Active Directory: Komfortable IT-Schaltzentrale mit Schwachpunkten

Himmelsgeschenk

Frank Ully

Für Administratoren ist das Active Directory ein wahrer Segen – komfortabler lassen sich Firmenressourcen wohl kaum managen. Doch wo viel Potenzial drinsteckt, sind auch Angriffe am verlockendsten und die Sicherheit ist stark gefährdet. Emotet und Co. lassen grüßen.

Seit seiner Einführung mit Windows Server 2000 hat sich das Active Directory, abgekürzt AD, zum am häufigsten verwendeten Dienst für die Ressourcenverwaltung entwickelt – genutzt von 90 Prozent aller Unternehmen weltweit. Für Administratoren ist AD ein bequemer Dienst zum Verwalten mehrerer Systeme und hat sich womöglich in den Köpfen vieler als Quasi-Synonym für reibungsloses Single Sign-on festgesetzt.

Dieser Erfolg mag auf die Vorteile zurückzuführen sein, die mit seinem Einsatz einhergehen: Ein AD kann die individuelle Netzwerkstruktur einer Organisation abbilden und darin Benutzereinstellungen, Zugriffsrechte und Sicherheitsrichtlinien steuern. Jeder Client und jeder Server innerhalb des Netzwerks lässt sich damit zentral verwalten. Über Protokolle wie Kerberos oder LDAP, von denen noch die Rede sein wird, können auch Nicht-Windows-Systeme wie Linux-Server sich gegenüber einem AD ausweisen oder Daten daraus lesen.

Mit den Jahren ergänzte Microsoft das Active Directory um weitere Dienste, beispielsweise zur Zertifikatsverwaltung für eine Public-Key-Infrastruktur. Wenn vom AD die Rede ist, meint dies in der Regel die Kernkomponente Active Directory Domain Services (AD DS): Sie stellt Authentifizierungs- und Autorisierungsdienste bereit und ist Basis für viele andere Microsoft-Produkte wie Exchange oder SharePoint.

Eldorado für Hacker und Malware

Als Verzeichnisdienst für Netzwerkressourcen, Benutzerkonten und Zugriffsrechte ist das AD für Angreifer eine sprichwörtliche Goldgrube. Aus Sicherheitssicht besteht ein großes Risiko, da darin alle für die Tätigkeiten der Organisation wesentlichen Systeme miteinander verbunden sind.

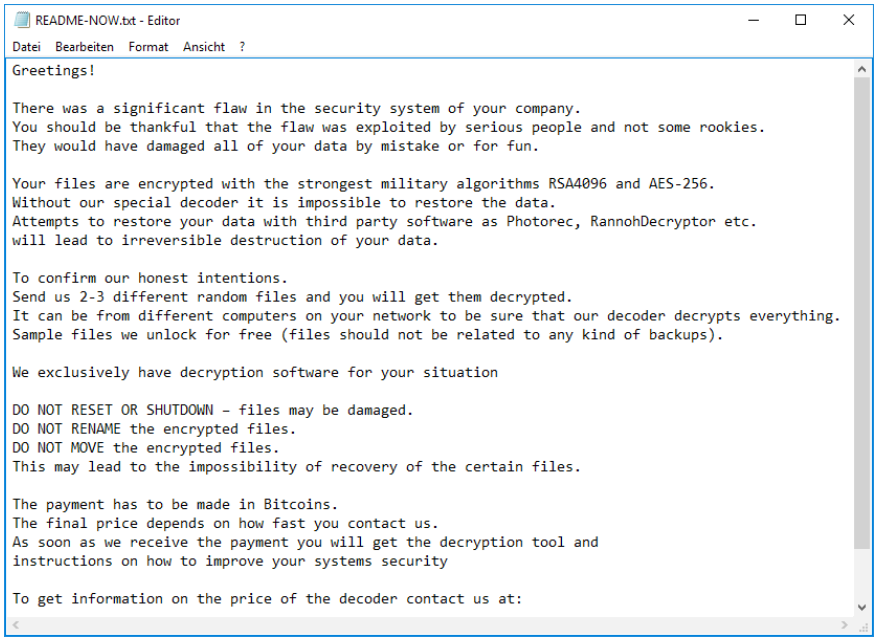
Durch Kompromittieren des Active Directory können Eindringlinge Rechte erlangen, die denen eines Unternehmens-

administrators entsprechen – und damit volle Kontrolle über das gesamte Netzwerk gewinnen.

Um dieses Ziel zu erreichen, müssen sich Angreifer zunächst Zugang zum internen Netzwerk verschaffen, das in den meisten Fällen nicht direkt aus dem Internet zugänglich, sondern etwa durch Firewalls geschützt ist. Bevorzugter Angriffsvektor ist das schwächste Glied der Kette – der Mensch. Auch ungeschützte Remote-Zugänge wie RDP (Remote Desktop Protocol) sind ein Einfallstor. Über Phishing eingeschleuste Schadsoftware nutzt anschließend Fehlkonfigurationen im AD aus, um sich automatisiert im Netzwerk auszubreiten.

Ein prominentes Beispiel ist die schlagzeilenträchtige Malware Emotet, die das Schadprogramm Trickbot nachlädt, um Kontrolle über das AD zu gewinnen, und anschließend alle im Netzwerk erreichbaren Systeme mit der Ransomware Ryuk verschlüsselt (Details zu diesem und allen nachfolgend beschriebenen Angriffen siehe ix.de/z9j3). Die Ausbreitungsgeschwindigkeit von Malware in einem AD ist enorm hoch: Ein Versuch der Sicherheitsforscher von Palo Alto zeigte, dass Emotet/Trickbot innerhalb von 20 Minuten nach der Erstinfektion eines Clients den dazugehörigen Windows-Domänencontroller (DC) infizierte, den zentralen Server in einem AD.

