Der Verzeichnisdienst Active Directory: einer für alle(s)

Allgegenwärtig

Frank Ully

Nicht zuletzt die Komplexität des Active Directory und die Fülle der darin enthaltenen Informationen sind es, die diesen Dienst so angreifbar machen. Um ihn abzusichern, gilt es zunächst, seine Struktur und seine Arbeitsweise zu verstehen.

Ein Verzeichnis dient dem Ablegen von Informationen: In einem Telefonverzeichnis stehen Informationen zu Telefonanschlüssen und deren Besitzer, ein Verzeichnis im Dateisystem beinhaltet Informationen zu den darin enthaltenen Dateien. Ein Verzeichnisdienst stellt Methoden zum Speichern, Verwalten und Abfragen der Informationen bereit.

Das Active Directory ist Microsofts Verzeichnisdienst, der Informationen zu Objekten in Netzwerken verwaltet. Das sind sowohl Geräte wie Clientrechner, Server oder Drucker als auch Dienste und Dateifreigaben sowie Benutzer und Gruppen. Zu jedem Objekt werden Informationen in Form von Attributen gespeichert, zum Beispiel Name, Standort oder Abteilung.

Kernstück des Active Directory: die Domäne

Im AD gespeicherte Daten werden dem Nutzer in einer hierarchischen Struktur präsentiert – ähnlich wie Verzeichnisse, Unterverzeichnisse und Dateien in einem Dateisystem. Innerhalb dieser hierarchischen Struktur werden zwei Arten von Objekten unterschieden: Container enthalten weitere Objekte, das heißt weitere Container oder Nicht-Container. Nicht-Container enthalten keine weiteren Objekte. Man bezeichnet sie daher auch als Endknoten oder Leaf (Blatt).

Ein Container kann beispielsweise eine Organisationseinheit sein, die mehrere Benutzer umfasst. Die Benutzer selbst sind hingegen Endknoten, da sie keine weiteren Objekte enthalten.

Die Basis der Hierarchie bildet ein spezielles Containerobjekt: die Stammdomäne. Für weitere strukturelle Unterteilungen und Gruppierungen können unterhalb der Stammdomäne zusätzliche Domänen angelegt werden. Eine solche Hierarchie von Domänen wird als Domänenbaum bezeichnet.

Jede Domäne muss über einen eindeutigen Namen verfügen, der den Konventionen des Domain Name Systems (DNS) folgt, beispielsweise ad.2consult.ch. Innerhalb eines Domänenbaums leitet sich der Domänenname einer Kinddomäne entsprechend von der Elterndomäne ab, beispielsweise produktion.ad.2consult.ch und entwicklung.ad.2consult.ch.

Die Domäne fungiert nicht nur als strukturierendes Element, das eine Gruppe von Containern und Objekten enthält. Sie dient vor allem als Verwaltungseinheit, die beispielsweise steuert, dass nur berechtigte Benutzer und Systeme Zugriff auf Ressourcen erhalten. Zudem ist sie

eine administrative Grenze beim Anwenden von Sicherheitsrichtlinien und -einstellungen.

So setzt sich die Sicherheitskennung SID zusammen (Abb. 1).

SID		Revisionsnummer		Identifier Authority		Domänen-SID		RID
S	-	1	-	5	-	21-1004336348-1177238915-682003330		- 512

Ordentlich sortiert: Benutzer, Computer und Co.

Benutzer- und Computerkonten bilden tatsächliche physische Gegebenheiten ab, zum Beispiel einen Mitarbeiter oder einen Rechner im Unternehmen. Mit einem individuellen Konto kann sich ein Benutzer an einem Computer in der Domäne anmelden und auf Ressourcen darin zugreifen. Neben personenbezogenen Benutzerkonten gibt es zudem dienstbezogene Konten (Service Accounts), die von bestimmten Anwendungen – beispielsweise Exchange, SharePoint oder SQL-Server – genutzt werden.

Ein Computerkonto dient dazu, Clients und Server, die Teil des Netzwerkes sind, zu authentifizieren, für den Domänenzugriff zu autorisieren und Sicherheitsrichtlinien darauf anzuwenden. Das gewährleistet, dass eine Anmeldung in der Domäne nicht von jedem beliebigen Rechner erfolgen kann. Der Name der Computerkonten endet mit einem Dollarzeichen (zum Beispiel dateiserver01$ für den ersten Dateiserver), und sie haben außerdem ein Passwort – zufällig generierte 120 Zeichen, die in der Standardeinstellung automatisch alle 30 Tage wechseln.

