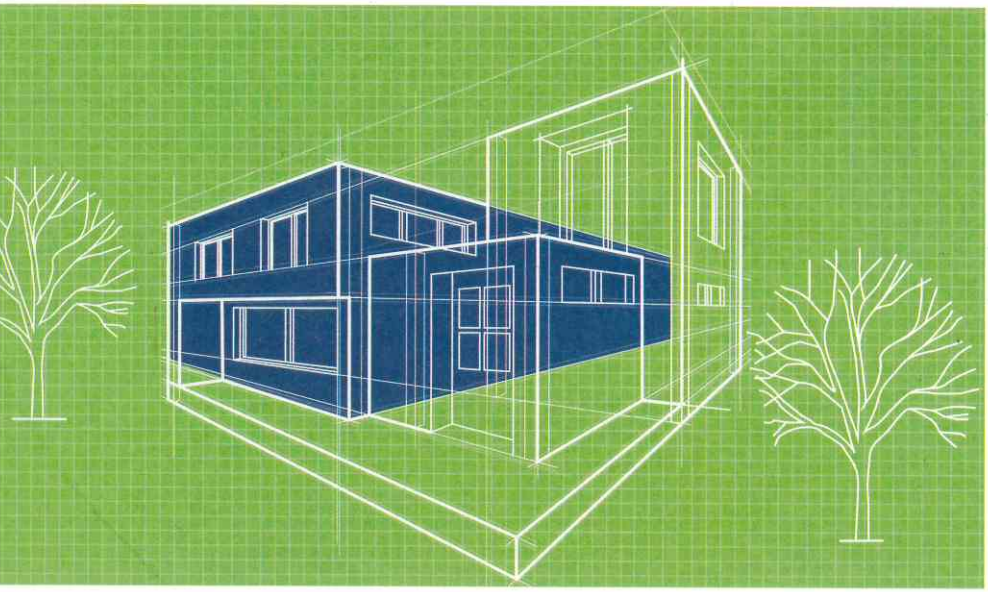


Privilegierte AD-Zugriffe managen

Der letzte Baustein einer sicheren Active-Directory-Infrastruktur besteht darin, Privileged Access Management in Microsofts Enterprise Access Model zu integrieren.

Von Hagen Molzer

Die Integration eines Privileged Access Management (PAM) in Microsofts Enterprise Access Model, vielen noch als Tiering-Modell geläufig, kann mehrere Probleme lösen. Durch die Trennung der administrativen Rechte auf den Tiers brauchen die Administratoren je nach Rollenverteilung zusätzliche Benutzerkonten, um nach der Umstellung der Administration auf das Tiering-Modell ihren verschiedenen Aufgaben nachgehen zu können [1]. Das können insgesamt bis zu fünf Benutzerkonten sein, wenn der Administrator in allen drei Tiers aktiv ist und neben seinem regulären Benutzerkonto auch noch ein lokales Administratorkonto auf seinem regulären Client hat.

Die Anforderung, dass diese Benutzerkonten über sehr sichere (und damit lange), einzigartige und nicht in Zusammenhang stehende Passwörter verfügen müssen, macht es nicht einfacher, sich diese zu merken und sie auch regelmäßig zu ändern. Hier kann die Einführung eines PAM-Produkts helfen, die zahlreichen Konten zu verwalten. Der Administrator muss sich dann je nach Implementierung nur noch zwei der fünf Passwörter merken, nämlich das des Benutzerkontos, mit dem er sich am regulären Client anmeldet, und das des Tier-0-Adminkontos, mit dem er sich an der Privileged Access Workstation (PAW) [2] anmeldet. Von dort hat er Zugriff auf das PAM-Werkzeug und die darin enthaltenen Konten.

Außerdem kann das PAM die regelmäßige Änderung der Passwörter der hochprivilegierten Konten mit besonders langen und kryptischen Passwörtern automatisieren, was die Sicherheit weiter erhöht. Ein gutes PAM-Produkt kann außerdem viele weitere sicherheitsrelevante Probleme beseitigen.

