsetzen. Es kommen ja immer mal wieder Funktionen hinzu. Mal baut man Server auf, mal hat man mehr Systeme. Da gibt es immer mal ein System, dass genau dem Muster nicht folgt oder es einfach so granular nicht unterscheiden kann. Die haben wegen der ganzen Sicherheitslücken sicher kein LDAP-Zugriff, haben also wieder extra-Admins - außerhalb des Modells. Wie soll man auch einen admsrv auf eine Firewall ausweiten, die man nicht am LDAP hat, weil die REST-API die LDAP-Zugangsdaten ungefiltert an alle Anfragenden brüllt? (side-eye auf Watchguard) Deswegen hat man sowas nicht am LDAP, dafür mit anderen Kennwörtern. Aber BSI-3-tier ist nun mal eben im LDAP, wenn nicht exakt so am Gerät dupliziert.
2. Einzelaccounts sammeln Berechtigungen. Das ist das gleiche wie mit Azubis, die im Laufe von drei Jahren durch ganze Firmen wandern. Wer hat die ausgeweiteten Rechte? Richtig – der Azubi, nicht der Sysadmin.
   Dem Domänenadmin wird immer mehr hineingeworfen, weil er laut dem Modell ja auch für viel zuständig ist. So sammelt genau der Domänenadmin immer weitere Rechte, die dann wieder gegen das Modell stoßen.
3. Unbequemlichkeit macht faul:
   Sicherheit ist unbequem, auch in dem Fall. Für lokale Admintasks auf dem PC erst einmal Client-Admin-Passwörter in die UAC einzutragen, nervt. So gibt es sicher einige Personen, deren erster Task mit dem Client-Admin ist erst mal dem eigenen Domänenaccount auf dem eigenen PC Adminrechte zu geben.
4. Einzelne Programme gehen von User-Adminrechten aus und kommen mit Domänengebundenen Admins, die zufällig auf die Maschine Zugriff haben, nicht immer klar. Ein großer Anwärter dafür sind zum Beispiel die Microsoft PowerToys, die für einige Funktionen Administrationszugriff benötigen und - einmal eingearbeitet in die Funktionen - für normale Nutzer und nicht nur für Admins irgendwann nicht mehr zu missen sind.
5. Wer hat die Hoheit über den verbliebenen Global Admin? Richtig: Der IT-Dienstleister oder derjenige, der das Modell eingeführt hat. Der wird diesen Global Admin entweder gehäuft nutzen, oder eben nicht in seinen Berechtigungen beschnitten haben - also das Modell nicht in Gänze umgesetzt haben, sondern nur für alle anderen erweitert haben.

> Im Endeffekt sollte man Dingen wie 2-Faktor-Authentifizierung deutlich mehr Beachtung schenken als diesem BSI-Modell. Klar, es trennt die Rechte und damit (hoffentlich) die Ebenen die eine Ransomware befällt, aber für sonderlich sicher halte ich es nicht, weil es mit

> der Zeit verwässert wird.

Warum nicht 20-Tier-Modell?

Das ganze Modell ist schön und gut, bis man sieht wie viel ein Domänenadmin macht. Damit muss man klarkommen, die IT ist ziemlich zentral.

Was also tun? die drei Ebenen sind nicht fix, man kann sicherlich Rechte zwischen dem einen zu dem anderen schieben. Zum Beispiel die Exchange Management Shell, wenn man sie denn per Remote-Shell irgendwo aufmacht als Serveradmin deklarieren, während die Mailverwaltung im adminportal von Microsoft (die zurückgebliebenen nennen das noch Exchange Control Panel) noch Domänenadmin bleibt...

Ist völlig frei. In meinen Augen.

Problematisch wirds, wenn man das in noch mehr Accounts unterteilt, weil die menschliche Psyche dann wieder die gleichen Kennwörter verwendet und ich habe noch nie ein System gesehen, dass Passwörter zwischen den Benutzern vergleicht.
Was also bei >3 Tier passieren wird, ist dass selbst admins gleiche Kennwörter setzen, was den ganzen Zweck von feiner unterteilten Rechten zunichte macht.

Ich sehe das Modell also recht statisch als 3-Tier an.

ExecutionPolicy bei Domänenscripts

Scheinbar hängen manche gerade an dem Bedarf die ExecutionPolicy für Scripts (z.B. Bitlocker Einführung etc) zu ändern.

Genau dafür ist der Scope Process eigentlich da...

Siehe Chocolatey

```
Set-ExecutionPolicy Bypass -Scope Process -Force;
[System.Net.ServicePointManager]::SecurityProtocol =
[System.Net.ServicePointManager]::SecurityProtocol -bor 3072; iex ((New-Object
System.Net.WebClient).DownloadString('https://community.chocolatey.org/install.ps1'))
```

Sprich: Die Powershell wird als Admin ausgeführt (was im Falle einer GPO ja auch so wäre), setzt die Policy im Scope Process und lädt ein Powershellscript aus dem Netz.

Kein Heckmeck, mit Batchscripts die Policy setzen und danach andere Powershellscripts starten. Einfach direkt in der GPO Policy auf Scope Process anpassen und Script ausm SYSVOL starten...

Scope Process bedeutet ja, dass sie für diese Shellsitzung gilt und fertig...

Eigentlich nichts, woran man groß hängen müsste.

Richtiger wäre es, die Scripts mit der Domänen-CA zu signieren, ist aber halt die Frage wie viel Zeit man da hereinstecken möchte und ob man als Dienstleister auf Zeit spielt, weil man die ja berechnen kann, oder nicht.

Azure Brainstorming

Azure AD sei funktionsmäßig nicht gleichzusetzen mit OnPrem, auf genauere Nachfrage was genau die Einschränkungen wären gibt es aber kaum einen technischen Grund.

> Fragt man nach Beispielen gibt es keinen technischen Grund nicht Fullcloud gehen zu können. Scheitern tut es an veralteten Betriebsrats-Regularien, oder daran, dass die Geschäftsführung nicht gegen eingesparte Lohn-Zeitkosten gegenrechnet oder einen sehr hohen Wert auf Quick-Wins legt...
> Azure Transitionen sind ein kostenintensiver Slow-Win, was gehen die Schnelllebigkeit heutzutage geht. Das muss auch finanziell verstanden werden.

1:1 Transition immer teurer

Azure und Microsoft Cloud sollte immer ein SaaS Umstieg bedeuten. 1:1 Transition von Rechenzentren ist möglich, resultiert aber in weit höheren Kosten, wegen dedizierten Ressourcen.

Daher sollte Cloud Einstieg immer mit SaaS Umstieg einhergehen.

Funktionseinschränkungen

Thema Anonyme Relays

Anonyme Relays (z. B. für Drucker) sind in Exchange Online nicht vorhanden. Alternative ist ein Cloud-Server mit aktivierter Mailfunktion.
Wenn wir beim Thema Drucker bleiben, bedeutet Cloud Umstieg also ein lizenziertes Scan-Postfach, was aber im Umkehrschluss bedeutet, dass man Drucker braucht, die mehr als nur anonyme Anmeldungen können.