illumio

EBOOK

Active Directory schützen

So verteidigen Sie eines der kritischsten und am häufigsten angegriffenen Systeme in modernen Umgebungen

Inhalt

Das Sicherheitsproblem im Zentrum moderner Umgebungen

Das Active Directory spielt in den meisten Umgebungen noch immer eine wichtige Rolle für die Identitätsverwaltung. Es bestimmt, wer sich einloggen kann, wer welche Systeme erreicht und inwieweit Benutzer, Geräte und Anwendungen sich vertrauen. Funktioniert das AD, bemerkt es niemand. Ist es aber kompromittiert, sind kritische Systeme und Daten in Gefahr.

Angreifer wissen das besser als so manches Abwehrteam. Für sie ist das Active Directory der schnellste Weg zur kompletten Kontrollübernahme. Mit einem kompromittierten AD können sie sich bewegen, Berechtigungen eskalieren, Persistenz sicherstellen, monatelang unerkannt operieren und am Ende sogar die Kontrolle über die gesamte Domäne übernehmen.

Das ist der Grund, warum das AD weiterhin so häufig angegriffen wird – und warum es besonders geschützt werden muss. Es ist ein Legacy-System, aber immer noch elementar.

Legacy, aber noch weit verbreitet

Seit Jahren wird ein System nach dem anderen in die Cloud verlagert und die Identitätsverwaltung modernisiert, aber das Active Directory nutzen viele Unternehmen nach wie vor für die On-Premises-Identitätsverwaltung und zum Synchronisieren von Benutzern und Gruppen mit Microsoft Entra ID.

Dieses Festhalten an einem Altsystem ist zwar aus Kostensicht ungünstig, aber in den meisten Unternehmen Normalität.

Das AD wird weiterhin für große lokale Umgebungen und kritische Systeme gebraucht, die Authentifizierungsprotokolle wie Kerberos und NTLM nutzen. Diese Abhängigkeiten bestehen, weil Unternehmen über Jahre, teilweise Jahrzehnte Anwendungen, Dienste und Infrastruktur angesammelt haben, die alle diese gemeinsame Identitätsschicht verwenden.

Das umzubauen, würde Jahre dauern und könnte den Betrieb stören. Selbst Unternehmen, die schon viel in die Cloud verlagert haben, haben das Active Directory deshalb (entgegen dem Rat ihrer Cyber-Abwehr) noch immer nicht abgeschafft.

Angreifer sehen das als Einladung: Ein tief verwurzeltes, allgemein vertrautes und eng vernetztes System ist für sie das ideale Ziel.

Das gilt besonders bei Umgebungen, in denen Stabilität wichtiger ist als Geschwindigkeit.

Hybride Identitätsmodelle

Viele Unternehmen sind angewiesen auf Legacy-Anwendungen, strikte Datenregeln und Kernsysteme, die auf keinen Fall ausfallen dürfen. Das Problem bei Identitäten ist: Änderungen wirken sich sehr schnell überall aus. Selbst kleinste Fehler können wichtige Abläufe zum Erliegen bringen.

Deshalb entwickelt sich häufig ein hybrides System: Cloud-Identitätsdienste wie Microsoft Entra ID sind für SaaS, Cloud-Anwendungen und Remote-Benutzer zuständig, während das Active Directory weiter für viele interne Systeme, Anwendungen und Authentifizierungsprozesse eingesetzt wird. Und das ist meist nicht nur eine Übergangslösung, sondern das langfristige Setup.

Die Cloud wächst, der Perimeter verschiebt sich, und doch ist es in vielen Umgebungen nach wie vor das AD, das die Verbindungen zwischen Systemen und die Zugriffsflüsse steuert.

Hybride Identitätsmodelle erhöhen die Reichweite und Flexibilität, bringen aber auch Risiken mit sich: Bei Modernisierungen werden Vertrauensstellungen, Berechtigungen, Zugriffspfade und Trust-Modelle oft einfach übernommen, wenn niemand sie aktiv neu konzipiert. Das Active Directory bleibt die primäre Autorität für Identität und Trust – und wird durch diese zentrale Rolle ein sehr attraktives Angriffsziel.[1]

Moderner Zugriff, der auf althergebrachtem Trust basiert: Das nutzen Angreifer aus.