Hilfe bei der Passwortflut

Ein solches PAM-Produkt kann beispielsweise dabei helfen, Standard- oder vorhersehbare Passwörter zu verhindern. Einzigartige Passwörter für jeden einzelnen Dienst und Account lassen sich ohne spezielle Werkzeuge kaum realisieren, da schon in einem kleinen Unternehmen schnell Hunderte Konten zusammenkommen, wenn man alle Systeme berücksichtigt, zum Beispiel Komponenten der Netzwerkinfrastruktur, Drucker, IP-Kameras, Zeiterfassungsterminals, Schließanlagen, Webanwendungen, Dienstbenutzer auf Servern und sonstige Dienste im Netzwerk.

All diese Passwörter wollen sicher verschlüsselt und zugriffsgeschützt gespeichert und gesichert (im Sinne eines Backups) werden. Insbesondere ein regelmäßiges Ändern dieser Passwörter ist manuell nicht zu leisten, stellt aber eine wichtige Maßnahme zur Absicherung der Administration dar. Paradebeispiele sind hier ehemalige Mitarbeiter, die das Passwort noch kennen, oder Skriptdateien, in denen vor Jahren das Klartextpasswort hinterlassen wurde, um etwas zu testen. Solche Änderungen kann ein PAM-Produkt typischerweise gut automatisieren. Das ist dann besonders hilfreich, wenn auch solche Systeme innerhalb des Tiering-Konzepts administriert werden, die nicht domänenintegriert oder für die Authentifizierung nicht an die Domäne angebunden sind.

Ein Administrator kann das PAM-Tool bei seiner regulären Arbeit beispielsweise wie folgt nutzen: Er loggt sich auf der PAW ein und greift mit einem Tier-Admin-

iX-TRACT

- Eine wichtige Säule der Active-Directory-Absicherung ist das Privileged Access Management, mit dem sich die nach Microsofts Tiering-Modell verteilten Adminbenutzerkonten einfacher verwalten lassen.
- Um die Rechtevergabe nach Tiers adäquat umzusetzen, ist in der Regel die Struktur der Organisationseinheiten im AD zu ändern. Hier spielen Unternehmensdetails wie Organisationsstruktur, Standorte oder die Art des IT-Betriebs eine Rolle.
- Die Beschränkung administrativer Zugriffe auf das Notwendigste und die Mikrosegmentierung zum Kontrollieren der Netzwerkkommunikation machen es Angreifern wie Penetrationstestern schwer, sich im Netzwerk auszubreiten.
- Penetrationstester oder echte Angreifer finden manchmal trotzdem einen Weg, müssen aber kreativ sein und werden schneller entdeckt.

konto auf das PAM zu. Dort sieht er einen Eintrag, beispielsweise für einen besonders wichtigen DMZ-Webserver, der nicht Mitglied der Domäne ist. Je nach Konfiguration und PAM kann er jetzt entweder mit einem Klick das aktuelle Administratorpasswort des DMZ-Servers an seine PAW übertragen und auf das System zugreifen oder es öffnet sich idealerweise der Desktop eines zur PAM-Lösung gehörenden Sprungservers. Dort liegen die zur Administration benötigten Werkzeuge, die bereits mit den richtigen Zugangsdaten ausgestattet sind. Nachdem der Administrator mit der Arbeit auf dem System fertig ist, ändert das PAM dann automatisch das Passwort auf dem DMZ-Server und speichert den neuen Wert.

Änderungen an AD-Struktur und Delegation

Um die Rechtevergabe nach Tiers möglichst effizient und sicher umzusetzen, sind Änderungen in der bestehenden Domäne erforderlich. Zur Trennung der Berechtigungsvergabe auf die Objekte im AD nach Tiers muss sehr wahrscheinlich die bestehende OU-Struktur (Organizational Unit) angepasst werden. Typischerweise reflektiert die OU-Struktur einer Domäne, die bisher nicht nach dem Tiering-Modell administriert wurde, eher die organisatorische Struktur des Unternehmens, zum Beispiel die geografische Untergliederung von Kontinent bis Standort, oder sie stellt ein historisch gewachsenes Konstrukt dar.

