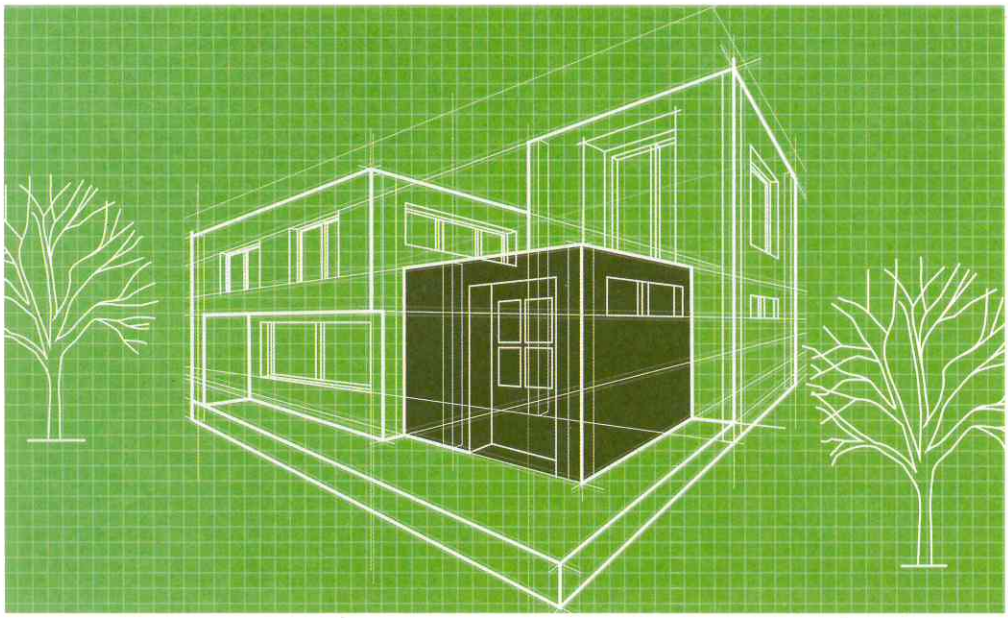


Active Directory mit dem Schichtenmodell schützen

Das Active Directory nur gegen Angriffe zu härten, reicht nicht aus. Microsofts Sicherheitskonzept zum Administrieren der IT-Infrastruktur, das Enterprise Access Model (Tiering-Modell), soll Angreifer daran hindern, sich nach dem Eindringen im AD auszubreiten und ihre Zugriffsrechte auszuweiten. Das neue Tutorial zeigt, wie man es umsetzt.

Von Hagen Molzer

In den in iX erschienenen Artikeln zur Sicherheit im Active-Directory-Umfeld wurden bereits viele wichtige Maßnahmen zur Absicherung einer Active-Directory-Domäne behandelt. Diese umfassen zum Beispiel das Aufspüren und Beheben von Schwachstellen, die im Laufe der Jahre durch unzureichende Administration entstanden sind, die Erhöhung der Qualität der Benutzerpasswörter oder das Implementieren von Werkzeugen zur Überwachung und Angriffserkennung im AD.

Die Königsdisziplin ist aber vermutlich die Entwicklung und Einführung eines Konzepts zur sicheren Administration der IT-Infrastruktur. Microsoft schlägt hierfür ein Schichtenmodell vor, das Tiering-Modell oder mittlerweile Enterprise Access Model (siehe ix.de/zjgm): ein grundlegendes Konzept, um die Active-Directory-Umgebung und gegebenenfalls weitere Teile der Infrastruktur vor diversen klassischen Schwachstellen zu schützen, die beim Administrieren entstehen können.

Abgeschottete Adminrechte

Die Grundidee ist, dass es einem Angreifer durch strikte Aufteilung der Rechte und Zugriffe von Administratoren erschwert wird, seine Berechtigungen im AD auszuweiten und sich dort auszubreiten. Die Kompromittierung eines Client-Administrators beispielsweise hilft dem Angreifer dann nicht, die regulären Server- oder Domänenadministratoren ebenfalls zu kompromittieren.

Wenn ein Angreifer auf ein Windows-System gelangt, kann er in der Regel andere an diesem System angemeldete Benutzer kompromittieren. Erlangt er zum Beispiel lokale administrative Rechte auf einem Terminalserver, nachdem er eine Privilege-Escalation-Schwachstelle ausgenutzt hat, könnte er einen Serveradministrator kompromittieren, der auch bei vielen anderen Servern Administratorrechte hat.

Der Angreifer kann hierzu eventuell mit einem Werkzeug wie Mimikatz (siehe ix.de/zjgm) die Zugangsdaten des Serveradministrators aus dem lsass.exe-Prozess auslesen oder einen Scheduled Task anlegen, der im Kontext jedes Benutzers ausgeführt wird, der sich auf dem Terminalserver einloggt. Der Kreativität des Angreifers sind kaum Grenzen gesetzt, da er mit den lokalen administrativen Rechten beliebige Manipulationen auf dem Terminalserver durchführen kann. Nach der Kompromittierung des Serveradministrators ist der Angreifer den Kronjuwelen seines Opfers, beispielsweise dem Domänencontroller, schon einen Schritt näher.