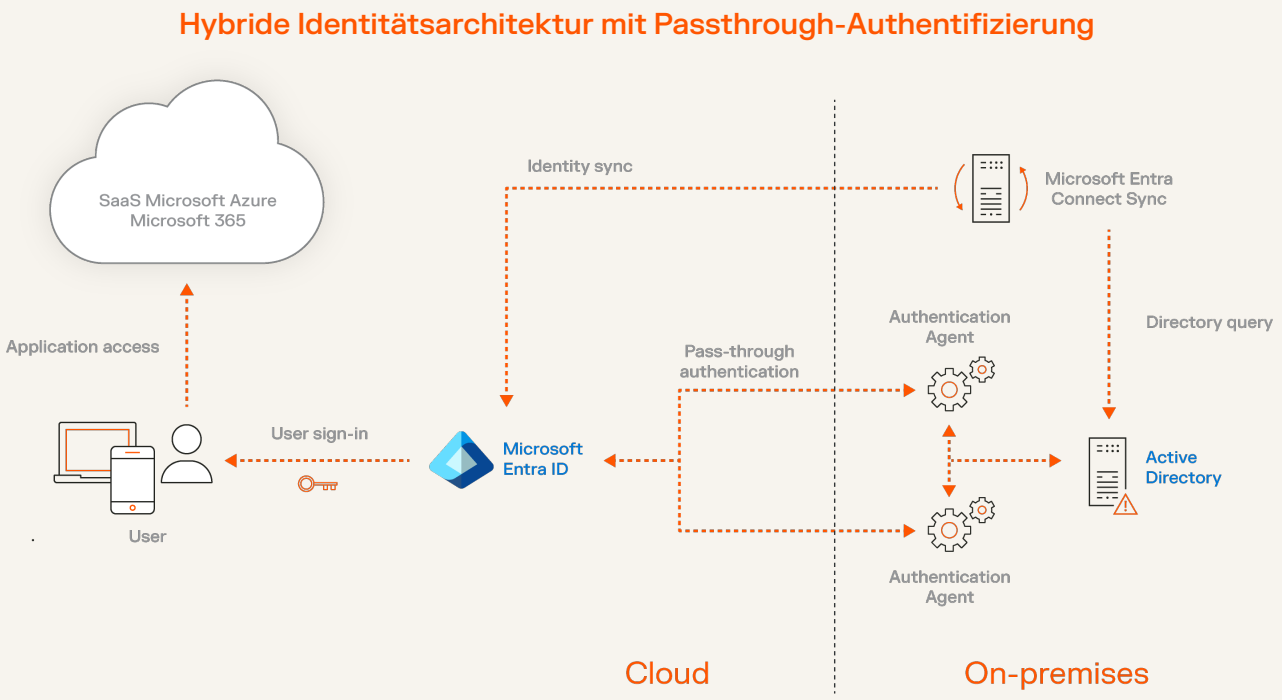


Abbildung 1: Hybride Identitätsarchitekturen sorgen dafür, dass lokale Benutzer auch auf Cloud-Systeme zugreifen können. Das On-Premises-AD wird dabei weiterhin für die zentrale Authentifizierung und die Systembeziehungen gebraucht.

[1] https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/choose-ad-authn

Der Weg zur AD-Kontrolle führt über Domain-Controller

Das Active Directory und die Domain-Controller sind unterschiedliche Dinge, in der Praxis aber unzertrennlich. Das AD definiert Identitäten, Berechtigungen und Trust in der gesamten Umgebung. Die Domain-Controller hosten dieses Verzeichnis und setzen die Regeln durch – sie verarbeiten die Authentifizierung, validieren den Zugriff und replizieren Identitätsdaten.

Angreifer sind nicht auf einzelne Systeme aus, sie wollen die komplette Kontrolle über Identitäten erlangen. Das Active Directory ist das Ziel, und über die Domain-Controller gelangen sie dorthin. Wer einen Controller kompromittiert, kontrolliert das AD.

Abbildung 2 zeigt, warum das so ist: Die Domain-Controller stehen bei der Authentifizierung und Richtlinienumsetzung immer im Mittelpunkt. Benutzer, Endpoints und Anwendungen funktionieren nur, wenn die Domain-Controller funktionieren. Diese zentrale Rolle nutzen Angreifer aus.

Auf ihrem Weg durch die Umgebung folgen Angreifer den bestehenden Trust-Pfaden. Diese führen zurück zu Domain-Controllern, weshalb sie bei lateraler Bewegung gezielt angesteuert werden.[2]