Betroffen sind nicht nur Unternehmen, sondern auch nationale und supranationale Institutionen: etwa beim viel publizierten „Bundestagshack“ im Sommer 2015, bei dem die Angreifer schnell Administratorrechte im AD des Bundestags erlangten und sich zeitweise ungehindert darin ausbreiten konnten. Auch bei der weniger prominenten Attacke auf die Vereinten Nationen 2019, bei der UN-Büros in Genf und Wien kompromittiert wurden, war der Verzeichnisdienst wesentliches Ziel der Hacker. Und schließlich bemängeln Kontrollorgane auch bei Bundesbehörden in den USA – die tendenziell in Sachen IT-Sicherheit besser gerüstet sind als andere Länder – die unzureichende Absicherung des Active Directory, etwa beim US-Patentamt oder der Steuerbehörde IRS.



Lösegeldforderung der Ransomware LockerGoga (Abb. 1)

Stecker ziehen, von vorne anfangen

Sobald Angreifer einmal über die Rechte eines Domänenadministrators verfügen, hilft nur noch, den Stecker zu ziehen und die AD-Umgebung vollständig neu aufzubauen, wenn man ihr wieder vertrauen will. Das passierte auch dem Heise-Verlag nach dem Befall durch Emotet/Trickbot im Sommer 2019: Bei den Aufräumarbeiten wurde ein neues Netz mit frischem Active Directory eingerichtet.

Ein Vorfall, über den in deutschsprachigen Medien nur wenige Details berichtet wurden, war der Ransomware-Angriff 2017 auf den Logistikgiganten Maersk. Innerhalb von Minuten war dessen Netzwerk durch den Verschlüsselungstrojaner NotPetya lahmgelegt. Auch alle Domänencontroller im weltweiten Maersk-Netz waren außer Gefecht, selbst die Online-Backups der DCs waren verschlüsselt. Nur durch Zufall war ein DC in einer Zweigstelle in Afrika zum Zeitpunkt des Angriffs wegen eines Stromausfalls gerade heruntergefahren. Seine Festplatte enthielt die einzige verbliebene Kopie der Domänencontrollerdaten des Unternehmens und wurde per Flugzeug ausgeflogen.

Selbst so vergingen neun Tage, bis das Active Directory wiederhergestellt war, noch Wochen später gab es Unterbrechungen in der Containerschifffahrt. Der Angriff kostete geschätzt 200 bis 300 Millionen Dollar. Ein ehemaliger Maersk-Mitarbeiter berichtet in einem lesenswerten Blogartikel, wie der Konzern jahrelang AD-Sicherheit vernachlässigt hatte, vom Angriff unvorbereitet getroffen wurde und welche Lehren daraus zu ziehen sind.

Backup-Server sind wesentlich für die Wiederherstellung im Falle einer Ransomware-Infektion. Wenn der Backup-Server jedoch mit dem AD verbunden ist und dort Administratorrechte gestohlen werden, kann er ebenfalls infiziert werden – und eine Wiederherstellung der Sicherungen somit unmöglich sein. Wesentlich sind also Offline-Backups.

Angriffe „in Handarbeit“

Im März 2019 legte eine Infektion mit der Ransomware LockerGoga (Abbildung 1) den Aluminiumhersteller Norsk Hydro lahm. Diese Schadsoftware verfügt im Ge-

iX-TRACT

- Das Active Directory hat sich zum meistgenutzten Verzeichnisdienst entwickelt. Grund dafür ist, dass sich damit Nutzer, Systeme und Richtlinien eines Unternehmens äußerst komfortabel verwalten lassen.
- Wenn an einer Stelle so viele Informationen und Administrationsmöglichkeiten wie beim AD zusammenlaufen, ist das für Angreifer äußerst verlockend – und hat besonders gravierende Auswirkungen bei einer Kompromittierung.
- Erst in jüngerer Zeit ist das Bewusstsein für diese Gefahren gestiegen. Viel Sensibilisierung ist noch nötig, damit Admins sich an die Absicherung des AD herantrauen.

gensatz zu NotPetya nicht über einen eingebauten Mechanismus zur Weiterverbreitung, sondern wird von Angreifern eingesetzt, die bereits durch manuelles Hacken Domänenadmin-Rechte erworben haben. Mit diesen Privilegien ausgestattet, nutzten die Erpresser eingebaute Active-Directory-Verwaltungswerkzeuge, um die LockerGoga-Ransomware auf Server und Clients zu verteilen. Auch bei Norsk Hydro war rasch die gesamte Infrastruktur betroffen und nur dank Papierausdrucken von Auftragsbüchern und Ersatzteillisten konnte das norwegische Unternehmen seine Arbeit während des Vorfalls fortsetzen.

Einer der neuesten Zugänge in der Riege der Ransomware 2020 ist „.SaveTheQueen“, benannt nach der Endung, die an verschlüsselte Dateien angefügt wird. Die Erpressertruppe, die diesen Verschlüsselungstrojaner nutzt, hat in ihren Zielumgebungen bereits manuell Domänenadministratorprivilegien erlangt und verwendet diese weitgehenden Rechte, um Malwaredateien in die zentrale SYSVOL-Freigabe auf dem Domänencontroller zu schreiben. Eine geplante Aufgabe, die per Gruppenrichtlinie ausgerollt wird, führt auf allen Rechnern in der Domäne PowerShell-Code aus, der die Ransomware vom Controller herunterlädt und ausführt.