Hat der Serveradministrator auch noch administrative Kontrolle über die Hypervisor-Umgebung, in der die Domänencontroller virtualisiert werden, über den Backup-Server, auf dem die Backups der Domänencontroller oder PKI-Server gespeichert sind, oder über den WSUS-Server (Windows Server Update Services), der Updates an die Domänencontroller verteilt, ist der Angreifer nur noch einen Schritt davon entfernt, die Domäne vollständig zu übernehmen.

Auch der „Credential Theft Shuffle" wäre eine Möglichkeit, mit der ein Angreifer seine Privilegien im AD schrittweise so

iX-TRACT

- Um eine Active-Directory-Domäne zu schützen, braucht es mehr als Absicherungs- und Härtungsmaßnahmen. Microsoft hat ein Sicherheitskonzept entwickelt, das auf der Abschottung privilegierter Zugriffsrechte beruht.
- Grundlage des Konzepts ist die Festlegung genau definierter Tiers, deren Admins mit unterschiedlichen Rechten ausgestattet und voneinander isoliert sind.
- Die Einführung des Tiering-Modells lässt sich in verschiedenen Abstufungen realisieren – von sehr aufwendig und sehr sicher bis akzeptabler und bezahlbarer Kompromiss.

Tutorialinhalt

Teil 1: Grundlagen – Design, Klassifizierung und Implementierung der Tiers

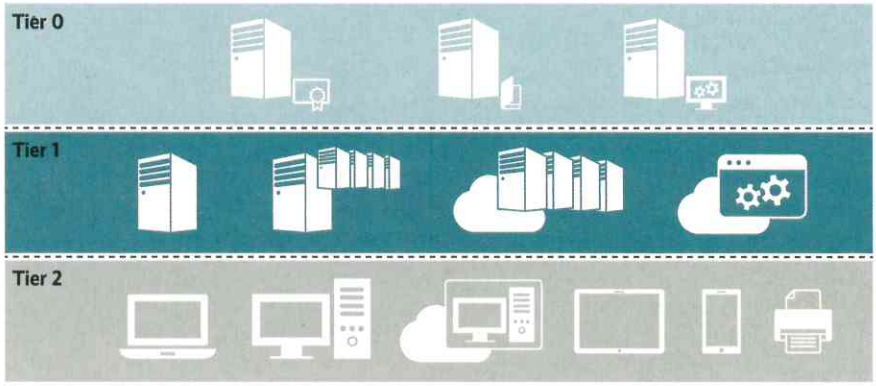
Teil 2: Privileged Access Workstations (PAW) – Absicherung, Werkzeuge und administrative Zugriffe

Teil 3: Privileged Account/Access Management (PAM), AD-Struktur, Netzwerksegmentierung

Quelle: Microsoft

Evolution from the legacy AD tier model

The enterprise access model supersedes and replaces the legacy tier model that was focused on containing unauthorized escalation of privilege in an on-premises Windows Server Active Directory environment.



Die frühe Version des Tiering-Modells fußt auf der Einteilung in voneinander abgegrenzte Tiers, die kein „Überspringen" erlauben (Abb. 1).

lange erweitern kann, bis er sein Ziel erreicht hat. Geprägt wurde dieser Begriff von Sean Metcalf, Betreiber der Website adsecurity.org und Koryphäe im AD-Security-Umfeld, in seinem Blogeintrag „Attack Methods for Gaining Domain Admin Rights in Active Directory" (siehe ix.de/zjgm). Dort vergleicht er diesen Angriff mit einem Tanz, bei dem sich ein Angreifer in verschiedene Richtungen bewegt und mit den erbeuteten Anmeldedaten peu à peu seine Berechtigungen erweitert.

Wenig Vertrauen nach Kompromittierung

Hat ein Angreifer eine Domäne einmal vollständig kompromittiert, kann man ihr in den meisten Fällen nie wieder vollständig vertrauen. Eine Chance, sie zu retten und nicht vollständig neu aufzusetzen, besteht nur, wenn man die Kompromittierung sehr schnell bemerkt, den Zeitpunkt und den Weg der Kompromittierung zweifelsfrei bestimmen kann und über Backups vom Zeitpunkt vor der Kompromittierung verfügt, mit denen man die Domäne wiederherstellen kann.

Umso wichtiger ist es, die Domäne vor der vollständigen Übernahme durch die Angreifer zu schützen. Die Umsetzung eines Tiering-Modells ist hierfür ein sehr mächtiges Mittel. Die Grundidee ist die Einteilung aller Systeme der Domäne in (typischerweise) drei Ebenen, sogenannte Tiers:

- Tier 0: Domänencontroller, PKI und weitere sicherheitskritische Systeme;
- Tier 1: Server;
- Tier 2: Clients.