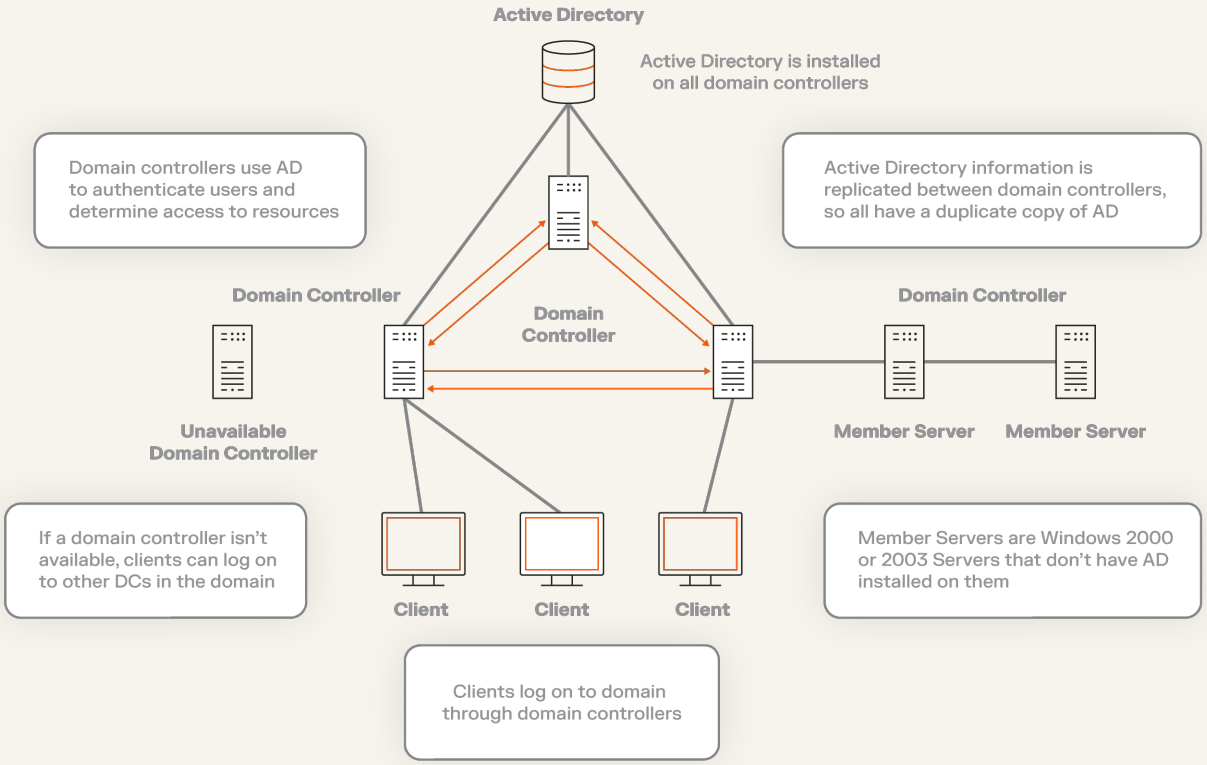


Abbildung 2: Beziehung zwischen Active Directory und Domain-Controllern

[2] https://www.sciencedirect.com/topics/computer-science/active-directory-user?__cf_chl_tk=I4eXbVwnEaTgiZ8x2cEkNln0KiP7fBWM3lmpHQlryJo-1777299782-1.0.1.1-L.ktuh6leFYCR7zZjQw9N58hT3ZUfUb10tDGFLY1alQ

Bekannte Angriffe mit AD-Beteiligung

Jahr	Vorfall	Was ist passiert?	Anteil AD/ Identitäten	Wie ist es passiert?
2017	WannaCry-Ransomware	Wurm-Ransomware nutzte SMB aus.	Verbreitete sich über domainverbundene Systeme.	AD-Vertrauensstellungen beschleunigten die Verbreitung.
2017	NotPetya-Angriff	Zerstörerische Malware getarnt als Ransomware.	Credential Harvesting und laterale Bewegung über Domain-Tools.	Ungeschütztes AD ermöglichte die schnelle Verbreitung der Schadsoftware.
2020	SolarWinds (Supply-Chain-Angriff)	Kompromittierte Orion-Updates ermöglichten Spionage.	Persistenz hergestellt über ADFS und SAML-Token.	Kompromittierte Identität ermöglichte dauerhaften Zugang.
2020	Ryuk-/Conti-Ransomware	Menschengesteuerte Ransomware-Kampagnen.	Credential Dumping und Domain-Übernahme im Vorfeld.	Domain-Übernahme vor dem eigentlichen Ransomware-Einsatz.
2021	ProxyLogon (Microsoft Exchange)	Exchange-Schwachstellen ausgenutzt.	SYSTEM-Zugriff und gestohlene Zugangsdaten führten zur AD-Kompromittierung.	Schwachstellen ermöglichten Identitätsfälschung.
2022–2023	BlackByte-Ransomware	Angriffe auf kritische Infrastruktur.	Nutzte AD für laterale Bewegung und Persistenz.	Identitäten bildeten die Angriffsgrundlage.
2023	LockBit-Ransomware	Globale Ransomware-Aktivitäten.	Domain-Enumerierung und Kompromittierung von Domain-Controllern.	Vor dem eigentlichen Ransomware-Einsatz wurden Identitäten angegriffen.
2023 (gemeldet)	Angriffe von Volt Typhoon	Staatlich geförderte APT-Gruppe greift Infrastruktur an.	LOTL-Techniken mit Ausnutzung von AD-Trust.	Identitätsmissbrauch führt zu Einnistung und großflächiger Ausbreitung.

Vom Breach zur Kontrolle: Wie Angriffe ablaufen

Die meisten Angriffe fangen klein an: eine Phishing-Mail, ein mehrfach verwendetes Passwort, ein einzelner kompromittierter Endpoint. Zunächst haben Angreifer nur eingeschränkten Zugriff und keine Domänen-Berechtigungen.

Doch dann beginnen sie mit der Informationssammlung. Sie durchsuchen das kompromittierte System nach Authentifizierungsmaterial – Passwort-Hashes, Kerberos-Tickets und Token von aktiven Benutzersitzungen, die noch im Arbeitsspeicher liegen. Mit speziellen Tools oder Frameworks können sie diese Artefakte aus Prozessen wie dem Local Security Authority Subsystem Service (LSASS) extrahieren und sich damit anschließend bei anderen Systemen mit diesem Benutzer anmelden, ohne das eigentliche Passwort knacken zu müssen, denn die Umgebung vertraut diesen Zugängen bereits. (Siehe dazu Abbildung 3.)

Mit Techniken wie Pass-the-Hash und Pass-the-Ticket können sich Angreifer wie legitime Benutzer lateral bewegen. Mit jedem Schritt erreichen sie neue Systeme und weitere Zugänge, die sie den Domain-Controllern und damit der vollen Kontrolle über die Umgebung immer näher bringt.

Angriffstechniken nach der ersten Kompromittierung

Technik	Beschreibung
Pass-The-Hash/-Ticket	Nutzt gestohlene Authentifizierungsdaten, um Zugriff zu erlangen
Ausnutzung schwacher Konfigurationen	Nutzt Fehlkonfigurationen aus, um hohe Zugriffsrechte zu erlangen
Living Off the Land (LOLBins)	Nutzt integrierte Tools, um Erkennung zu umgehen
Credential Dumping	Extrahiert Zugangsdaten aus Arbeitsspeicher oder Systemen
Session-Hijacking/Token-Missbrauch	Stiehlt oder fälscht Token, um auf Systeme zuzugreifen
Network Sniffing	Fängt Netzwerk-Traffic ab, um Zugangsdaten zu sammeln

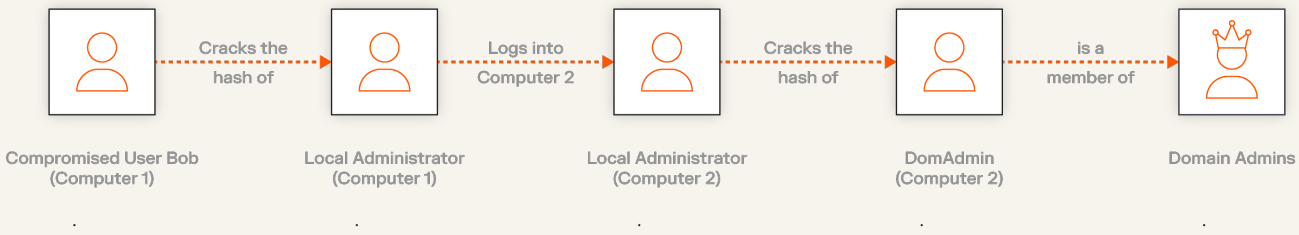


Abbildung 3: Während der lateralen Bewegung erhöhen Angreifer ihre Berechtigungen mithilfe von gestohlenen Hashes und Zugangsdaten von einem einzelnen kompromittierten Benutzer bis zum Domain-Admin, ohne Passwörter knacken zu müssen.