Eine sinnvolle neue Struktur ist stark davon abhängig, wie das Unternehmen aufgestellt ist. So müssen zum Beispiel Antworten auf die folgenden Fragen in das neue Design einfließen: Wie viele Tiers umfasst das Tiering-Konzept? Ist die IT-Infrastruktur weltweit, in mehreren Ländern oder an mehreren Standorten verteilt? Gibt es eine zentrale IT für das gesamte Unternehmen oder auch autarke IT-Abteilungen in den Ländern? Wie sieht die bestehende OU- und GPO-Struktur (Group Policy Objects, Gruppenrichtlinien) aus? Wie werden die Rechte im AD bisher delegiert? Abbildung 1 zeigt eine mögliche neue OU-Struktur.

Die genaue Struktur ist nebensächlich, solange sie effizient die nach Tier getrennte Delegierung von Rechten beziehungsweise die Verlinkung von GPOs ermöglicht. Die Domänencontroller sollten nicht aus ihrer standardmäßigen „Domain Controllers"-OU in die Tier-0-OU verschoben werden, da das von Microsoft nicht vorgesehen ist und zu Problemen führen kann.

Im Active Directory haben alle authentifizierten Benutzer sehr weitgehende Leserechte auf einen großen Teil der in der Domäne vorhandenen Objekte. Deshalb ist es auch möglich, mit regulären Benutzerberechtigungen und dem Werkzeug BloodHound so viele Informationen auszulesen und entsprechende Angriffspfade zu visualisieren.

Weniger Leserechte, weniger Angriffsfläche

Diese großzügige Berechtigungsvergabe im AD können Administratoren aber auch ändern und authentifizierten Benutzern zur Verschleierung der Existenz und der Struktur der Tier-Konten das Leserecht auf die entsprechenden OUs entziehen. Damit sind sie zum Beispiel in BloodHound nicht mehr sichtbar – es sei denn, der Angreifer hat die Datensammlung mit einem Benutzer durchgeführt, der über anderweitige Gruppenmitgliedschaften verfügt, die ihm das Lesen wieder erlauben. Abbildung 2 zeigt die beschriebene Berechtigungsvergabe für die authentifizierten Benutzer und wie sie geändert werden kann.

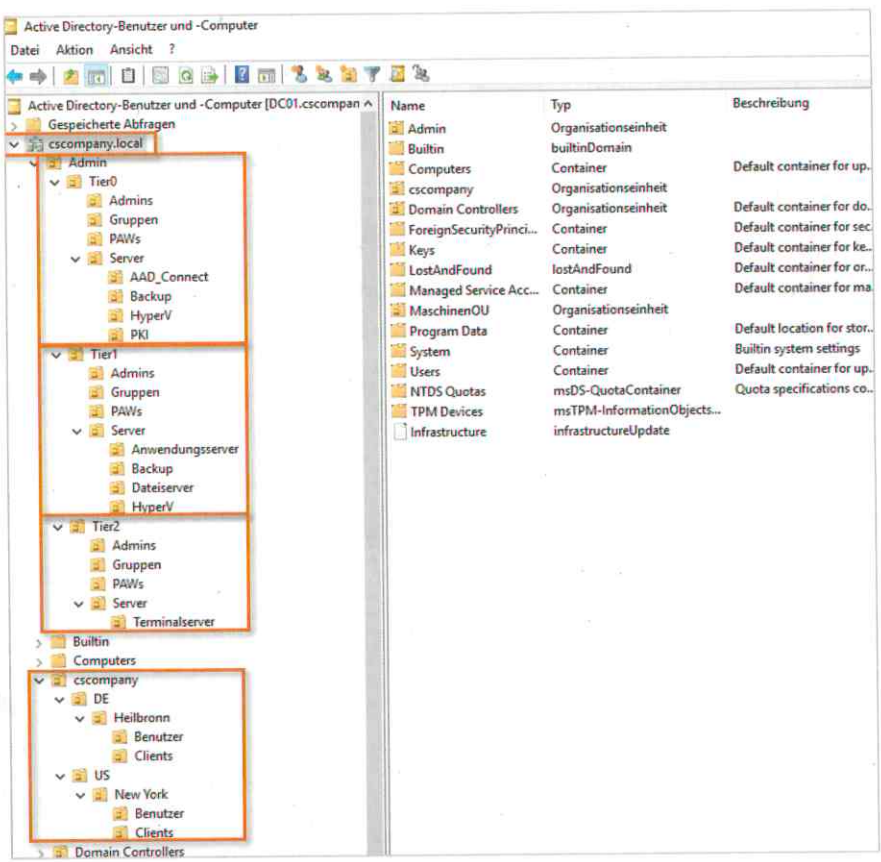
Um Probleme zu vermeiden, sollte das Entziehen dieser Berechtigungen zunächst auf einer Unter-OU getestet werden, die nur wenige Prinzipale enthält. Außerdem sollten in dem in Abbildung 1 dargestellten Beispiel zur OU-Struktur nicht die Rechte auf die ganze Admin-OU entzogen werden, da sich darunter auch die regulären Computerkonten wie Terminal- oder Webserver befinden und manche Anwendungen oder Dienste eventuell darauf angewiesen sind, bestimmte Informationen auslesen zu können. Es lohnt sich deshalb, zunächst mit den OUs zu beginnen, in denen sich die Tier-Adminkonten und PAWs befinden. Diese sind besonders wertvolle Ziele für einen Angreifer und die Wahrscheinlich-