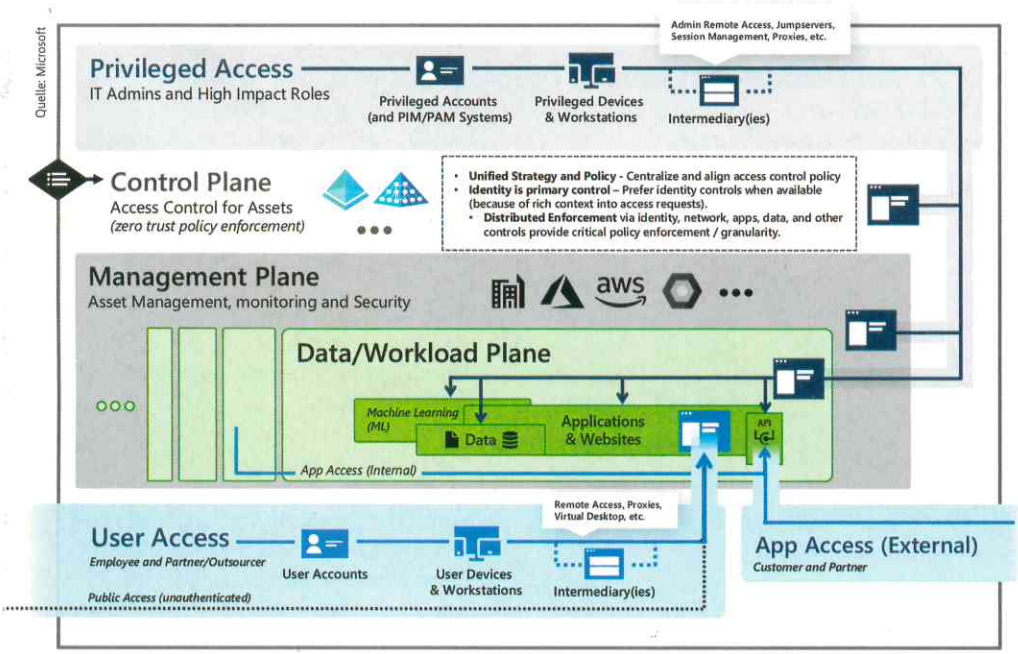
Auch wenn es irritierend ist, ist beim Tiering-Modell die umgekehrte numerische Reihenfolge zu beachten: Tier 0 ist die „höchste Tier" trotz niedrigster Nummer.

Dann wird die Administration der Systeme so angepasst, dass die Kompromittierung einer niedrigeren Ebene nicht die Kompromittierung einer höheren Ebene erleichtert. Das Tiering-Modell wurde von Microsoft lange wie in Abbildung 1 dargestellt.

Vor einiger Zeit wurde es weiterentwickelt und umbenannt. Das neue Enterprise Access Model, von Microsoft dargestellt wie in Abbildung 2, ist nun deutlich ausgefeilter, die Grundidee blieb.

Weiterhin teilt man die verschiedenen Systeme in Kategorien ein und sichert deren Administration ab. Die detailreichere Ausgestaltung berücksichtigt laut Microsoft moderne Anforderungen eines Unternehmens, etwa das Einbeziehen lokaler Standorte, mehrerer Clouds, interner oder externer Benutzerzugriffe, etwa für Nutzer von Partner- oder Kundenunternehmen, und mehr.

Quelle: Microsoft



Privileged Access
Enables IT administrators and other high impact roles to access to sensitive systems and data. *Stronger security for higher impact accounts*

Control and Management Planes
Provide unified access and management for workloads and assets *(and provide attackers shortcut for illicit objectives)*

Data/Workloads
Create and store business value in
- Business processes (in apps/workloads)
- Intellectual property (in data and apps)

User and App Access
How employees, partners, and customers access these resources

Die Weiterentwicklung des alten Modells berücksichtigt moderne Unternehmensanforderungen, etwa das Einbinden Externer oder mehrerer Cloud-Dienste (Abb. 2).

In diesem Artikel wird die ursprüngliche Bezeichnung der Systemkategorien und Maßnahmen verwendet, da diese leichter verständlich sind und sich das Prinzip kaum verändert hat.

Auswirkung auf Administration

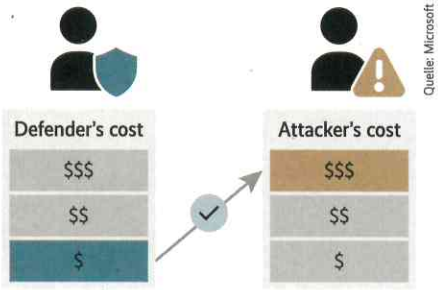
Die Einführung eines Tiering-Modells hat große Auswirkungen auf die Arbeitsweise und die Zugriffsrechte der Administratoren. Es legt fest, wie und von wo zukünftig administriert werden kann. Gegebenenfalls kann es Kosten durch zusätzliche Hardware und Softwarelizenzen sowie durch eine höhere Komplexität der Administration verursachen.

Aus diesem Grund gibt es auch nicht das eine Tiering-Modell, das für alle Umgebungen passt, vielmehr muss man bei der Umsetzung typischerweise Kompromisse eingehen. Deshalb sollten schon in der Designphase neben den Sicherheitsanforderungen an die Umgebung auch das Budget und die Aufwandsbereitschaft des Unternehmens berücksichtigt werden. Ziel ist es, mit geringen eigenen Investitionen den Aufwand für Angreifer überproportional zu erhöhen, sodass sie sich im besten Fall ein leichteres Opfer suchen. Microsoft stellt dieses Prinzip in Abbildung 3 anschaulich dar.

Dieses dreiteilige Tutorial beschreibt die verschiedenen Möglichkeiten der Implementierung, erläutert erforderliche Kompromisse und ihre Restrisiken und stellt die technischen Maßnahmen dar.