Living Off the Land: Tarnung im Normalbetrieb

Sobald die Angreifer Zugänge haben, brauchen sie gar keine eigenen Tools mehr. Die bereits in der Umgebung installierten Werkzeuge – PowerShell, PsExec, WMI, SMB, RDP, WinRM, SSH – reichen völlig aus, um sich zwischen den Systemen zu bewegen, die Umgebung abzufragen und auf die Domänen-Übernahme hinzuarbeiten.[3] Dieses Vorgehen, „Living Off the Land" (LOTL) genannt, ist inzwischen das beliebteste: Bei einer Auswertung von über 700.000 Vorfällen stellte Bitdefender 2025 fest, dass bei 84 % der schwerwiegenden Angriffe LOTL-Techniken zum Einsatz kamen.[4]

Der Grund ist einfach: Mit diesem Vorgehen bleiben Angreifer für die Abwehr meist unsichtbar. LOTL-Aktivität sieht wie normale Aktivität aus. Sie läuft im Arbeitsspeicher, geht im regulären Betrieb unter und hinterlässt weniger offensichtliche Spuren als Malware-Angriffe.

So verbringen Angreifer oft mehr als 200 Tage in der Umgebung und springen von einem System zum anderen – vom Endpoint zum Server, vom Server in die Infrastruktur und schließlich zu den Domain-Controllern.[5] Das läuft immer gleich ab: kompromittieren, eskalieren, weiterbewegen und dann wieder von vorn.

In Active-Directory-Umgebungen geht das sehr schnell, weil sie von Natur aus hochgradig vernetzt sind.

Kompromittieren, eskalieren und weiterbewegen in Dauerschleife

Laterale Bewegung läuft in zwei Phasen ab – und wenn eine scheitert, scheitert der ganze Angriff. LOTL ist dabei so effektiv, weil es wie normale Aktivität aussieht.

Auf dem Host: Bevor sich Angreifer weiterbewegen, stärken sie ihre Position in dem System, das sie bereits kompromittiert haben: Sie extrahieren Zugangsdaten, eskalieren Berechtigungen und führen Tools im Arbeitsspeicher aus, um unerkannt zu bleiben. Wenn sie keinen Admin-Zugang erlangen oder wiederverwendbare Zugangsdaten finden können, endet ihre Ausbreitung dort.

Zum nächsten Host: Mit den erbeuteten Zugangsdaten bewegen sich die Angreifer zum nächsten System – über Protokolle, denen die Umgebung vertraut: SMB, PsExec, RDP, WinRM, SSH. Aus einem kompromittierten System werden mehrere, bis die Angreifer schließlich bei den Domain-Controllern ankommen.

Diese beiden Phasen wiederholen sich: kompromittieren, eskalieren, weiterbewegen und dann wieder von vorn. Jeder Durchlauf erweitert den Zugriff und bringt Angreifer der kompletten Übernahme näher. Und das nur mit den Mitteln der Umgebung, ohne irgendeinen Exploit.