Server innerhalb einer Domäne fungieren entweder als Domänencontroller – dazu in Kürze mehr – oder als Mitgliedsserver. In diese Kategorie fallen alle Server, die keine AD-Dienste bereitstellen, etwa Datei-, Datenbank- oder Webserver.

Sicherheitsgruppen bilden, Rechte zuteilen

Benutzer- und Computerkonten werden zur gemeinsamen Verwaltung in Gruppen zusammengefasst. Rechteeinstellungen für eine bestimmte Sicherheitsgruppe gelten für alle Mitglieder dieser Gruppe, also alle zugehörigen Benutzer- und Computerkonten oder Untergruppen.

Als weiteres Strukturierungsobjekt innerhalb einer Domäne dienen Organisationseinheiten, im Englischen Organizational Units (OU). Sie sind Container, die Abteilungen, Standorte oder Teams darstellen und die dazugehörigen Objekte konsistent verwalten. Durch OUs als administrative Einheiten können Berechtigungen zum Verwalten von Objektgruppen delegiert werden. Ein Abteilungsleiter kann etwa die Rechte erhalten, Objekte innerhalb seiner Abteilungs-OU zu verwalten. Ähnlich einer Domäne lässt sich eine OU in eine Struktur unterteilen und man kann Sicherheitsrichtlinien an sie knüpfen. Da OUs verwendet werden, um Sicherheitsrichtlinien anzuwenden, kann das Speichern von Benutzern oder Computern in einer falschen OU mittelbar zur Kompromittierung der Domäne führen.

Verwaltet wird die Domäne von Administratoren mit Protokollen wie Windows Management Instrumentation (WMI), PowerShell-Remoting (WinRM) oder dem klassischen Remote Desktop Protocol (RDP).

Eindeutige Sicherheitskennungen

Jedes Objekt innerhalb des Active Directory, einschließlich Domänen, OUs und Gruppen, besitzt eine eindeutige 128-Bit-Kennung, den Globally Unique Identifier (GUID).

Sicherheitsrelevante Objekte – sogenannte Sicherheitsprinzipale wie Benutzer- und Computerkonten – verfügen zusätzlich über eine Sicherheitskennung (Security Identifier, SID), die domänenspezifisch ist. Wird beispielsweise ein Benutzerkonto von einer Domäne in eine andere verschoben, ändert sich auch die Haupt-SID des Benutzerkontos und die alte SID wird in einer Historie gespeichert.

Dies hängt mit dem in Abbildung 1 dargestellten Aufbau von SIDs zusammen, die aus der SID der Domäne und einer Objekt-ID (Relative Identifier, RID) bestehen.

Es gibt eine Reihe festgelegter RIDs, beispielsweise 512 für Domänenadministratoren. Regulär angelegte Konten beginnen in der Zählung bei 1000. Zur Identifizierung von Konten, Autorisierung und Zugriffssteuerung wird im Active-Directory-Kontext aus Gründen der Abwärtskompatibilität stets die SID, nicht die GUID verwendet.

Der zentrale Server und seine Datenbank

Der Domänencontroller (Domain-Controller, DC) ist das Herz einer Domäne und verantwortlich für die Authentifizierung von Nutzern, die Zugriffskontrolle auf Ressourcen sowie das Hinzufügen, Bearbeiten und Entfernen von Objekten und Attributen innerhalb einer Domäne. Aus diesem Grund sollte der Domänencontroller möglichst auf einem dedizierten Server laufen und keinesfalls gleichzeitig als Mail- oder Dateiserver fungieren. Bei einem Ausfall des Domänencontrollers können Benutzer sich nicht mehr in der Domäne anmelden. Um einen Single Point of Failure zu vermeiden, gibt es in der Regel mehrere Controller pro Domäne.

Das AD ist nur auf der Präsentationsebene eine hierarchische Struktur. Auf der Speicherebene handelt es sich tatsächlich um eine flache Datenbank mit nur drei Tabellen. Diese Datenbank wird auf Domänencontrollern in der Datei NTDS.dit gespeichert, standardmäßig im Verzeichnis %SystemRoot%\NTDS. Sollte sie dort nicht zu finden sein, lässt sich der Speicherort über den Registrierungsschlüssel HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters\DSA Database File ermitteln.