Der erste Schritt – die Designphase

Die Designphase beginnt mit der Überlegung, in wie viele Tiers man die Systeme der IT-Infrastruktur beziehungsweise der Domäne einteilt. Microsoft sieht drei Tiers vor, dies kann aber an die tatsächlichen Gegebenheiten angepasst werden.



Eine Strategie beim Tiering-Modell: mit wenig Aufwand die Kosten für den Angreifer so hochzutreiben, dass sich der Einbruch für ihn nicht lohnt und er sich einfachere Ziele sucht (Abb. 3).

In einer DMZ-Domäne beispielsweise ist Tier 2 unter Umständen nicht sinnvoll, da es hier vielleicht keine Clients gibt. Auch könnte Tier 1 in Tier 1.1 (Server der zentralen Infrastruktur) und Tier 1.2 (Server für Entwicklung/Spezialanwendungen) aufgesplittet werden, wenn auf einem Teil der Server eine größere Anzahl an Entwicklern oder externen Dienstleistern administrative Rechte bekommt und dies aus Sicherheitsgründen abgetrennt werden soll.

Anschließend werden die Systeme der IT-Infrastruktur oder der Domäne den Tiers zugeteilt. Die folgende Liste enthält typische Systeme einer IT-Landschaft:

- Domänencontroller;
- ADFS-Server (Active Directory Federation Services), Azure-AD-Connect-Server;
- Virtualisierungshardware/-software;
- Privileged Access Workstations (PAW);
- zentrale Passwortverwaltung;
- Monitoringsystem (z. B. SCOM);
- Softwareverteilung (z. B. SCCM, WSUS);
- Backup-System/Storage;
- Antivirenlösung, Endpoint Detection and Response (EDR);
- PKI;
- Terminalserver;
- Anwendungsserver;
- Clients;
- gegebenenfalls Infrastruktur in der Cloud.

In der Designphase gilt es auch zu entscheiden, ob neben den domänenintegrierten Systemen zusätzliche Systeme in das Tiering-Konzept einzubeziehen sind, beispielsweise

- Linux-Systeme;
- Infrastrukturhardware (zum Beispiel Netzwerkhardware);
- Kameras;
- Schließsysteme;
- Cloud-Benutzer (beispielsweise der Global Admin im Azure Active Directory);
- weitere Cloud-Provider (etwa Cloud-Proxy, Mail-Security).

In die Entscheidung sollte unter anderem einfließen, wie sich Systeme und Nutzer bei der Anmeldung authentifizieren: ob sie bereits an das Active Directory angebunden sind und wie hoch der Schutzbedarf für diese Systeme oder Benutzer ist. Je höher die Bedeutung der Systeme aus Sicherheitssicht ist, desto wichtiger ist ihre Einbindung in das Tiering-Konzept.

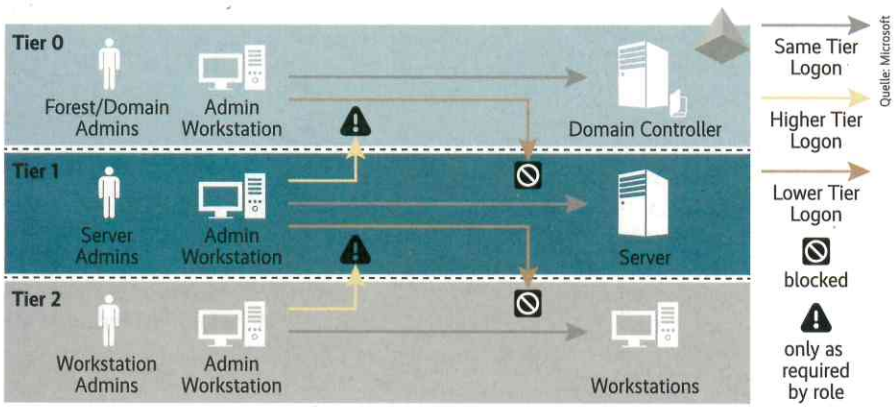
Strikte Trennung der Rollen

Im nächsten Schritt ist eine strikte Rollen- und Kontentrennung der administrativen Tier-Benutzer zu konzipieren. Eine Tier-übergreifende Berechtigungsvergabe für administrative Benutzer darf es nicht geben. Dies hat zur Folge, dass etwa ein Administrator, der Systeme in allen drei Tiers administriert, zukünftig mindestens vier verschiedene Benutzerkonten benötigt:

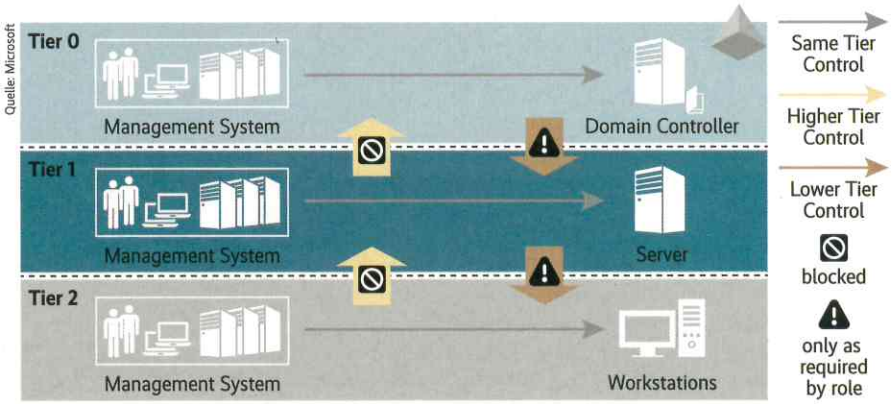
- reguläres Benutzerkonto: michael.mueller (damit werden beispielsweise E-Mails gelesen und im Internet gesurft; keinerlei administrative Rechte);
- Tier-0-Administrator: T0-michael.mueller;
- Tier-1-Administrator: T1-michael.mueller;
- Tier-2-Administrator: T2-michael.mueller.

Die Namensgebung bei den zukünftigen administrativen Konten sollte die Tier-Zugehörigkeit widerspiegeln. Das erleichtert das Erkennen von Verstößen gegen das Tiering-Modell erheblich und vereinfacht dessen Implementierung.

Die bisherigen Adminkonten sind zwingend zu deaktivieren und zu löschen, sobald die neuen Tier-Adminkonten genutzt werden und funktionieren. Versäumt man es, können hier „Leichen“



Die Adminanmeldungen und -zugriffe auf andere Tiers sind stark reglementiert und in eine Richtung gänzlich blockiert (Abb. 4).



Ebenso wie die Zugriffe sind die Berechtigungsvergaben über die Tiers hinaus eingeschränkt oder vollständig unterbunden (Abb. 5).

zurückbleiben, die das Tiering-Modell wieder aushebeln.

Die Trennung der Tier-Adminkonten sollen zum einen Tier-übergreifende Benutzeranmeldungen verhindern, wie in Abbildung 4 dargestellt. Der Zugriff von höheren in die niedrigeren Tiers wird komplett blockiert. Zugriff von niedrigeren in die höheren Tiers wird nur gestattet, wenn es die Rolle es erfordert (zum Beispiel Zugriff aller Benutzer auf Dateifreigaben der Domänencontroller zum Lesen der Gruppenrichtlinien).

Zum anderen soll die strikte Trennung eine Tier-übergreifende Berechtigungsvergabe verhindern. Die Details sind in Abbildung 5 dargestellt.

Anschließend muss festgelegt werden, wie viel Aufwand für den Schutz dieser neuen hochprivilegierten Identitäten betrieben wird. Wenn die Administratoren ihre neuen Tier-Adminkonten auf ihren regulären Clients – neben ihrem regulären Benutzerkonto – nutzen, ist nicht viel gewonnen. Gelingt es einem Angreifer, den regulären Client eines Administrators zu kompromittieren, gibt es etliche Möglichkeiten, auch das darauf verwendete Tier-Adminkonto zu kompromittieren. Es seien hier zum Beispiel Software-Keylogger, Screen-Monitoring-Software oder wieder die lsass.exe und das Werkzeug Mimikatz genannt.

Die Bausteine des Tiering-Modells

Die sicherste Variante ist es, für die Benutzer mit Tier-Adminkonten speziell geschützte Privileged Access Workstations (PAWs) einzurichten. Dabei handelt es sich um separate Geräte (Workstations oder Notebooks), die ausschließlich für die Administration verwendet werden und an denen sich ausschließlich Tier-Adminkonten anmelden können.

Aus Kostengründen scheint es naheliegend, den regulären Client und die PAW auf einem Computer zu vereinen, zum Beispiel mithilfe von Virtualisierung. Hier gilt es aber, einige Fallstricke zu vermeiden, damit man sich nicht unbemerkt größere Sicherheitslöcher in sein administratives Konzept reißt. Auch dies wird später noch ausführlich behandelt.

Eine weitere Variante ist es, ein Privileged Access Management (PAM) in das administrative Konzept zu integrieren. Es kann dabei helfen, die Zahl der zukünftig extra zu beschaffenden PAWs zu reduzieren, und vermeidet, dass sich die Administratoren die vielen Passwörter der neuen Tier-Adminkonten merken müssen. Zudem kann die Sicherheit durch Mehr-Faktor-Authentifizierung (MFA) und häufige, automatisierte Passwortwechsel erhöht werden. Auf PAWs, ihre Absicherung und PAM-Lösungen geht diese Artikelreihe später noch im Detail ein.

Die mittels des Tiering-Modells erreichte klare Trennung der Systeme und die Definition, welche Person administrativen Zugriff auf welche Systeme haben soll, macht es einfacher, eine strikt filternde Netzwerksegmentierung einzurichten und Zugriff auf die Managementports der Systeme nur noch von da zu erlauben, wo sie auch wirklich benötigt werden. Dazu später mehr, wenn es um Netzwerksegmentierung und Einschränkung der administrativen Zugriffe geht.

Schritt für Schritt vorgehen

Nachdem nun alle wichtigen Kernkomponenten des Tiering-Modells einmal angesprochen wurden, wird der geneigte Administrator vom potenziellen Aufwand des Gesamtprojekts womöglich eingeschüchtert sein und sich fragen, wie das alles neben dem regulären Tagesgeschäft umzusetzen ist. Je nach Größe der IT-Landschaft des Unternehmens und Zustand des bisherigen administrativen Konzepts zählt dieses Projekt sicher zu den größeren und aufwendigeren, aber auch dieser Elefant kann in Scheiben gegessen werden.