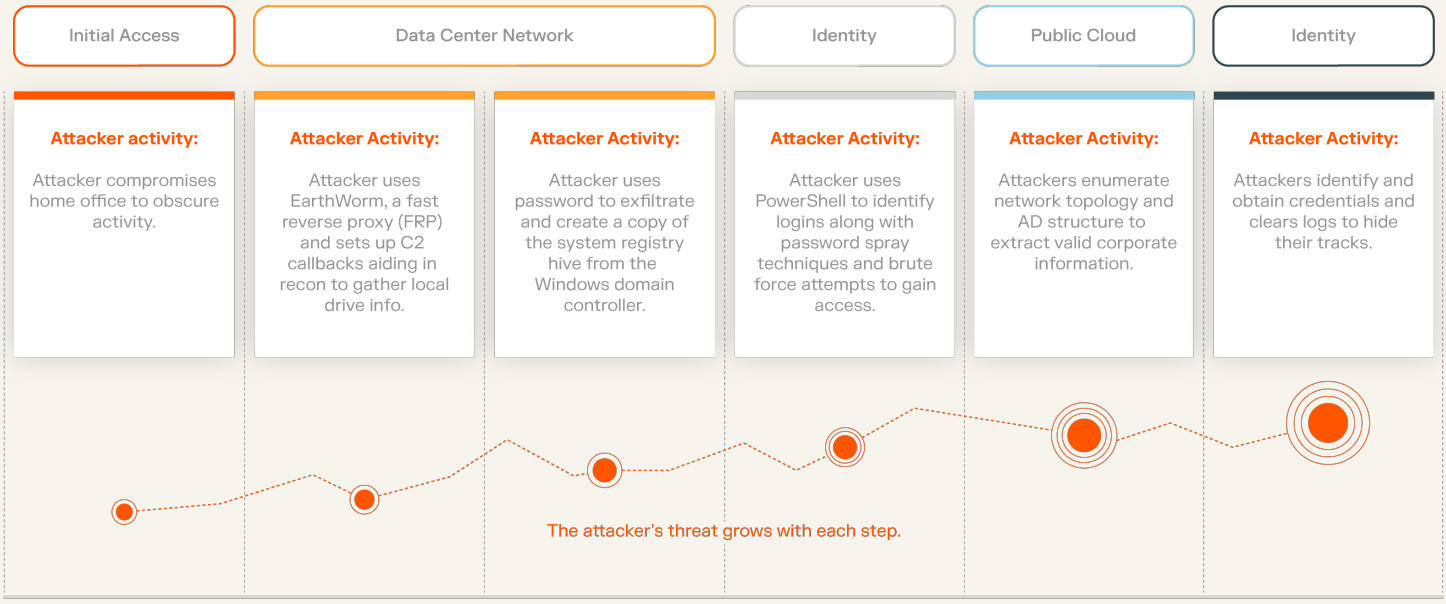


Abbildung 4: Simulierter Living-Off-the-Land-Angriff mit EarthWorm, einem leistungsstarken Open-Source-Tool für das Tunneling

[3] https://www.illumio.com/blog/modern-trojan-horse-how-attackers-live-off-the-land-and-how-to-stop-them
[4] Bitdefender, „How Analyzing 700,000 Security Incidents Helped Our Understanding of Living Off the Land Tactics", Juni 2025.
[5] IBM, „Cost of a Data Breach Report", 2025.

Warum das AD angegriffen wird

Ein einzelner kompromittierter Endpoint ist nur der erste Zugangspunkt. Um an ihr Ziel zu kommen, brauchen Angreifer vor allem das Active Directory.

Nachdem sie sich Zugang zum System verschafft haben, raten Angreifer nicht blind, wohin sie als Nächstes gehen könnten. Die Umgebung selbst verrät ihnen den schnellsten Weg zum Ziel – und dieser führt in den meisten Unternehmen über das Active Directory. Mit integrierten Tools können Angreifer dann weiterarbeiten:

- Das AD abfragen, um die Umgebung abzubilden
- Privilegierte Konten und Zugriffspfade finden
- Näher an Domain-Controller kommen
- Zugriff eskalieren, ohne Malware einzusetzen
- Netzwerk-Shares und Dateisysteme erreichen

Das alles macht das Active Directory möglich. Angreifer können damit die Domänenstruktur, privilegierte Beziehungen und andere hilfreiche Informationen ermitteln. Jeder Schritt baut auf dem letzten auf, und alles läuft auf ein Ziel hinaus: den Domain-Controller. Dort werden die Zugriffsregeln umgesetzt und dort kann die Kontrolle über die ganze Umgebung übernommen werden.

Das ist nicht kompliziert, denn die Umgebung ist für Konnektivität optimiert, nicht für Containment.

Angreifer kennen Ihre Umgebung besser als Sie selbst

Angreifer bewegen sich nicht blind durch das Active Directory – sie haben sich vorher eine Karte erstellt.

Mit den richtigen Werkzeugen können sie die gesamte Umgebung analysieren: Wer hat worauf Zugriff, wer hat hohe Berechtigungen, wie kann man sich zwischen Systemen bewegen?

Dabei kristallisiert sich etwas heraus, das der Abwehr selten bekannt ist: der kürzeste Weg zur Kontrollübernahme – für Angreifer der perfekte Wegweiser.

Das Problem der Unternehmen ist, dass sie oft nur Ereignisse sehen, aber keine Beziehungen. Logs, Alerts und punktuelle Daten sind nützlich, reichen aber nicht aus.