Ein Sicherheitsteam von Microsoft hat im März 2020 den Artikel „Human-operated Ransomware Attacks: A Preventable Disaster“ veröffentlicht (siehe ix.de/z9j3). Er beschreibt solche fortgeschrittenen Angriffe, bei denen nicht nur automatisierte Schadsoftware läuft, sondern Menschen mit umfassenden Kenntnissen der Systemadministration das Zielnetzwerk gründlich erkunden und sich an das anpassen, was sie im kompromittierten Netzwerk entdecken.

Aber auch alte Malware wie Trickbot lernt neue Tricks, die sie ohne menschliches Zutun ausführen kann: In neueren Versionen gibt es ein Modul namens „ADll“, das mit eingebauten Windows-Befehlen von Domänencontrollern die zentrale Datenbank des Verzeichnisdienstes NTDS.dit kopiert und an die Angreifer zurückschickt, die damit über wesentliche Daten der angegriffenen Organisation verfügen.

Wie das AD zu einer so großen Zielscheibe werden konnte

Lange haben IT-Verantwortliche und Administratoren ihr Augenmerk auf klassische Netzwerksicherheit gelegt, etwa durch Firewalling nach außen oder Netzsegmentierung in unterschiedliche Zonen im Inneren. Danach rückten Webanwendungen und die dazugehörige Infrastruktur verstärkt in den Fokus, womöglich gar die Migration in die Cloud. Die Sicherheit des AD als zentraler Dienst im Herzen des Unternehmens fristete oft ein Schattendasein. Dabei können dort verwaltete Gruppenzuordnungen und legitim gewährte Benutzerrechte missbraucht werden – von den Anwendern selbst oder von Angreifern, die sie gestohlen haben.

Zudem wurden zahlreiche heute noch aktive AD-Umgebungen bereits vor vielen Jahren, vielleicht gar einem Jahrzehnt zum ersten Mal aufgesetzt. Zwar gab es damals schon gezielte Angriffe, aber das Wissen darüber war auch unter Hackern und Sicherheitsfachleuten weniger verbreitet als etwa über Schwachstellen in Webanwendungen wie die klassische SQL-Injection.

Diese älteren ADs konzentrierten sich nur auf den Aufbau der Verzeichnisstruktur, die Kontenverwaltung und Delegierung von Rechten oder das Nutzen von Gruppenrichtlinien zum Härten der Umgebung. Andere Sicherheitseigenschaften wurden ignoriert.

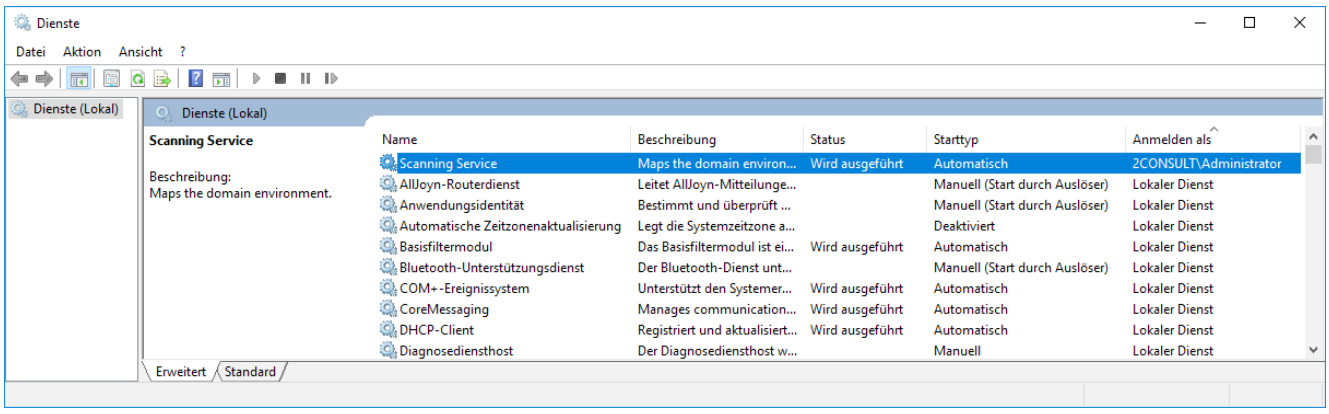
Auch wenn wichtige Server im AD von einer veralteten Version von Windows auf die neueste Version aktualisiert wurden und dabei ihre Funktionsebene angehoben wurde (die unter anderem bestimmt, welche Sicherheitsfeatures zur Verfügung stehen), wurden bestehende Fehlkonfigurationen oft nicht systematisch gesucht und behoben.

Sicherheitsforscher wie Sean Metcalf, der seit 2012 den Blog adsecurity.org betreibt, berichten seit Langem im Web und auf vorrangig englischsprachigen Konferenzen wie der Black Hat über Lücken in typischen AD-Umgebungen – bei vielen IT-Verantwortlichen fehlt aber das Bewusstsein für diese Art von Schwachstellen.

Inzwischen hat sich eine blühende Sicherheitsindustrie rund um die Absicherung des Active Directory entwickelt (einige Beispiele siehe ix.de/z9j3). Wie aber meist in der IT-Sicherheit können Werkzeuge nur ein Baustein im Sicherheitskonzept sein. Das grundlegende Verständnis bei Verantwortlichen und Detailkenntnisse bei Administratoren sind wesentlich wichtiger.