Zunächst sollte man Tier 0 absichern. Das hat den Vorteil, dass zunächst relativ wenige Systeme und Administratoren betroffen sind, nämlich nur die besonders hoch privilegierten. Dennoch führen die Maßnahmen direkt zu einem sehr hohen Sicherheitsgewinn, da dann die besonders kritischen Systeme geschützt sind.

Die Anzahl der technischen Anpassungen und der zu ändernden Arbeitsweisen der Administratoren ist also im Vergleich zu Tier 1 und Tier 2 überschaubar und das Administratorenteam kann Erfahrungen darin sammeln, was es bedeutet, das Konzept umzustellen und nach dem Tiering-Modell zu administrieren. Diese Erkenntnisse sind für die Umstellung der Administration von Tier 1 und 2 viel wert.

Unterschiedliche Implementierungsarten

Wie erwähnt gibt es kein universelles Tiering-Modell, sondern jedes Unternehmen muss für sich die passende Variante und entsprechende Kompromisse finden.

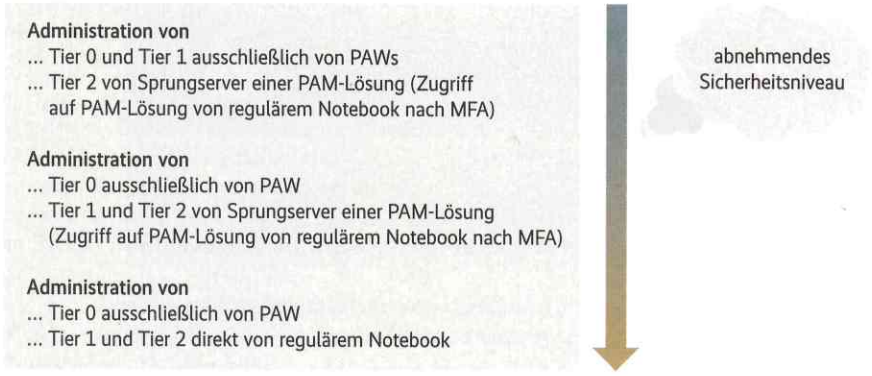
Bevor die verschiedenen Implementierungsarten behandelt werden, ist noch das „Assume Breach"-Szenario anzusprechen. Geht man davon aus, dass das AD bereits unwissentlich kompromittiert wurde, hilft es wenig, in der bestehenden produktiven Domäne die neuen Admin-Tierkonten anzulegen und zu verwenden. Der Angreifer verfügt über diverse Möglichkeiten, die neuen Identitäten zu kompromittieren und sich unerkannt in die neue Art der Administration einzugliedern.

Um das zu erschweren, kann man die Tier-Adminkonten und die PAWs nicht in der produktiven Domäne, sondern in einem neu zu schaffenden, getrennten administrativen Forest (Red oder Bastion Forest) anlegen und die Administration der produktiven Domäne dann ausschließlich aus diesem Red Forest durchführen.

Ein separater Admin-Forest?

Auch für dieses Prinzip gibt beziehungsweise gab es mit dem Enhanced Security Admin Environment (ESAE) einen Designvorschlag von Microsoft samt einigen technischen Features. Laut der Microsoft-Website wurde dieser Vorschlag durch die neuen und modernen Herangehensweisen „Privileged Access Strategy" und „Rapid Modernization Plan (RAMP)" als neue Standardempfehlung abgelöst. Microsoft weist jedoch darauf hin, dass es sich bei ESAE weiterhin um einen validen Ansatz handelt, zum Beispiel

- bei isolierten On-Premises-Umgebungen oder wenn der Einsatz von Cloud-



Die Umsetzung des Tiering-Modells lässt viel Spielraum nach oben und unten. Der Sicherheitsgewinn wächst mit dem betriebenen Aufwand (Abb. 6).

Technologien nicht möglich oder gewünscht ist,
- in stark regulierten Umgebungen oder
- wenn die Sicherheitsanforderungen besonders hoch sind beziehungsweise die Risikotoleranz besonders niedrig ist.

Die Umsetzung des Tiering-Modells nach ESAE mit einem separaten Admin-Forest ist die sicherste, aber auch die aufwendigste Variante. Typischerweise kommt sie dann zum Einsatz, wenn die Sicherheitsanforderungen besonders hoch oder die Unternehmen besonders groß sind. Dieses Modell ist insbesondere für Unternehmen interessant, die entweder eine hohe Anzahl interner Domänen oder Forests betreiben oder für Managed Service Provider (MSSPs), die viele Domänen ihrer Kunden betreuen.

Wird eine Vielzahl von Domänen ausgehend von einem Red Forest verwaltet, kann dies den Aufwand sogar reduzieren, da die Administratoren nur noch Accounts in dieser einen Red-Forest-Domäne benötigen und nicht einen Account in jeder verwalteten Domäne. Das ESAE- oder Red-Forest-Konzept ist allerdings so komplex, dass es den Rahmen dieser Artikelserie sprengen würde.