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



Die Struktur kann nach Bedarf gestaltet werden, wichtig ist nur, die Delegierung von Rechten nach Tiers zu trennen (Abb. 1).

keit ist geringer, dass die Anpassung zu Problemen führen wird.

Nach der Umstrukturierung des Active Directory und der Anpassung der Berechtigungsvergaben getrennt nach Tiers muss weiterhin sichergestellt sein, dass die Administratoren zu jeder Zeit die volle Kontrolle über ihre Umgebung haben. Das bedeutet, dass sie bei technischen Problemen und Ausfällen trotz der Einschränkungen durch das Tiering-Modell die Systeme aller Tiers weiterhin administrieren können. Hierzu empfiehlt es sich, sogenannte Break-Glass-Konten mit vollen administrativen Rechten pro Tier zu hinterlegen, zum Beispiel in einem Tresor oder einer verschlüsselten Off-Premises-Passwortdatenbank wie KeePass.

Dabei sollte der Tresor auch bei Ausfall der IT-Systeme erreichbar sein und sich öffnen lassen (Gebäudeschließanlage, Schlüssel, Zahlenkombination et cetera). Die Off-Premises-Passwortdatenbank sollte sich an mehreren Orten befinden und mehrere Personen sollten Zugriff darauf haben. Des Weiteren muss sichergestellt sein, dass das Passwort nicht vergessen wird.

Einschränkung der administrativen Zugriffe

Nach der Einführung des Tiering-Modells sind die administrativen Wege und Zugriffe stark reglementiert und definiert. Das bedeutet, es ist klar geregelt, welche Administratoren von wo welche Systeme über welche Wege verwalten. Das macht es deutlich einfacher, die administrativen Zugriffe auf der Netzwerkebene großflächig einzuschränken. Administrative Zugriffe wie RDP, PowerShell Remoting, weitere administrative Schnittstellen (HTTP, HTTPS, SSH), NetBIOS over TCP/IP (NBT) und SMB werden im Netzwerk nur noch von dort erlaubt, wo sie auch wirklich benötigt werden.

Einen Sonderfall stellen dabei die Protokolle NetBIOS over TCP/IP (NBT) und SMB dar. Für Zugriffe über diese Protokolle sind potenziell administrative Rechte nötig, sie werden aber auch von regulären Benutzern für den Zugriff auf Dateifreigaben benötigt. Der Zugriff darauf sollte also ebenfalls nur dort erlaubt sein, wo er wirklich benötigt wird, zum Beispiel auf den Dateiserver.

Beispiele für nötige administrative Zugriffe und deren Quellen sind:

- von den PAWs aus PAW-Netzwerken;
- von der PAM-Lösung aus dem PAM-Netzwerk;
- vom Monitoringwerkzeug;
- von der Softwareverteilung;
- eventuell aus dem IT-Infrastrukturnetzwerk;
- eventuell aus dem Client-Helpdesk-Netzwerk (Tier 2).