Das neue Sicherheitsbewusstsein

In dieser Hinsicht hat sich allein in den vergangenen Monaten einiges getan: Der Sicherheitsforscher Nikhil Mittal hat auf der englischsprachigen Onlinelernplattform „Pentester Academy: Red Team Labs“ virtuelle Labore und zugehörige Videokurse veröffentlicht, in denen Penetrationstester, Sicherheitsberater und andere Interessierte Angriffe auf AD-Umgebungen und deren Verteidigung lernen können. Die Heidelberger IT-Sicherheitskonferenz „Troopers“ bietet seit 2018 einen eigenen Vortragstrack zu Active Directory und Ende 2019 erschien auf Deutsch das



Mithilfe eines Windows-Dienstes, der mit den Rechten eines Domänenadministrators gestartet wird, können Angreifer die gesamte Domäne unter ihre Kontrolle bringen (Abb. 2).

Buch „Penetration Testing mit Mimikatz“, einem der beliebtesten Werkzeuge für Angriffe auf Domänen.

Die mit dieser *iX* beginnende Artikelreihe soll ein weiterer Vorstoß sein, Verteidiger sowie Pentester zu schulen; sie basiert auf den Vorarbeiten vieler Sicherheitsforscher. Denn wie oben beschrieben: Kriminelle wissen längst sehr gut Bescheid.

Fehlkonfigurationen – schlimmer als Softwarebugs?

Es ist keine leichte Aufgabe für eine große Organisation, die gesamte AD-Konfiguration zu überprüfen. Große Active-Directory-Umgebungen ändern sich im Detail häufig und viele IT-Verantwortliche haben Schwierigkeiten, die mit AD-Fehlkonfigurationen verbundenen Risiken wirklich zu verstehen.

Aus diesem Grund verwalten Organisationen ihre AD-Sicherheit kaum, und so gibt es nach wie vor eine Vielzahl von Fehlkonfigurationen – die aber erheblich das Risiko erfolgreicher Hacker- oder Malwareangriffe erhöhen.

Eine schlecht konzipierte Rechteverwaltung im Active Directory ist eine Hauptquelle für Risiken. Benutzer im Active Directory können über direkte Rechte an anderen Objekte verfügen, aber auch Mitglieder von Gruppen oder Eigentümer von Objekten sein, die in der Lage sind, Berechtigungen an andere zu delegieren. Clientrechner von normalen Benutzern sind wie Server ebenfalls Objekte im Active Directory und können aktive Sitzungen zu anderen Maschinen haben und ebenfalls Mitglieder in Gruppen sein. Es sind Beziehungen im Spiel und diese Beziehungen sind oft implizit und wenig intuitiv. Angreifer sind weitaus geschickter darin als Administratoren, diese Lücken zu finden und auszunutzen, indem sie Angriffspfade durch eine Umgebung schlagen, um Zugang zu Daten und Diensten zu erhalten, die eigentlich isoliert sein sollten.

Angreifer denken in Graphen, Verteidiger in Listen

Eine oft grundlegende Verteidigungsmaßnahme in Unternehmen ist die Inventarisierung und Klassifizierung von Schutzobjekten in Form von Asset-Inventaren oder Konfigurationsdatenbanken (Configuration Management Database, CMDB). Das Ziel dahinter ist klar: Was man nicht kennt, kann man nicht schützen.

So wichtig solche Inventarisierungsbemühungen sind – oftmals werden dabei jedoch sicherheitstechnisch relevante Beziehungen zwischen den Assets vernachlässigt. Diese ergeben sich beispielsweise, wenn derselbe Benutzer Zugang zu verschiedenen Systemen besitzt, für verschiedene lokale Administratorenkonten dasselbe Passwort verwendet oder wenn ein zentral gehostetes Skript auf verschiedenen Systemen ausgeführt wird. Es genügt folglich nicht, einzelne wertvolle Systeme wie Domänencontroller technisch bestmöglich abzusichern, dabei aber außer Acht zu lassen, wer sich wie und von wo damit verbindet.

Auf diesen Umstand weist das in der IT-Sicherheitsbranche öfter zitierte Bonmot von John Lambert hin, dem Leiter des Threat Intelligence Center von Microsoft: „Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win“ (Lamberts Blogeintrag dazu siehe ix.de/z9j3). Während Vertei-

diger also mit ihren Inventaren und Datenbanken Systeme isoliert im Blick behalten, nutzen Angreifer gezielt die Beziehungen zwischen diesen aus, um sich so Schritt für Schritt zu ihrem eigentlichen Ziel vorzuarbeiten. Dabei genügt es ihnen, wenn sie in einer Barrikade nur eine Lücke finden, während Verteidiger stets alle Schwachstellen in den verschiedenen Ebenen ihrer Sicherungslinien kennen und beseitigen müssen.

Aus Angriffskenntnissen Schutzmaßnahmen ableiten

Um das Vorgehen der Täter besser zu verstehen und daraus Schutzmaßnahmen abzuleiten, bilden dieser und die folgenden Artikel den Auftakt zu einer Reihe, die sich typischen Sicherheitsmängeln von Active-Directory-Installationen widmet, durch die das AD schnell komplett kompromittiert werden kann. Insbesondere geht die Reihe dabei auf schwache Standardeinstellungen, fehlende Härtungsmaßnahmen und unabsichtliche Fehlkonfigurationen ein.