Die NTDS.dit enthält alle Daten einer Domäne, einschließlich der Passwort-Hashes von Benutzern. Die sogenannte Multi-Master-Replikation stellt sicher,

iX-TRACT

- Um das Active Directory abzusichern, ist eine gute Kenntnis aller Elemente und ihrer Zusammenhänge sowie der Funktionsweise des AD nötig.
- Die Sicherheit des Verzeichnisdienstes steht und fällt mit gut aufgesetzten Authentifizierungsprozessen, Zugriffslisten und Vertrauensbeziehungen.
- An zahlreichen Schaltstellen können Systemverantwortliche durch falsches Konfigurieren den Dienst ungewollt angreifbar machen.
- Eine der wenig bekannten Kardinalregeln der AD-Sicherheit: Nicht die Domäne ist die Sicherheitsgrenze, sondern der Forest.

dass die Daten auf allen Domänencontrollern konsistent sind und alle Änderungen enthalten, die einer der Controller vornimmt. Das bedeutet, dass eine Domäne als Replikationsgrenze fungiert, da gespeicherte Objektdaten nur zwischen Domänencontrollern derselben Domäne repliziert werden.

Die NTDS.dit ist zwar verschlüsselt, der verwendete Schlüssel steht aber in der Registry: Ein Benutzer, der etwa über ein altes Domänencontroller-Backup an eine Kopie von NTDS.dit und den Registrierungsschlüssel gelangt, kennt alle Domänengeheimnisse.

Wissen, wo nachsehen: DHCP, DNS und SMB

Wie kann ein Benutzer über das AD auf Ressourcen zugreifen? Voraussetzung dafür ist, dass der Client, über den der Benutzer eine Ressource anfordert, den Domänencontroller im Netzwerk findet. Dazu ist ein DNS-Server erforderlich, in dem Domänencontroller eine Reihe von Einträgen registrieren, um von Clients, aber auch von anderen Domänencontrollern gefunden zu werden. In der Regel hostet der Domänencontroller auch den DNS-Server und integriert die Konfiguration der DNS-Zonen ins AD, um einen separaten Mechanismus zu vermeiden.