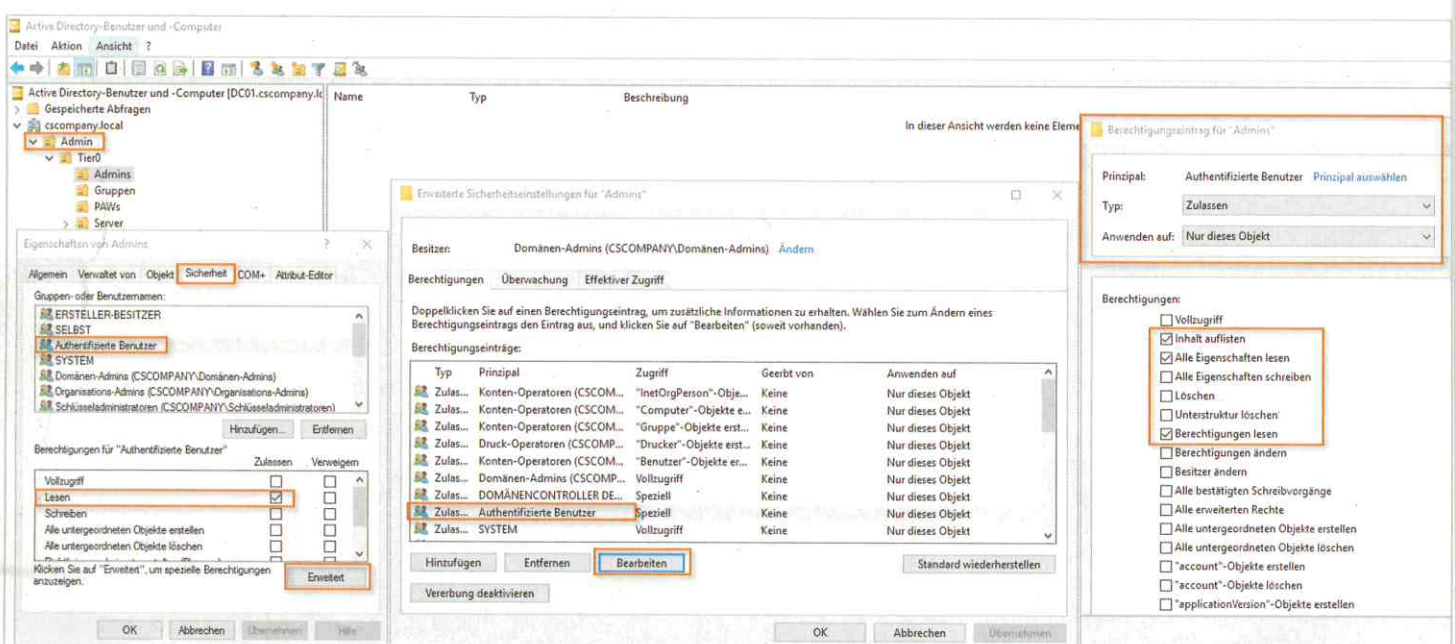
Netzwerkzugriffe einzuschränken und flache Netzwerke abzuschaffen gilt in Fachkreisen schon sehr lange als wirksames Mittel zur Eindämmung von Angriffen und zur Verkleinerung der Angriffsfläche, wird aber oft aufgrund des großen Aufwands nicht umgesetzt. Es stellt sich jetzt also die Frage: Wie geht man es am besten an?

Gut segmentiert ist halb gewonnen

Grundsätzlich gibt es zwei Herangehensweisen. Die klassische Methode besteht darin, mittels Netzwerkfirewalls den Verkehr an den Netzwerk-/VLAN-Grenzen zu filtern. Der Nachteil dieser Methode ist, dass eine Einschränkung des Netzwerkverkehrs innerhalb eines Netzwerksegments (VLAN) nicht möglich ist. Zwei Systeme, die sich im selben Netzwerk befinden, können also ungefiltert miteinander kommunizieren.

Die alternative Methode ist die Einführung einer Form der Mikrosegmentierung. Hier wird das Firewallregelwerk zum Betriebssystem gebracht. Das Client- beziehungsweise Serverbetriebssystem filtert den Netzwerkverkehr also selbst.

Hierfür gibt es wieder zwei Möglichkeiten: Entweder man nutzt die im Windows-Betriebssystem bereits enthaltene Windows-Firewall oder eine dedizierte Lösung zur Mikrosegmentierung. Die Windows-Firewall ist viel mächtiger, als viele Administratoren glauben. Wenn man ihre Funktionsweise und die einzelnen Konfigurationsmöglichkeiten einmal verstanden hat, lässt sie sich überraschend flexibel und vielseitig einsetzen. Der Vortrag „Demystifying the Windows Firewall" einer Mitarbeiterin von Microsoft ist als YouTube-Video abrufbar und



Administratoren können die Leserechte authentifizierter Benutzer beschränken. Damit können Angreifer mit Tools wie BloodHound weniger Daten für die Visualisierung von Angriffspfaden sammeln (Abb. 2).