Der Fokus liegt auf On-Premises-Installationen. Cloud-Dienste wie Azure Active Directory (Azure AD) oder unternehmensübergreifende Lösungen wie Active Directory Federation Services (ADFS) werden nicht berücksichtigt, um den Rahmen nicht zu sprengen.

Die Artikelreihe setzt voraus, dass der Leser mit dem grundlegenden Ablauf eines Angriffs auf IT-Systeme vertraut ist (Beispiele finden sich in früheren *iX*-Ausgaben, siehe ix.de/z9j3). Die skizzierten Szenarien gehen nach dem „Assume Breach"-Ansatz davon aus, dass sich ein Angreifer erfolgreich initial Zugang zum internen Netzwerk verschaffen konnte.

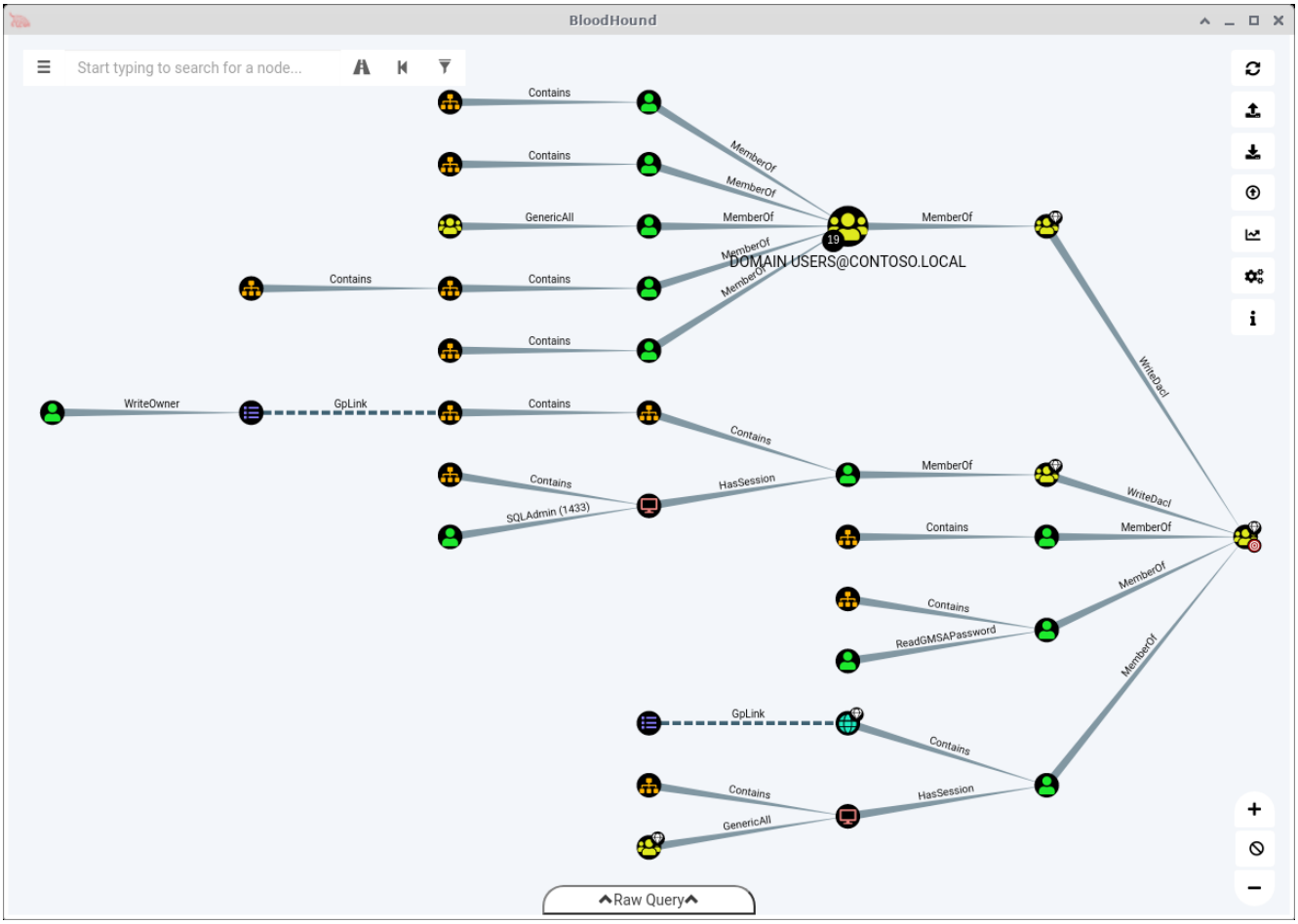
Zudem wird angenommen, dass eine Organisation wesentliche Sicherheitsgrundregeln beherzigt, beispielsweise Client- und Serverbetriebssystemversionen verwendet, die der Hersteller noch regulär unterstützt – also auf Servern mindestens Windows Server 2012 (R2) und auf Clients Windows 8.1 oder Windows 10 in einer noch gepflegten Version.

Ebenso sollte zügiges Einspielen von Patches selbstverständlich sein. Es werden keine Schwachstellen vorgestellt, die durch Installieren von Sicherheitsupdates beseitigt werden können. Das heißt nicht, dass Kernbereiche des Active Directory frei von klassischen Schwachstellen durch Bugs wären. Wenn sie aber von Microsoft garantierte Sicherheitseigenschaften verletzen, werden sie in der Regel zügig behoben. Beispiele aus jüngerer Zeit sind die Schwachstellen „Drop the MIC", bei der Integritätsprüfungen in der Net-NTLM-Authentifizierung ausgehebelt und darin Felder manipuliert werden konnten, und „PrivExchange" in Microsofts Maildienst Exchange, bei der Zugriff auf ein Exchange-Postfach genügte, um zum Domänenadministrator zu werden. Beide Lücken sind inzwischen gestopft.