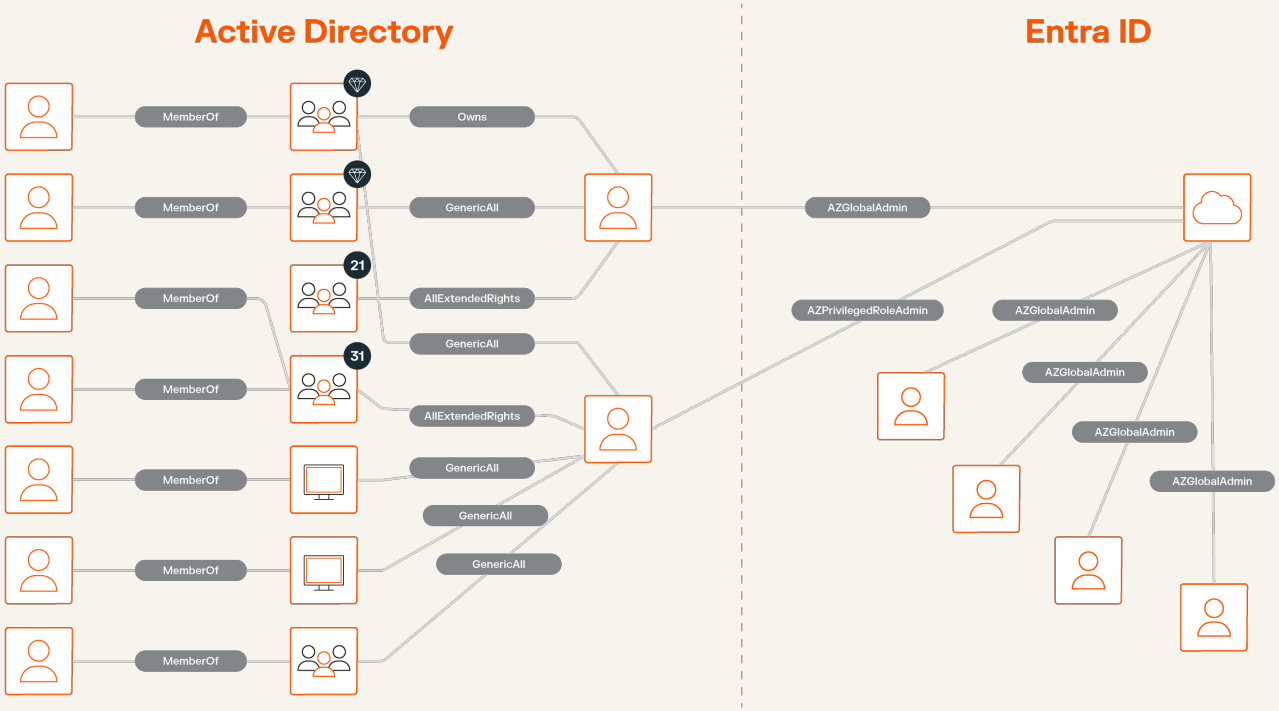


Abbildung 5: Visualisierungstools wie BloodHound bilden die Identitätsbeziehungen im Active Directory ab und machen dabei versteckte Pfade sichtbar, über die sich Berechtigungen bis hin zur Domain-Kontrolle erhöhen lassen.

Angriffstools bilden Ihre Umgebung ab

Angreifer raten nicht. Sie verwenden Spezialwerkzeuge, um Identitäten, Zugriffsregeln und Beziehungen in Ihrer Umgebung auszuwerten:

- **BloodHound:** Bildet AD-Beziehungen und Angriffspfade ab.
- **SharpHound:** Datensammler, wird zusammen mit BloodHound eingesetzt.
- **PingCastle:** Prüft die AD-Sicherheit und ermittelt Risiken.
- **PowerView:** Enumeriert Domains, Benutzer und Berechtigungen über PowerShell.
- **ADFind:** Fragt das AD nach Objekten und Beziehungen ab.
- **CrackMapExec:** Automatisiert die Verifizierung von Zugangsdaten, Remote-Ausführung und laterale Bewegung.
- **Mimikatz:** Extrahiert Authentifizierungsdaten (Passwörter, Hashes, Tickets) und ermöglicht das Erhöhen von Berechtigungen.
- **Rubeus:** Missbraucht Kerberos-Tickets (Pass-the-Ticket, Ticket-Requests).

Die meisten Security-Tools überwachen das Falsche

Sobald es ein Angreifer in die Umgebung geschafft hat, ändert sich die Fragestellung der Abwehr. Statt „Wie passiert ein Angriff?“ heißt es nun: „Können wir den laufenden Angriff klar genug sehen, um ihn aufzuhalten?“

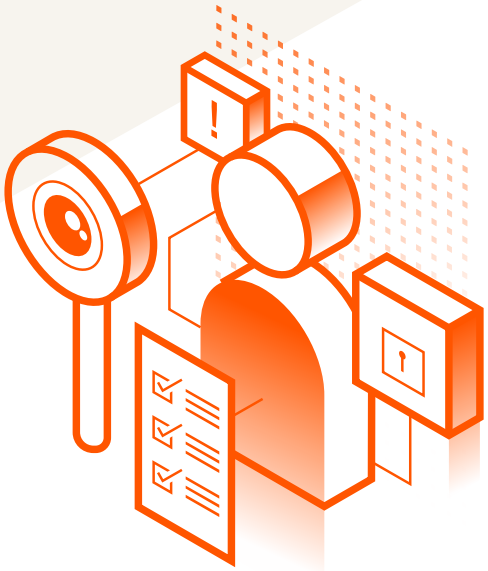
Die meisten Umgebungen großer Unternehmen sind stark verdichtet: Es gibt Tausende Systeme, Identitäten und Berechtigungen, die in Echtzeit interagieren. Das Security-Team überwacht diese Aktivität mit Logs und Alerts, die Ereignisse wie Logins, Dateizugriffe und Prozessaufrufe aufzeichnen – aber nicht die Zusammenhänge zwischen diesen Ereignissen.

Das ist der blinde Fleck. Ohne Überblick darüber, wie die Systeme kommunizieren und wie der Zugriff fließt, sieht man sehr deutlich die einzelnen Bäume, aber nicht den ganzen Wald.

Vier Aspekte sind wichtig, um diese Lücke zu schließen:

- **Einblick in laterale Bewegung:** Wie sind die Systeme untereinander verbunden, welche Pfade werden tatsächlich genutzt?
- **Verhaltenskontext:** Welche Aktivität ist normal, welche riskant?
- **Risikopriorisierung:** Bei welchen Verbindungen und Zugriffspfaden wäre eine Kompromittierung am schlimmsten?
- **Schnelle Eindämmung:** Es muss innerhalb von Minuten möglich sein, die Kommunikation zu kappen oder Systeme zu isolieren.

Mit diesem Einblick wird die Aktivität in der Umgebung lesbar. Ohne ihn sieht die Abwehr das Ereignisprotokoll eines Angriffs, aber nicht den Angriff selbst.



BloodHound: Was Angreifer sehen

Angreifer kennen Ihr Active Directory oft besser als Sie selbst, und das liegt unter anderem an BloodHound.

Dieses Open-Source-Tool wertet Active-Directory-Daten aus (Benutzer, Gruppen, Berechtigungen, Systeme) und visualisiert Angriffspfade.

Was dabei herauskommt, ist ein Graph, der genau zeigt, wie ein niedrig privilegierter Benutzer Schritt für Schritt die volle Kontrolle über die Domäne erlangen kann.

So verstehen Angreifer Ihre Umgebung: nicht als Ansammlung voneinander getrennter Systeme, sondern als Verkettung von Konten und Berechtigungen.