Einige Lehren aus dem NotPetya-Angriff auf Maersk

Grundlagen #1:

Hören Sie auf zu reden. Fangen Sie an zu handeln.

Sie können Risiken für immer und ewig akzeptieren, aber irgendwann wird es Sie erwischen und jemand wird am Ende die Arbeit machen. Nennen Sie es Technologieschulden oder was auch immer Sie wollen.

Grundlagen #6:

Wenn Ihre Administratoren daran gewöhnt sind, jederzeit auf alles zugreifen zu können, ist es höchste Zeit, dies zu ändern – da hilft keine noch so große Risikoakzeptanz.

Ganz gleich, ob Sie sich strikt an das Microsoft Tiered Access Model halten oder sich für eine etwas leichtere Lösung entscheiden, zumindest sollten Sie: (Es folgen zahlreiche Maßnahmen zur Begrenzung von Adminzugriffen.)

Jetzt höre ich schon hundert Leute sagen (denn das habe ich schon oft gehört): Ja, aber das klingt schwierig. Ja, aber das hört sich teuer an. Ja, aber das wird lange dauern.

Alles zu verlieren wird viel schwieriger sein, wird viel teurer sein, wird viel mehr Zeit in Anspruch nehmen und wird viele Menschen Arbeitsplätze, Beziehungen oder Schlimmeres kosten. Dies sind grundlegende Dinge. Wie das Abschließen der Haustür. Oder eine PIN für Ihre Bankkarte. Es ist eine Schande, dass Microsoft diese Kontrollen nicht schon im Jahr 2000 von Anfang an eingebaut hat, aber so ist es nun einmal. Legen Sie los.

bietet einen hervorragenden knapp einstündigen Crashkurs (siehe ix.de/zfyr).

In kleinen bis mittleren Umgebungen reicht der Funktionsumfang der Windows-Firewall eventuell aus, in mittleren bis großen Umgebungen hingegen stößt die Windows-Firewall schnell an ihre Grenzen. Insbesondere in komplexen Szenarien mit unterschiedlichen Anforderungen wird die Windows-Firewall unkomfortabel zu konfigurieren, zu betreiben und zu überwachen. Hier helfen dedizierte Produkte zur Mikrosegmentierung, zum Beispiel von den Herstellern Guardicore oder Illumio.

Die Mikrosegmentierungsprodukte bringen die Firewallfunktion über Agenten in das Betriebssystem, entweder mit einer eigenen Softwarefirewall oder durch das Verwalten der bereits integrierten Firewall. Sie bieten eine komfortable Verwaltungsoberfläche, unterstützen beim Erstellen des Regelwerks und sind besser zu verwalten und zu überwachen als die Windows-Firewall – dafür aber nicht kostenlos.

Nicht überall einsetzbar

Die Windows-Firewall und dedizierte Mikrosegmentierungslösungen haben gemein, dass sie nicht überall eingesetzt werden können. Naturgemäß ist die Windows-Firewall nur auf Windows-Systemen vorhanden. Die Mikrosegmentierungsprodukte der Drittthersteller unterstützen typischerweise noch weitere Betriebssysteme wie Linux oder Mac. Zur Isolierung von Druckern und einigen anderen Systemen ist jedoch weiterhin eine Netzwerkfirewall nötig.

Unabhängig davon, ob ein Unternehmen klassische Netzwerkfirewalls, die Windows-Firewall oder Mikrosegmentierungsprodukte eines Drittherstellers einsetzt, sollten die nachfolgenden Anforderungen an die Netzwerksegmentierung während der Einführung des Tiering-Modells beachtet und entweder parallel oder anschließend umgesetzt werden.