Informationspreisgaben und einfache Angriffe

Um die Schwachstellen und Angriffsvektoren des Active Directory zu verstehen, ist eine Kenntnis der grundlegenden Konzepte, Strukturen und verwendeten Protokolle nötig, beispielsweise Net-NTLM oder Kerberos zur Authentifizierung.

Dabei werden immer wieder überraschende Eigenschaften deutlich: etwa, dass eine Domäne keine Sicherheitsgrenze bil-



Der „BloodHound" spürt den kürzesten Weg zu Domänenadministratoren auf (Abb. 3).

det, sondern nur die übergeordnete Einheit des Forest (auf Deutsch: Gesamtstruktur). Das bedeutet: Wird nur eine einzige Domäne gehackt, fällt mit ihr der gesamte Forest. Oder: In der Standardeinstellung kann jeder Benutzer einer Domäne neue Rechner an ihr anmelden. Möchte ein Insider ungestört von Malwarescannern arbeiten, kann er einen eigenen Rechner an der Domäne registrieren. Weitere Grundlagen beschreibt der Artikel „Allgegenwärtig“ auf Seite 48.

Aufbauend auf den skizzierten Konzepten und Funktionsweisen des Active Directory lässt sich das weitere Vorgehen von Angreifern nachzeichnen. Wie überraschend gesprächig Domänencontroller gegenüber allen angemeldeten Benutzern sind und wie viele Informationen jedes normale Domänenmitglied auslesen kann, ohne dazu besondere Rechte auf dem lokalen System oder innerhalb des AD zu benötigen, zeigt der Artikel „Nach oben gehangelt“ auf Seite 58. Zahlreiche weitere Angriffsmethoden und Schutzmaßnahmen kommen in den nächsten Heften zur Sprache.

Neben anderen offensichtlich klaffenden Lücken wie Passwörtern in einer Excel-Tabelle, die auf einer Netzfreigabe für jeden angemeldeten Benutzer zugänglich sind, wird in einer kommenden *iX*-Ausgabe demonstriert, warum Windows-Dienste nicht mit zu hoch privilegierten Domänenaccounts gestartet werden sollten – jeder lokale Administrator kann die Passwörter für diese Konten aus der Registrierungsdatenbank im Klartext auslesen. Ist der für den Dienst verwendete Domänenaccount ein Domänenadministrator, ist das AD gefallen.

Vom normalen Benutzer zum Domänenadmin

Im Lauf der Reihe werden Wege gezeigt, wie ein Angreifer nur mit physischem Zugriff auf eine Domänenumgebung über Spoofing und Relaying erste Benutzerkonten knacken kann. Eine ältere (und bei nicht gehärteter Konfiguration noch immer funktionierende) Methode dafür wurde bereits in einem *iX*-Artikel [1] beschrieben.

Inzwischen helfen auch grafische Werkzeuge wie BloodHound (siehe ix.de/z9j3) dabei, Beziehungen zwischen Benutzern und Computern zu visualisieren (Abbildung 3), und zeigen Angreifern etwa den schnellsten Weg vom zuerst kompromittierten Benutzer auch über viele Zwischenstationen zu einem Domänenadministrator. Für die Suche nach privilegierten Benutzern hat sich bezeichnenderweise der Name „User Hunting“ (auf Deutsch: Benutzerjagd) etabliert. Komplexe Angriffswege mit mehreren Schritten, die Angreifer früher in wochenlanger Arbeit manuell heraussuchen mussten, apportiert ihnen der Bluthund unmittelbar.

Benutzen Administratoren etwa ein Domänenadmin-Konto, um sich an normalen Windows-Servern anzumelden oder um mit diesem Account regelmäßig die gesamte Serverumgebung per Schwachstellenscanner oder Inventarisierungstool automatisiert zu prüfen, wobei sich der jeweilige Dienst an den einzelnen Rechnern anmeldet, ist der Zugang des Domänenadmins leichte Beute.

Hat ein Angreifer den Rechner eines Benutzers oder einen Server mit angemeldeten Administratoren kompromittiert, dient oft das Werkzeug Mimikatz dazu, deren Zugangsdaten in Form von Hashes – und in bestimmten Fällen selbst in modernen Umgebungen als Klartextpasswörter – aus dem Arbeitsspeicher auszulesen (Abbildung 4). Mimikatz wurde auch in prominenten Fällen eingesetzt, etwa beim „Bundestagshack“.

Überhaupt sind Hashes für Angreifer interessant: Haben sie etwa bereits einen Administrator der Domäne kompromittiert, können sie die Passwort-Hashes aller Benutzer und Computer im sogenannten DCSync-Angriff einfach vom Controller abfragen oder dessen Datenbank NTDS.dit kopieren und offline daraus alle Geheimnisse der Domäne auslesen.

Mit den gewonnenen Zugangsdaten bewegen sich Angreifer innerhalb der Umgebung und machen sich dabei Eigenheiten der Authentifizierungsprotokolle Net-NTLM und Kerberos zunutze. Diese Bewegung innerhalb der Umgebung wird unter Hackern „Lateral Movement“ genannt [2].

Da brat mir einer ein Passwort!