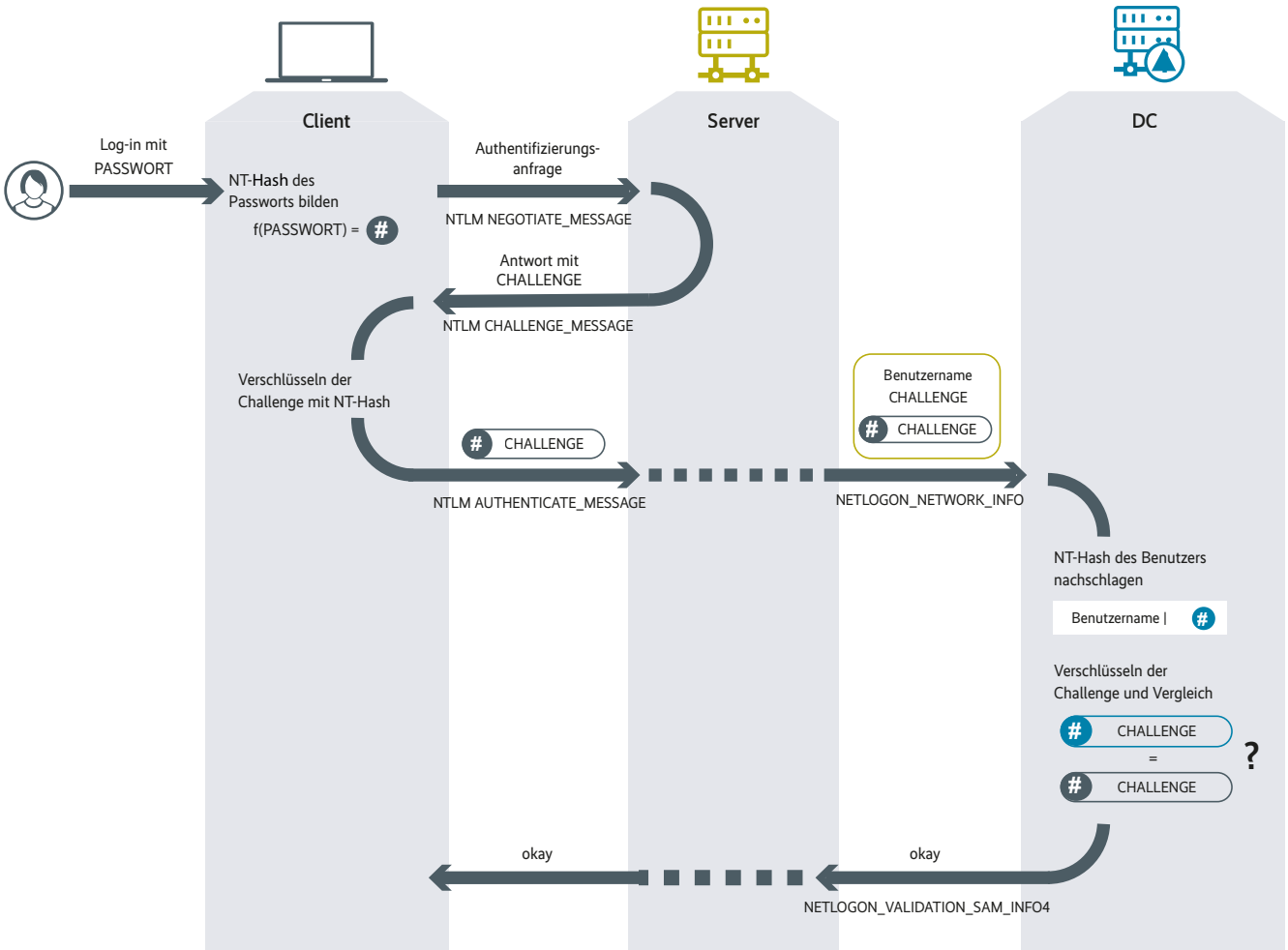
Das Dynamic Host Configuration Protocol (DHCP) gewährleistet, dass ein Windows-Client zunächst den DNS-Server findet. Der DHCP-Server, oft auch eine Funktion des Domänencontrollers, weist Clients in einem Netzwerk dynamisch IP-Adressen zu und übermittelt weitere Konfigurationen an sie, unter anderem die IP-Adresse des DNS-Servers.

Ist in einer Domäne einmal kein DNS-Server erreichbar, gibt es dezentrale Fallback-Mechanismen wie NetBIOS-Nameservice (NBT-NS), Link Local Multicast Name Resolution (LLMNR) oder Multicast DNS (mDNS), mit denen ein Client versucht, den Namen über Multicast-Anfragen ins lokale Netzwerk in eine IP-Adresse aufzulösen. Sind solche alternativen Auflösemechanismen in ihrer Standardeinstellung aktiv, werden Name-Spoofing-Angriffe möglich, die in einer früheren *iX*-Ausgabe beschrieben wurden [1] und in einer neuen Variante für IPv6 in einem der kommenden Artikel vorgestellt werden.

Für den tatsächlichen Zugriff auf eine Ressource spielt das Dateiübertragungsprotokoll SMB (Server Message Block) die Hauptrolle. SMB ermöglicht das Lesen und Schreiben von freigegebenen Verzeichnissen und den darin enthaltenen Dateien auf einem entfernten Rechner über ein lokales Netzwerk. Eine Implementierung von SMB ist das Common Internet File System, dessen Abkürzung CIFS zwar noch im AD-Kontext auftaucht, das als Protokoll selbst jedoch nur noch selten verwendet wird – seit Windows Server 2012 dient SMB 3 zum Dateiaustausch.

Weise nach, wer du bist

Bevor Zugriff auf eine Ressource gewährt wird, muss zunächst die Identität des anfragenden Sicherheitsprinzipals verifiziert werden, sprich, der Benutzer oder der Computer muss authentifiziert werden. Dazu unterstützt das AD sowohl das in die Jahre gekommene Protokoll Net-NTLM



Challenge und Response: So erfolgt der Authentifizierungsprozess mit dem Protokoll Net-NTML (Abb. 2).

(kurz für NT LAN Manager, auch häufig nur als NTLM abgekürzt) als auch das bevorzugt genutzte Kerberos.