Die PAWs und die zum PAM gehörenden Systeme sollten sich in speziell isolierten Netzwerksegmenten befinden. Zugriffe auf die administrativen Schnittstellen der Tier-0-Systeme sollte ausschließlich von den Tier-0-PAWs oder anderen Tier-0-Systemen möglich sein. Systeme unterschiedlicher Tiers sollten sich nicht im selben Netzwerksegment befinden und der erlaubte Netzwerkverkehr zwischen den Segmenten sollte auf ein Minimum reduziert werden. Das bedeutet zum Beispiel, dass Zugriffe von Tier-2-Systemen auf Tier-1-Systeme und von Tier-2- und Tier-1-Systemen auf Tier-0-Systeme generell möglichst auf IP-Adress-/Port-Ebene eingeschränkt sind und nur erlaubt wird, was wirklich nötig ist.

Die Kehrseite der Medaille

Der deutlich eingeschränkte Netzwerkzugriff verkleinert die Angriffsfläche enorm und erschwert einem Angreifer die Ausbreitung, erschwert aber auch die Arbeit der Administratoren. Deshalb braucht es Alternativen für den Datei- und Datenaustausch. Zum Beispiel ist es trotz aller Sicherheitsvorkehrungen hin und wieder nötig, Dateien aus dem Internet herunterzuladen und diese in Tier 0 oder auf die PAWs zu übertragen. Oder es müssen Daten zwischen Systemen in verschiedenen Tiers transferiert oder mit externen Dienstleistern ausgetauscht werden.

Die Anforderungen an ein solches zentrales System zum Datenaustausch (auch Datendrehscheibe genannt) können beispielsweise sein:

- Prüfung der Dateien mit verschiedenen Antivirenscanner-Engines;
- dynamische Analyse der Dateien (Sandbox-Analyse);
- granulares Rechtesystem zur Einschränkung von Zugriffen.

Was bringt das alles in der Praxis?

Zum Schluss stellt sich die Frage, welchen Mehrwert die ganzen Änderungen, der ganze Aufwand und die zusätzliche Komplexität tatsächlich bringen.

Konkret behindern die Maßnahmen die Versuche eines Angreifers, seine Rechte auszuweiten und sich im Netzwerk weiter auszubreiten, erheblich, wenn er bereits Zugriff auf einen regulären Domänenbenutzer oder ein domänenintegriertes System erlangt hat. Im besten Fall lässt der Angreifer von dieser Infrastruktur ab und sucht sich ein einfacheres Opfer. Falls es sich bei ihm um einen motivierten und kompetenten Akteur handelt, verschaffen die Maßnahmen den Verteidigern wertvolle Zeit, um den Angreifer zu erkennen und zu stoppen, bevor er sein Ziel erreicht.

Das setzt jedoch neben der Implementierung des Tiering-Modells Produkte zur Angriffserkennung voraus, etwa einen Antivirenschutz, eine EDR-Lösung (Endpoint Detection and Response) auf den Clients und Servern, ein AD-Monitoringwerkzeug, das Angriffe erkennen kann [3], sowie eine gute Sichtbarkeit dessen, was auf Netzwerkebene passiert. Wenn diese Lösungen Alarm schlagen, müssen umgehend die entsprechenden Incident-Response-Prozesse anlaufen, damit keine wertvolle Zeit verschenkt wird. Ziel ist es, den Angreifer aus dem Netzwerk zu werfen und seinen initialen Eintrittsvektor zu blockieren, bevor Schlimmeres passiert.

Die Sicht des Pentesters

Aus der Sicht eines Penetrationstesters hört ein Pentest einer Domäne mit implementiertem „erwachsenem" Tiering-Konzept oft schnell auf, Spaß zu machen. Selbst in sehr großen Umgebungen sind die BloodHound-Graphen „Shortest Path to Domain Admins" und „Shortest Path to High Value Targets" mit möglichen Angriffspfaden zu hochwertigen Zielen dünn gesät. Es ist quasi ausgeschlossen, dass ein beliebiger regulärer Benutzer als Einstieg in solch einen Angriffspfad dienen kann. Mit anderen Worten: Der Penetrationstester muss sich schon deutlich mehr anstrengen und erst einmal andere Benutzer-/Adminkonten oder Systeme kompromittieren, um einen Einstieg zu finden.