Aber auch auf anderen Wegen kommt man im AD an mehr Rechte: Wenn an einem Dienstkonto nur ein schwaches Passwort gesetzt ist, gelingt es Angreifern unter Umständen, mit der Angriffstechnik „Kerberoasting“ (für das „Braten von Kerberos“) dieses Passwort durch Brute Force oder Wörterlisten mit einem Passwortcracker zu knacken – und all das offline, ohne dafür weiter an der Domäne angemeldet zu sein.

Unter Systemverwaltern wenig bekannt: Mitglieder in manchen Gruppen wie DNS-Administratoren (DnsAdmins), Kontenoperatoren (Account Operators) oder Sicherungsoperatoren (Backup Operators) sind nur wenige Kommandozeilenbefehle davon entfernt, Domänenadministratoren zu werden – also lohnende Ziele für Angreifer.

Ebenso bei Fehlkonfiguration in Bezug auf Gruppenrichtlinien schlummert das Potenzial für Angreifer, höhere Privilegien innerhalb der AD-Umgebung zu erlangen: Wenn zu viele Benutzer Rechte zum Bearbeiten von Gruppenrichtlinien haben oder bestehende Richtlinien mit anderen Organisationseinheiten verknüpfen können. Aber auch bei individuell vergebenen Rechten besteht das Risiko. Das Recht „WriteOwner“ erlaubt es, den Objekteigentümer zu ändern. Damit kann ein vom Angreifer kontrollierter Benutzer das Objekt übernehmen.

Eine ähnliche Gefahr der Privilegienerhöhung lauert bei den verschiedenen Arten der Kerberos-Delegierung, bei der ein Server im Namen eines Benutzers agieren kann, um den Zugriff auf Ressourcen auf anderen Systemen ohne erneute Eingabe der Anmeldedaten zu ermöglichen. Jede Art von Delegierung – uneingeschränkte, eingeschränkte und selbst ressourcenbasiert eingeschränkte – kann auf individuelle Art missbraucht werden.

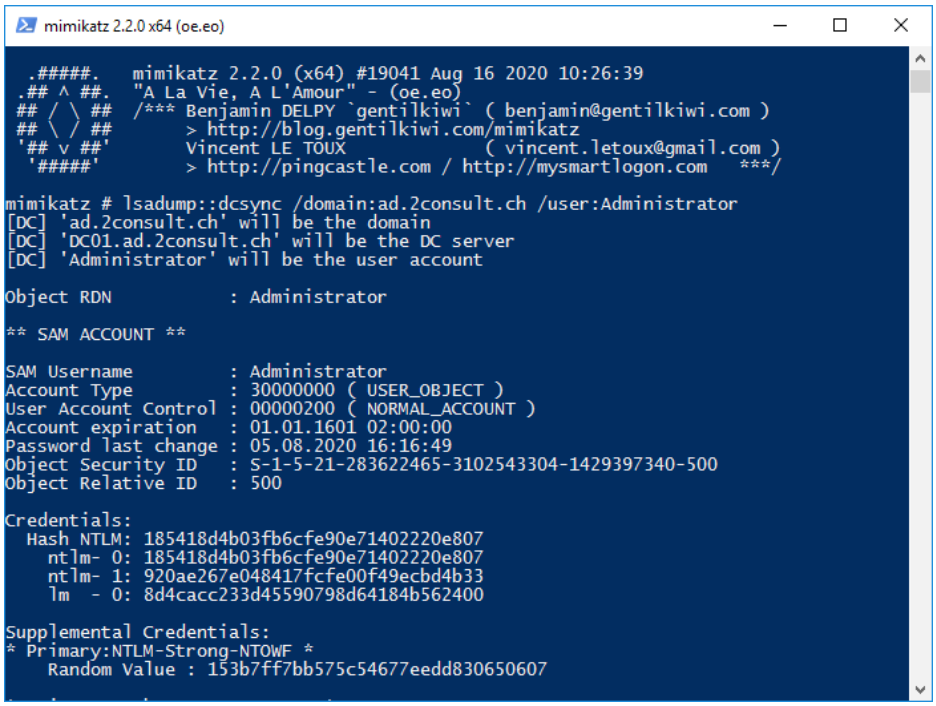
Nicht nur einen Baum, sondern den kompletten Wald

Da der Forest von Microsoft als Sicherheitsgrenze implementiert wurde, können Angreifer wegen des Vertrauensverhältnisses zwischen Domänen innerhalb eines Forest zu Administratoren anderer Domänen oder Enterprise-Administratoren der Gesamtstruktur werden. Dabei helfen wenig bekannte Artefakte wie Trust-Tickets oder die SID-Historie (Security Identifier) – Letztere ursprünglich geschaffen, um die Migration mehrerer ADs im Zuge von Unternehmenszusammenschlüssen zu bewältigen.

Doch selbst zwischen zwei Forests kann es durch fehlerhafte Administration, freimütig vergebene Rechte oder Forestübergreifend verkettete Komponenten wie SQL-Server für einen Angreifer möglich sein, von einer Gesamtstruktur auf die andere Gesamtstruktur überzuspringen.

Persistenz: langfristig und unbemerkt festgesetzt

Ist es einem Angreifer einmal gelungen, zum Domänenadministrator zu werden, hat er viele Möglichkeiten, seinen Zugriff



Mit Mimikatz wird beim DCSync-Angriff zum Beispiel der Passwort-Hash des Domänenadministrators vom Controller abgefragt (Abb. 4).

dauerhaft und vom Opfer mehr oder weniger unbemerkt zu sichern. Naheliegend, aber auffällig ist das Erstellen eines neuen Administratorkontos.