Der Authentifizierungsmechanismus von Net-NTLM basiert auf einem Challenge-Response-Verfahren und umfasst vereinfacht folgende Schritte:

1. Der Benutzer meldet sich mit seinem Benutzernamen, seinem Passwort und dem Domänennamen auf einem Client an.
2. Der Client wandelt das Passwort um in einen NT-Passwort-Hash (der verwirrenderweise manchmal als NTLM-Hash bezeichnet wird).
3. Der Client kontaktiert den Server, auf den der Nutzer zugreifen möchte, und sendet den Benutzernamen.
4. Der Server antwortet mit einer Challenge, einer zufälligen Zeichenfolge.
5. Der Client verschlüsselt die Challenge mit dem Passwort-Hash des Benutzers und sendet sie zurück an den Server.
6. Der Server sendet Benutzername, Challenge und verschlüsselte Challenge an den Domänencontroller.
7. Der Domänencontroller schlägt den gespeicherten Passwort-Hash für den angegebenen Benutzernamen in der Datenbank nach und verschlüsselt damit die Challenge. Anschließend vergleicht er sein Ergebnis mit der vom Server gesendeten verschlüsselten Challenge. Sind beide gleich, heißt das, dass der Benutzer das korrekte Passwort verwendet hat.
8. Der Domänencontroller teilt dem Server mit, dass die Authentifizierung des Benutzers erfolgreich war.

Net-NTLM ist mehr als 20 Jahre alt und wurde seinerzeit nicht unter Sicherheitsaspekten entwickelt. In neueren Versionen wurde das Protokoll verstärkt. Beispielsweise fügt Net-NTMLv2 im fünften Schritt einen Zeitstempel bei, der Replay-Angriffe (Wiedereinspielung von Authentifizierungsdaten) unterbindet.

Dies behebt jedoch nicht andere Schwachstellen wie die veralteten kryptografischen Algorithmen – wodurch Passwörter mit Brute-Force- oder Wörterbuchangriffen geknackt werden können – oder das Fehlen einer gegenseitigen Authentifizierung von Client und Server, was Man-in-the-Middle-Angriffe ermöglicht.

Der Höllenhund: Kerberos

Standardauthentifizierungsprotokoll für das AD ist Kerberos. Sein Name leitet sich ab vom dreiköpfigen Höllenhund, der laut griechischer Mythologie den Eingang zur Unterwelt bewacht. Die drei Köpfe des Hundes stehen im übertragenen Sinn für die drei Komponenten, auf denen das Kerberos-Protokoll beruht: Client, Server und Key Distribution Center (KDC).

Das KDC besteht wiederum logisch aus dem Authentication Service (AS), der die Identität des Benutzers bestätigt und ihm ein Ticket Granting Ticket ausstellt, und dem Ticket Granting Service (TGS), der Tickets für den Zugriff auf Netzwerkressourcen ausgibt.

Das Active Directory verwendet eine Microsoft-eigene Kerberos-Implementierung mit Erweiterungen namens MS-KILE, die jedoch auf dem offenen Kerberos-Standard Version 5 basiert und sich auch für die Anbindung von Linux-Systemen eignet.

Die Authentifizierung umfasst folgende Schritte:

1. Der Benutzer meldet sich mit seinem Benutzernamen und seinem Passwort auf seinem Client an.
2. Der Client wandelt das Passwort in einen NT-Passwort-Hash um.
3. Der Client verschlüsselt einen Zeitstempel mit dem Passwort-Hash und sendet diesen an das Key Distribution Center des Domänencontrollers.
4. Das KDC schlägt den gespeicherten Passwort-Hash für den angegebenen Benutzernamen in der Datenbank nach und entschlüsselt damit den gesendeten Zeitstempel. Ist das Entschlüsseln nicht möglich, war das Passwort des Benutzers nicht korrekt.
5. Das KDC erstellt einen Sitzungsschlüssel und verschlüsselt diesen mit dem Passwort-Hash des Benutzers. Das KDC erstellt außerdem ein Ticket Granting Ticket (TGT) mit Informationen unter anderem zum Benutzernamen und Gültigkeitszeitraum sowie dem Sitzungsschlüssel. Das TGT wird mit dem Passwort-Hash des Kerberos-Service-Accounts (krbtgt) verschlüsselt und signiert. Sitzungsschlüssel und TGT werden an den Client geschickt.