Diese Übersicht brauchen auch Sie, um die Risiken zu erkennen:

- Veraltete oder überprivilegierte Konten
- Verborgene Vertrauensstellungen
- Indirekte Pfade zu Domain-Controllern

Was auf den ersten Blick sicher aussieht, ist es bei genauerem Hinsehen oft nicht. Und wenn Angreifer die Umgebung besser kennen als das Unternehmen selbst, lässt sich laterale Bewegung kaum verhindern.

Firewalls sind darauf nicht ausgelegt

Selbst wenn Unternehmen dieses Risiko erkannt haben, können sie es oft nicht so einfach reduzieren.

Domain-Controller nutzen sowohl statische als auch dynamisch zugewiesene Ports. In großen Unternehmen können sich durch die kontinuierliche Kommunikation zwischen den Systemen Millionen möglicher Kommunikationspfade ergeben.

Und kritisch sind dabei nicht nur Anfang und Ende des Pfads, sondern auch alle Gabelungen dazwischen: Jeder Workload, jeder Dienst, jede Identitätsbeziehung kann Angreifer in der Umgebung einen Schritt weiterbringen.

Herkömmliche Schutzmaßnahmen sind auf solche Maßstäbe nicht ausgelegt. Firewalls brauchen statische Regeln, das Active Directory braucht dynamische Kommunikation. In diesem Dilemma entscheiden sich die meisten Unternehmen für die Variante, bei der die Systeme weiter funktionieren: Sie lassen intern umfangreichen Zugriff zu. Das Ergebnis ist eine funktionierende Umgebung – mit einer enormen Angriffsfläche.

Das Problem hat aber noch eine zweite Ebene: Die Umgebung ist meist historisch gewachsen. Statt Umgebungen neu aufzusetzen, werden über Jahre, manchmal Jahrzehnte, neue Systeme über die alten gelegt und moderne Dienste an alte Infrastruktur angeschlossen. Die alten Systeme werden dann oft nicht mehr intensiv überwacht, sind aber noch genauso eng mit dem Active Directory verbunden – und damit das ideale Angriffsziel.

Das Problem ist inhärent: Die Umgebung, die die Abwehr zu schützen versucht, wurde für ständige Kommunikation optimiert, aber nicht für Eindämmung.

Die neue Verteidigungsstrategie: Mikrosegmentierung und Eindämmung lateraler Bewegung

Wenn es nicht mehr reicht, das Eindringen zu verhindern, muss sich der Fokus verschieben – von der Zugriffskontrolle zur Einschränkung der Bewegung. (Siehe dazu Abbildung 6.)

Moderne Security-Lösungen spiegeln das wider:

- Assume-Breach-Ansatz
- Transparenz in Form von Maps oder Graphen
- Überwachung der Systembeziehungen
- Schnelle Eindämmung von Angreifern
- Einschränkung der Berechtigungen

Damit das alles möglich ist, braucht es Zero Trust. Sie müssen genau kontrollieren können, wie Systeme miteinander kommunizieren – statt nur zu sehen, was bereits passiert ist. (Siehe dazu Abbildung 7.)

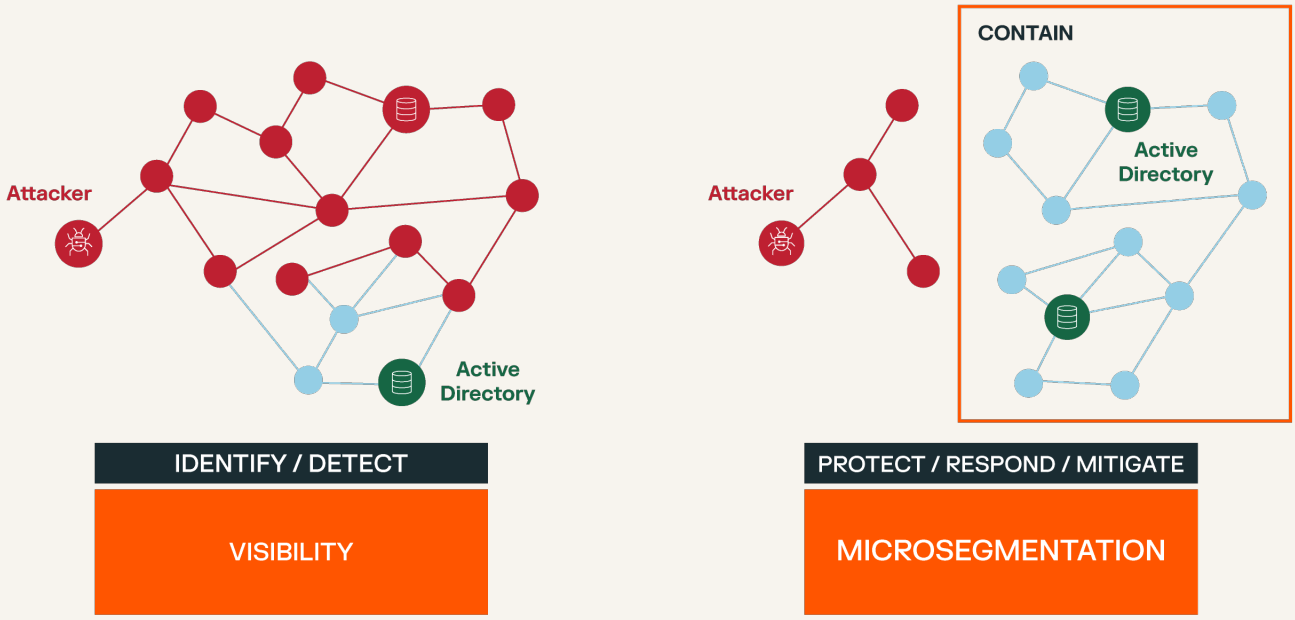


Abbildung 6: Graphen zeigen, wo sich der Angreifer bewegt, aber nur mit Mikrosegmentierung lässt sich die laterale Bewegung auch aufhalten.