Wegen der Eigenheiten von Kerberos kann sich ein Angreifer mit Kenntnis des zentralen AD-Geheimnisses – des krbtgt-Hashes – ein sogenanntes „goldenes Ticket" ausstellen, ein Langzeit-Ticket, das ihn als Mitglied der Gruppe der Domänenadministratoren ausweist und das er jederzeit wieder vorzeigen kann – selbst dann, wenn alle kompromittierten Accounts gelöscht wurden. Damit ein solches Ticket ungültig wird, muss dessen Kompromittierung zunächst auffallen und die Verteidiger müssen einigen Aufwand betreiben. Analog dienen „silberne Tickets" zum Zugriff auf einzelne Dienste, wenn man deren Geheimnis kennt.

Auch indem ein Angreifer sich gezielt spezifische Rechte auf einzelne Objekte im AD verschafft oder deren Eigenschaften subtil verändert, kann er sich persistenten Zugriff sichern, mit einem normalen Benutzerzugang immer wieder via DCSync die Passwort-Hashes sämtlicher Konten abfragen oder Konten so verändern, dass Roasting-Angriffe zum Passwortknacken möglich sind. Ähnliche Hintertüren zum dauerhaften Zugriff auf einzelne Systeme können durch Rechteveränderungen auf Servern oder Clients eingerichtet werden.

Selbst das von Administratoren oft stiefmütterlich behandelte Passwort für den Verzeichnisdienst-Wiederherstellungsmodus (Directory Service Restore Mode, DSRM), das sie beim Aufsetzen einer Domäne eingeben müssen, kann nicht nur als Einfallstor zur Anmeldung auf einem Domänencontroller dienen – sondern auch als Hintertür, wenn Angreifer es selbst vergeben und die inzwischen sichere Konfiguration so verändern, dass es zur Remoteanmeldung genutzt werden kann.

Technisch einer der interessantesten Angriffe ist DCShadow. Hier gibt der Angreifer gegenüber einem Domänencontroller vor, ein anderer (Schatten-)Domänencontroller zu sein, der ihm neue Daten übermitteln will. Dadurch kann er Änderungen vornehmen, ohne dass die sonst üblichen Logeinträge entstehen. Damit kann er auch SIEM-Produkte (Security Information and Event Management) umgehen, deren Hauptaufgabe das Sammeln und Korrelieren solcher Logs zu Sicherheitszwecken ist.

All dies macht deutlich, dass eine einmal kompromittierte Umgebung nicht verlässlich gesäubert werden kann, sondern komplett neu aufgebaut werden muss.

Verteidigen, erkennen und täuschen

Die detaillierte Kenntnis der Einfallstore und Angriffsarten ist die Basis dafür, dass Administratoren lernen, ihre AD-Umgebung abzusichern. Neben generellen Härtungsmaßnahmen wie der spärlichen Vergabe von Domänenadministratorrechten und der gezielten Delegierung von Einzelrechten im Sinne eines „Least Privilege"-Modells (Vergabe des niedrigsten Rechts, das für eine Aufgabe erforderlich ist), dem Nutzen von sicheren Workstations zur Administration oder der Einführung von Verwaltungsebenen (Tiers) gilt es, die einzelnen Angriffe auf ihre Abwehrstrategie hin zu analysieren. Dienlich dabei können auch die Werkzeuge der Angreifer sein (PowerView oder BloodHound), mit denen man Schwachstellen in der eigenen Umgebung findet. Auch damit wird sich ein Artikel der Serie befassen.

Wichtig ist nicht nur das Verhindern, sondern auch das Erkennen von Angriffen. Man muss immer damit rechnen, dass die eigene AD-Umgebung von innen oder außen unter Beschuss steht. Insbesondere Domänencontroller verarbeiten viele Anfragen. Wenn dort keine Spuren eines Angriffs entdeckt werden, ist ein Einbruch unter Umständen schwierig zu erkennen. Dabei helfen das gezielte Scharfschalten von Log- und Auditeinstellungen sowie das zentrale Auswerten der entstehenden Protokolle im Rahmen eines Monitorings.

Den Abschluss der Reihe bilden Hinweise zum Aufstellen von Stolperfallen für Angreifer unter dem Schlagwort „Tricksen und Täuschen": Honigtopf-Maschinen und vermeintlich fehlkonfigurierte Konten, die aussehen, als seien sie echt, bei Missbrauch aber Alarm auslösen. Sie sollen helfen, Angriffsversuche schnell zu erkennen, und führen Angreifer in die Irre. Damit können Systemverwalter auch ohne kommerzielle Werkzeuge Angreifer in ihrer Umgebung aufspüren und in die Falle locken. (ur@ix.de)

Quellen

[1] Hans Martin Münch; Mein Name ist Hase; Kompromittierung von Windows durch LLMNR Spoofing und NTLM Relaying; *iX* 10/2016, S. 106

[2] Sascha Herzog; Seitwärtsbewegungen, Red Teaming – Post Exploitation and Lateral Movement; *iX* 12/2018, S. 82

[3] Sämtliche im Artikel angesprochenen Angriffe und Werkzeuge sowie weitere Informationen sind über ix.de/z9j3 zu finden.

Frank Ully

ist Chief Technology Officer der Oneconsult Deutschland GmbH in München. Er beschäftigt sich mit aktuellen Themen der offensiven IT-Sicherheit.