Glossar

AS; Authentication Service: bestätigt Identität des Nutzers und stellt ihm ein Ticket Granting Ticket aus

CIFS; Common Internet File System: veraltete Implementierung des Netzprotokolls SMB für Datei-, Druck- und weitere Dienste

DFSR; Distributed File System Replication: repliziert Daten auf verschiedenen Controllern, um sie synchron zu halten

DHCP; Dynamic Host Configuration Protocol: ermöglicht die dynamische Zuweisung von IP-Adressen in einem Netzwerk

DN; Distinguished Name: bezeichnet den eindeutigen Pfad eines Objekts innerhalb des AD

GPO; Group Policy Object: Sammlung von Richtlinien für Benutzer und Computer

GUID; Globally Unique Identifier: 128-Bit-Kennung für verteilte Computersysteme

KDC; Key Distribution Center: Schlüsselverwaltungszentrale für angemeldete Nutzer in einem Netzwerk

LLMNR; Link-Local Multicast Name Resolution: Protokoll, um bei Ausfall des DNS einen Host im Netzwerk zu identifizieren

mDNS; Multicast DNS: Protokoll zum Auflösen von Hostnamen in IP-Adressen in Computernetzwerken ohne lokalen Nameserver

NBT-NS; NetBIOS-Nameservice: Teil des ursprünglichen NetBIOS-Stacks von Windows, Identifizierung eines Hosts im Netzwerk

Net-NTLM; NT LAN Manager: Authentifizierungsverfahren für Rechnernetze, oft auch nur als NTLM bezeichnet

OU; Organizational Unit: Organisationseinheit innerhalb einer Domäne

RDP; Remote Desktop Protocol: Microsofts Netzwerkprotokoll für Fernzugriff

RID; Relative Identifier: relative Kennung, die einem Objekt bei der Erstellung zugewiesen wird und Teil seiner Sicherheitskennung in einer Domäne wird

SID; Security Identifier: Sicherheitskennung auf der Basis des RID

SMB; Server Message Block: Dateiübertragungsprotokoll in Rechnernetzen

SPN; Service Principal Name: Name, über den ein Client eine Instanz eines Diensts eindeutig identifiziert

TGS; Ticket Granting Service: gibt Tickets für Zugriff auf Netzwerkressourcen an Nutzer aus

TGT; Ticket Granting Ticket: enthält Informationen zum Nutzer, Gültigkeitszeitraum sowie den Sitzungsschlüssel

WinRM; Windows Remote Management: Verwalten eines Rechners remote über Eingabeaufforderung; wird bei PowerShell Remoting genutzt

WMI; Windows Management Instrumentation: Kernfunktion des webbasierten Enterprise-Managements für Windows

6. Der Client nutzt den Benutzerpasswort-Hash, um den Sitzungsschlüssel zu entschlüsseln, und speichert das TGT.

Um nach der Authentifizierung Zugriff auf eine Ressource oder einen Dienst zu erhalten, sind folgende Schritte notwendig: Der Client sendet sein aktuelles Ticket Granting Ticket mit dem Service Principal Name (SPN) der angeforderten Ressource an das Key Distribution Center. Um seine Identität zu belegen, schickt der Client außerdem einen Authentikator mit seinem Benutzernamen und einen Zeitstempel, verschlüsselt mit dem Sitzungsschlüssel.

Das Key Distribution Center entschlüsselt mit seinem krbtgt-Passwort-Hash das TGT, das beim Anlegen der Domäne automatisch erstellt wurde. Dadurch erhält es den Sitzungsschlüssel und kann damit den Authentikator entschlüsseln. Gelingt das Entschlüsseln und stimmen die Informationen in TGT und Authentikator überein, gilt die Identität des Clients als bestätigt.

Das KDC stellt ein Ticket Granting Service (TGS) Ticket aus, indem es die Daten aus dem TGT-Ticket kopiert. Außerdem wird ein neuer Sitzungsschlüssel erzeugt und dem TGS-Ticket beigefügt. Das neue Ticket wird mit dem Passwort-Hash des gewünschten Dienstes verschlüsselt. Das TGS-Ticket und der neue Sitzungsschlüssel werden mit dem ersten Sitzungsschlüssel verschlüsselt und an den Client gesendet.