Abbildung 7: Auf *Containment* ausgerichtete Mikrosegmentierung nach Zero-Trust-Prinzipien

Dafür müssen Sie die Umgebung nicht komplett neu aufbauen, sondern nur steuern, wie sich die Systeme miteinander verbinden. Das schränkt die Bewegung ein und hindert Angreifer daran, sich weiter auszubreiten.

Wenn ein Angriff bereits läuft, nützen reaktive Tools nur noch wenig. Der Schaden weitet sich oft schneller aus, als Alerts untersucht werden können. Ein kontinuierlicher Einblick ist wichtig, damit man laterale Bewegung in Echtzeit erkennen und vor allem einschränken kann. Das hält Angreifer auf, bevor sie noch tiefer in Ihr Netzwerk vordringen können.

Mikrosegmentierung: Angreifer aufhalten, bevor sie das Active Directory erreichen

Wie genau ein Angriff anfängt, ist gar nicht entscheidend. Wichtig ist, was danach passiert.

Gestohlene Zugangsdaten allein richten noch keinen Schaden an. Nur wenn sich Angreifer nach dem Erstzugriff ungehindert weiterbewegen können, wird die Umgebung selbst zur Waffe. Können sie das nicht, bleibt der Angriff stecken. Das ist der Faktor, der entscheidet, ob es bei einem kleineren Vorfall bleibt oder die komplette Domäne übernommen wird.

Angriffsradius von Anfang an eingrenzen

Nicht jedes System muss mit dem Active Directory verbunden sein. Und doch ist es in vielen Umgebungen auf mehr Wegen erreichbar, als das Security-Team überblicken oder kontrollieren kann. Mikrosegmentierung ändert das: Sie schränkt ein, welche Workloads mit Domain-Controllern kommunizieren können – und von wo. Selbst mit gültigen Zugangsdaten können Angreifer dann das Active Directory nicht über unerwartete Systeme oder Pfade erreichen.

Die Gesamtanzahl der möglichen Pfade sinkt, und damit auch die potenzielle Angriffsfläche und der Angriffsradius.

Wie wird das AD tatsächlich genutzt?

Die meisten Angreifer machen sich nicht bemerkbar. Sie verwenden echte Zugangsdaten und vertrauenswürdige Protokolle, weshalb signaturbasierte Tools sie nicht erkennen. Was sie verrät, ist ihr Verhalten – wenn Sie vorher wissen, wie reguläres Verhalten aussieht.

Finden Sie heraus, wie Ihr Active Directory *normalerweise* genutzt wird: Welche Systeme fragen das AD ab, welche Konten authentifizieren sich wo, welche Protokolle übertragen legitimen Traffic zwischen welchen Workloads?

Wenn Sie diese Baseline haben, fallen Angreiferbewegungen sofort als Anomalien auf, selbst wenn echte Zugangsdaten verwendet werden.

Bewegung erkennen, bevor es zu spät ist

Zwischen dem Erstzugriff und der Domänenübernahme gibt es ein Zeitfenster, in dem sich Angriffe noch stoppen lassen – wenn Sie sie rechtzeitig sehen.

Im Abgleich mit der Baseline gibt es deutliche Anzeichen, dass sich ein Angreifer gerade lateral bewegt:

- Das AD wird von einem System abgefragt, das vorher nie eine Query gestellt hat.
- Die Anzahl der Authentifizierungsanfragen schnellt plötzlich hoch.
- RDP- oder SMB-Traffic tritt zwischen Workloads auf, die bisher nie miteinander kommuniziert haben.
- Zugriffsabfolgen eskalieren in Richtung Domain-Controller.

Diese Signale weisen auf einen Angriff hin, der gerade im Gang ist, aber noch nicht sein Ziel erreicht hat. Wird er rechtzeitig erkannt, kann der Breach eingedämmt werden, bevor er größeren Schaden anrichtet.

Sofort eindämmen

Nachdem eine Bedrohung erkannt wurde, ist Schnelligkeit wichtiger als eine gründliche Untersuchung. Jetzt geht es nicht darum, Systeme abzuschalten, sondern den Angreifer wirksam aufzuhalten. Wenn der kompromittierte Workload auf Netzwerkebene isoliert wird, ist der Angreifer sofort vom Rest der Umgebung abgeschnitten, ohne dass dafür der Betrieb unterbrochen werden muss. Der Breach wird gleich dort eingedämmt, wo Sie ihn erkannt haben – bevor er das Active Directory erreicht.

Fazit

Jeden Einstiegspunkt zu blockieren, ist unrealistisch. Angreifer werden einen Weg finden, in Ihre Umgebung einzudringen, sei es über eine Phishing-Mail, ein gestohlenes Passwort oder einen ungepatchten Server. Das ist mittlerweile unbestritten.

Deswegen lautet die wichtigste Frage nun: Was passiert danach? Ein Angreifer, der bis zum Active Directory vordringt, kann am Ende die ganze Domäne übernehmen. Wird er dagegen gleich beim ersten Workload aufgehalten, passiert nicht viel. Entscheidend ist also, ob die laterale Bewegung kontrolliert wird.

Breach Containment ist kein theoretisches Konzept, sondern eine ganz praktische operative Disziplin. Es sorgt dafür, dass Incidents sich nicht zur Katastrophe ausweiten und beherrschbar bleiben.

Angriffe können Sie nie ganz verhindern. Katastrophen schon.

Illumio stoppt Active-Directory-Angriffe, bevor sie sich ausbreiten.

Testen Sie es selbst mit Illumio Segmentation.