Tiering-Modell innerhalb der verwalteten Domäne

Die mit Abstand am häufigsten anzutreffende Variante ist die Umsetzung des Tiering-Modells in der bestehenden Domäne, das bedeutet, die Tier-Adminkonten und die PAWs oder das PAM befinden sich in der produktiven Domäne, die es zu administrieren gilt. Doch auch hier gibt es unterschiedliche Varianten, die ein höheres oder niedrigeres Sicherheitsniveau bieten.

Alle Varianten teilen die Objekte innerhalb des AD in die bereits angesprochenen (drei) Tiers auf. Dann muss entschieden werden, wie viel Aufwand man betreibt, um die Tier-Adminkonten zu schützen. Am sichersten ist es, die Tier-Adminkonten aller drei Tiers ausschließlich auf PAWs zu verwenden.

Etwas weniger sichere, aber kostengünstigere oder leichter umsetzbare Kompromisse sind viele vorstellbar. Abbildung 6 zeigt einige Beispiele.

Vorsicht jedoch vor einer zu pragmatischen Umsetzung. Das folgende Beispiel ist in Unternehmen öfter anzutreffen, berücksichtigt aber viele Risiken nicht angemessen: Alle Administratoren erhalten neben dem regulären Benutzerkonto einen zusätzlichen Administratoraccount, der vom regulären Notebook aus für die Administration aller Tiers verwendet wird (einschließlich Domänenadministratoraccounts). Das sind die Penetrationstests, die Spaß machen, denn es ist oft möglich, die Domäne noch vor dem Mittagessen das erste Mal zu kompromittieren.

Klassifizierung der Systeme in (drei) Tiers

Auch bei der Klassifizierung der Systeme in die einzelnen Tiers gibt es einiges zu beachten, damit das neue Konstrukt den gewünschten Sicherheitsgewinn bringt. Die Grundregel lautet: Ein System, das Kontrolle über ein anderes System hat, ist auf derselben Ebene oder höher anzusiedeln.

Es empfiehlt sich, den Top-down-Ansatz bei der Klassifizierung zu wählen und mit Tier 0 zu beginnen. Die typischerweise zu klassifizierenden Systeme wurden eingangs bereits aufgelistet. Bei genauerer Betrachtung ist die Klassifizierung aber nur bei wenigen dieser Systeme unstrittig.

So gehören die folgenden Systeme offenkundig zu Tier 0: Domänencontroller, ADFS-Server, Azure-AD-Connect-Server und PKI. Eindeutig zu Tier 1 gehören hingegen Anwendungsserver, während Clients unstrittig zu Tier 2 gehören. Bei den übrigen zentralen Systemen in der Liste wird es schon schwieriger und es stellen sich verschiedene Fragen:
- Virtualisierungshardware/-software: Werden hier Tier-0-Systeme virtualisiert?
- Privileged Access Workstations: Verwaltet eine PAW mehrere Tiers oder gibt es nach Tiers getrennte PAWs?
- Zentrale Passwortverwaltung: Die Passwörter welcher Tiers sind hier gespeichert und wer genau benötigt Zugriff?
- Monitoringsysteme (z. B. SCOM): Überwachen sie auch Tier-0-Systeme und ist eine Kontrolle über die überwachten Systeme möglich?
- Softwareverteilung (z. B. SCCM, WSUS): Werden auch Software- oder Windows-Updates an Tier-0-Systeme verteilt?
- Backup-System/Storage: Sind hier Tier-0-Systeme oder deren Daten gespeichert?
- Antivirenlösung, EDR: Ist hierüber administrative Kontrolle über Tier-0-Systeme möglich?

Wenn sich ein Unternehmen zum ersten Mal Gedanken über dieses Thema macht, kommt es typischerweise sehr schnell zu dem Schluss, dass viele zentrale Systeme zu Tier 0 gerechnet werden müssen. Dies zeigt, dass bislang viele Administratoren überprivilegiert waren, ohne sich dessen bewusst zu sein. Ein verbreitetes Beispiel verdeutlicht das:

Ein Unternehmen betreibt einen zentralen WSUS-Server, der Updates für alle Clients, Server und Domänencontroller bereitstellt. Die Freigabe der Updates sowie die Administration von WSUS und dem darunterliegenden Betriebssystem erfolgen durch die regulären Helpdesk-/Serveradministratoren. Ein Angreifer muss nur einen dieser Administratoren kompromittieren, um im nächsten Schritt durch Einschleusen eines schädlichen WSUS-Updates die Domänencontroller zu kompromittieren. Die Kompromittierung eines solchen Administrators ist häufig bedeutend einfacher als die eines Domänenadministrators, da diese Benutzerkonten auf einer Vielzahl leicht kompromittierbarer Systeme (wie regulärer Clients oder Server) verwendet werden.

Einfallstor Software-Update

Um ein schädliches WSUS-Update anzufertigen, kann ein Angreifer im Internet frei verfügbare Open-Source-Werkzeuge wie SharpWSUS nutzen. Mit wenigen Kommandozeilenaufrufen ist das Update

erstellt und genehmigt und der Angreifer muss nur noch auf den Update-Vorgang warten. Die Payload muss allerdings zwingend von Microsoft signiert sein. Aber auch das ist kein Problem, weil es dafür zum Beispiel die Programme psexec.exe, msiexec.exe oder msbuild.exe von Microsoft selbst gibt.