Selbst wenn ein realer Angreifer es schafft, ausgehend von seinem Einstiegspunkt einen Benutzer zu kompromittieren, der beispielsweise (administrative) Zugriffsrechte für ein interessantes System hat, kann er idealerweise aufgrund des eingeschränkten Netzwerkzugriffs weder die Remote-Verwaltungsports noch das betreffende System selbst erreichen. Und was man nicht erreichen kann, kann man auch nicht angreifen. Der Angreifer muss also kreativ werden und löst genau damit oftmals Alarm in den Sicherheitssystemen aus.

Aber auch für uns Penetrationstester gibt es noch Chancen. Am vielversprechendsten ist es, nach Verstößen gegen das Tiering-Modell in der alltäglichen Administration zu suchen oder nach den Kompromissen, die ein Unternehmen eingegangen ist.

Zum Beispiel kann SharpHound (die Datensammelkomponente von BloodHound) mit den Parametern `-c session --loop --loopinterval 00:15:00 --loopduration 12:00:00` gestartet werden, damit er in den nächsten 12 Stunden alle 15 Minuten neue Session-Daten sammelt. Der Pentester hofft, dadurch die Anmeldung eines Tier-Adminkontos einer höheren Ebene auf einem System in einer niedrigeren Ebene, auf die man bereits Zugriff hat, mitzubekommen. Vielleicht ist auch die Session eines Tier-Admins „erreichbar", die einen innerhalb einer Ebene weiterbringt.

Kreativ wie ein Angreifer

Ein anderer Ansatz ist es, in BloodHound weitere Objekte als High-Value-Targets zu markieren. BloodHound weiß in der Standardkonfiguration bereits, dass zum Beispiel die Mitglieder der Gruppe Domänenadministratoren oder Domänencontroller einen hohen Wert haben, und markiert diese als High Value. Bei vielen anderen Systemen oder AD-Gruppen, mit denen sich gegebenenfalls weitere Tiers kompromittieren lassen, ist Handarbeit, Erfahrung und die Kreativität des Penetrationstesters gefragt.

Er kann beispielsweise die Konfiguration bereits kompromittierter Systeme analysieren und diese Erkenntnisse mit den BloodHound-Daten verknüpfen, um zum Beispiel den WSUS-Server ausfindig zu machen, der vielleicht auch Updates an Domänencontroller verteilt, oder die AD-Gruppe, deren Mitglieder administrative Rechte in der VMware-Umgebung haben. Sind diese Objekte zusätzlich als High Value markiert, sehen die von BloodHound identifizierten Angriffspfade zu High-Value-Targets vielleicht schon erfolgversprechender aus.

Eventuell hat man als Penetrationstester auch Glück und auf den Systemen niedriger Tiers finden sich noch „Leichen" aus der Zeit vor der Einführung des Tiering-Modells, zum Beispiel in Form von Passwörtern in Skripten, Cached Credentials oder Backups von Systemen, die jetzt zu höheren Tiers gehören. Wenn man ganz viel Glück hat, kompromittiert man beispielsweise ein Tier-2-Adminkonto und findet dann heraus, dass der Administrator dasselbe Passwort oder eine vorhersehbare Abwandlung davon auch für sein Tier-1- oder Tier-0-Konto verwendet.

Um den in diesem Tutorial angesprochenen Konzepten und Maßnahmen mehr Gewicht zu verleihen und die Notwendigkeit ihrer Umsetzung zu verdeutlichen, sei die Lektüre des persönlichen Erfahrungsberichts von Gavin Ashton zu dem verheerenden Angriff auf die IT-Infrastruktur von Maersk nahegelegt (siehe ix.de/zfyr). Gavin Ashton hat den Angriff als Administrator aus erster Hand miterlebt. Einige wichtige Lehren aus dem Vorfall sind im Kasten aufgeführt. Die wahrscheinlich wichtigste ist: Hören Sie auf, darüber zu reden, und fangen Sie an! (ur@ix.de)

Quellen

[1] Hagen Molzer; Active Directory mit dem Schichtenmodell schützen; iX 2/2023, S. 120

[2] Hagen Molzer; Privilegierte Zugriffe besonders schützen; iX 3/2023, S. 136

[3] Hagen Molzer; (Hilfs-)Mittel zum Zweck Active Directory: Tools für mehr Sicherheit; iX 3/2022, S.82

[4] Der erwähnte NotPetya-Angriffsbericht sowie der Vortrag zur Windows-Firewall sind über ix.de/zfyr 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.