Vergleichbare Angriffswege lassen sich oft mit wenig Aufwand auch für andere Systeme der zuvor genannten Liste entwickeln. Zur Lösung dieses Problems gibt es drei Möglichkeiten.

Möglichkeit 1: Das zentrale System bekommt die höchste Klassifizierung der Systeme, die es kontrollieren kann (zum Beispiel Tier 0). Alle Administratoren, die Zugriff benötigen, erhalten ein Tier-0-Adminkonto und arbeiten damit nach Tier-0-Standards (beispielsweise von PAWs). Das ist eine sichere Lösung, weil sie eine strikte Trennung der Administration der Systeme nach Tiers implementiert und der Verwaltungszugriff auf das zentrale System über das Netzwerk einfach einschränkbar ist. Die Anzahl der zu Tier 0 gehörenden Adminkonten kann dabei aber stark anwachsen, was nicht unbedingt gewünscht ist und aufgrund der Anschaffung zahlreicher PAWs teuer werden kann.

Möglichkeit 2: Es werden mehrere Instanzen des zentralen Systems implementiert, getrennt nach Tiers, also etwa eine eigene Softwareverwaltung pro Tier. Auch dabei handelt es sich um eine sichere Lösung, da sie die Systeme strikt nach Tiers trennt und sich der Netzwerkzugriff auf die Remoteverwaltungsschnittstellen über das Netzwerk einfach einschränken lässt.

Doch auch hier ist der Nachteil, dass es schnell teuer werden kann, da gegebenenfalls zusätzliche Hard- und Software angeschafft werden muss und der Verwaltungsaufwand sich erhöht.

Möglichkeit 3: Diese Lösung versucht, einen Kompromiss zwischen Sicherheitsanforderungen und zusätzlichen Kosten zu finden. Sie kommt nur für Systeme infrage, die über eine umfangreiche RBAC (Role-based Access Control) verfügen. Es muss also möglich sein, die Berechtigungsvergabe innerhalb des zentralen Systems granular zu regeln. Dann kann man darüber nachdenken, das zentrale System als Tier-0-System zu klassifizieren, aber die Tier-1- und Tier-2-Adminkonten über die Berechtigungsvergabe auf den Systemen ihrer jeweiligen Ebene zu berechtigen.

Ein klassisches Beispiel dafür ist die Vergabe von Berechtigungen innerhalb des vCenter von VMware auf die VMs unterschiedlicher Tiers für die verschiedenen Tier-Benutzer. Dabei ist penibel darauf zu achten, dass zum Beispiel keine Tier-1- oder 2-Adminkonten Rechte auf Tier-0-Systemen erhalten. Hier fallen weniger Kosten für Hard- und Softwarelizenzen und ein geringerer Verwaltungsaufwand an als bei den zuvor genannten Möglichkeiten.

Nicht ohne rollenbasierte Zugriffskontrolle

Jedoch zählt zu den Nachteilen dieser Variante, dass Schwachstellen im System selbst beziehungsweise in RBAC die Systeme eines höheren Tier ausgehend von niedrigeren Tiers oder Tier-Benutzern gefährden. Schwachstellen dieser Art gab es in der Vergangenheit bereits in verschiedenen Produkten. Darüber hinaus ist das System netzwerkseitig schlechter isolierbar, da eine größere Anzahl von Administratoren niedrigerer Tiers Zugriff auf die Remoteverwaltungsschnittstellen benötigt. Außerdem ist es keine universelle Lösung, da nicht alle Systeme die granularen Rechteeinschränkungen ermöglichen.

Zum Thema Terminalserver sei darauf hingewiesen: Auch wenn Systeme der Kategorie Terminalserver das Wort Server im Namen tragen, sollten sie dennoch zwingend zu Tier 2 gezählt und wie Clients behandelt werden, wenn sie von regulären Benutzern genutzt werden.

Auf diese Server hat typischerweise eine große Anzahl an Benutzern Zugriff, es sind oft viele verschiedene Programme installiert, zudem sind die Terminalserver oft lange im Einsatz, sodass sich im Laufe der Zeit viele Schwachstellen ansammeln können. Ein Angreifer, dem es gelingt, lokale administrative Rechte darauf zu erlangen, kann auf einen Schlag eine Vielzahl angemeldeter Benutzer kompromittieren. Daher sollten sich hier niemals Administratoren aus der höheren Tier 1 und natürlich auch niemals aus Tier 0 anmelden. Dem Autor haben bei seinen Penetrationstests Privilege-Escalation-Schwachstellen in der Wald-und-Wiesen-Terminalserver- oder -Citrix-Umgebung schon unzählige Male als Ausgangspunkt für Angriffspfade gedient, um die Domäne zu kompromittieren. (ur@ix.de)

Quellen

Die erwähnten Microsoft-Artikel sowie der Blogartikel von Sean Metcalf sind über ix.de/zjgm zu finden.

HAGEN MOLZER

ist Leitender Berater bei der cirosec GmbH. In seinen Schwerpunktbereichen Active-Directory- und Windows-Betriebssystem-Sicherheit führt er Penetrationstests, Beratungsprojekte sowie Red-Team-Assessments durch.