Der Client entschlüsselt die Nachricht mit dem ersten Sitzungsschlüssel und erhält so das Ticket Granting Service Ticket und den neuen Sitzungsschlüssel. Der Client erzeugt erneut einen Authentikator mit seinem Benutzernamen sowie einem Zeitstempel und verschlüsselt diesen mit dem neuen Sitzungsschlüssel. Nun kontaktiert er den gewünschten Service und präsentiert den Authentikator sowie das TGS-Ticket.

Der Service entschlüsselt das TGS-Ticket mit seinem eigenen Passwort-Hash und erhält so den neuen Sitzungsschlüssel. Mit dem neuen Sitzungsschlüssel kann der Service nun den Authentikator entschlüsseln und dessen Informationen mit denen im TGS-Ticket vergleichen. Stimmen sie überein, gewährt der Service dem Client Zugriff.

Einmal authentifizieren, mehrfach zugreifen

Dank Kerberos ist Single Sign-on in Windows-Domänen möglich. Nach der initialen Authentifizierung stellt das Protokoll im Hintergrund eine Vertrauensbeziehung zu anderen Domänenmitgliedern sicher und es ist nicht notwendig, sich bei jedem Dienst innerhalb der Domäne einzeln zu authentifizieren.

Auch wenn Kerberos einige konzeptionelle Schwachstellen von Net-NTLM behebt, bietet es Angriffspunkte. Da der krbtgt-Passwort-Hash als Vertrauensanker dient, kommt ein Verlust dieses Passwort-Hashes dem Verlust der Kontrolle über das Active Directory gleich.

Damit Kerberos einem anfragenden Client ein Session-Ticket für den Zugriff auf einen Dienst ausstellen kann, muss der Dienst eindeutig identifizierbar sein. Dies geschieht über den Service Principal Name (siehe ix.de/zvnk), der für den Zugriff auf eine Netzwerkfreigabe auf einem Dateiserver beispielsweise lautet: CIFS/DATEISERVER01.ad.2consult.ch.

Der dreiköpfige Höllenhund nutzt SPNs, daher funktioniert Kerberos nicht, wenn eine IP-Adresse als Verweis auf den Server verwendet wird: also etwa \\10.0.0.100 anstelle von \\dateiserver01. Die Authentifizierung fällt dann auf Net-NTLM zurück.

Das Gegenstück zum SPN für Dienste ist der UPN (User Principal Name) für Benutzer: Zur Anmeldung am AD kann statt des Schemas Domäne\Benutzername auch der Benutzerprinzipalname verwendet werden. Er setzt sich aus dem Anmeldenamen des Benutzers und dem UPN-Suffix zusammen, verbunden durch ein @-Zeichen. Um Verwirrung zu vermeiden, sind oft UPN und E-Mail-Adresse identisch, zum Beispiel peter.pan@2consult.ch.

Daten einfach auslesen: LDAP

Zur direkten Kommunikation mit dem AD – also zum Abfragen und Austauschen von Informationen zu Objekten – dient das Lightweight Directory Access Protocol (LDAP). Jedes Objekt innerhalb des AD hat einen sich aus der Hierarchie ableitenden Pfad, an dem es existiert, einen sogenannten Distinguished Name (DN). Dieser setzt sich aus dem Namen des Objekts (Common Name, CN), den übergeordneten Organisationseinheiten (Organizational Unit, OU) und dem Domänennamen (Domain Component, DC) zusammen.

Beispielsweise kann ein Distinguished Name für den Benutzer Peter Pan lauten: CN=Peter Pan, OU=Lostboys, DC=ad, DC=2consult, DC=ch.

Über LDAP-Abfragen können Objekte gezielt anhand ihrer Attribute gesucht und Informationen dazu abgerufen werden, beispielsweise alle Benutzer der Domänenadministratorgruppe. Dank LDAP ist der Austausch von Benutzern, Gruppen und weiteren Informationen aus dem AD mit anderen Systemen möglich. So lassen sich diese Informationen zentral verwalten und mit verknüpften Anwendungen synchronisieren.

Wie der Artikel „Nach oben gehangelt“ auf Seite 58 zeigt, können Angreifer über LDAP allerdings sehr einfach interessante Daten über die Domänenumgebung auslesen.

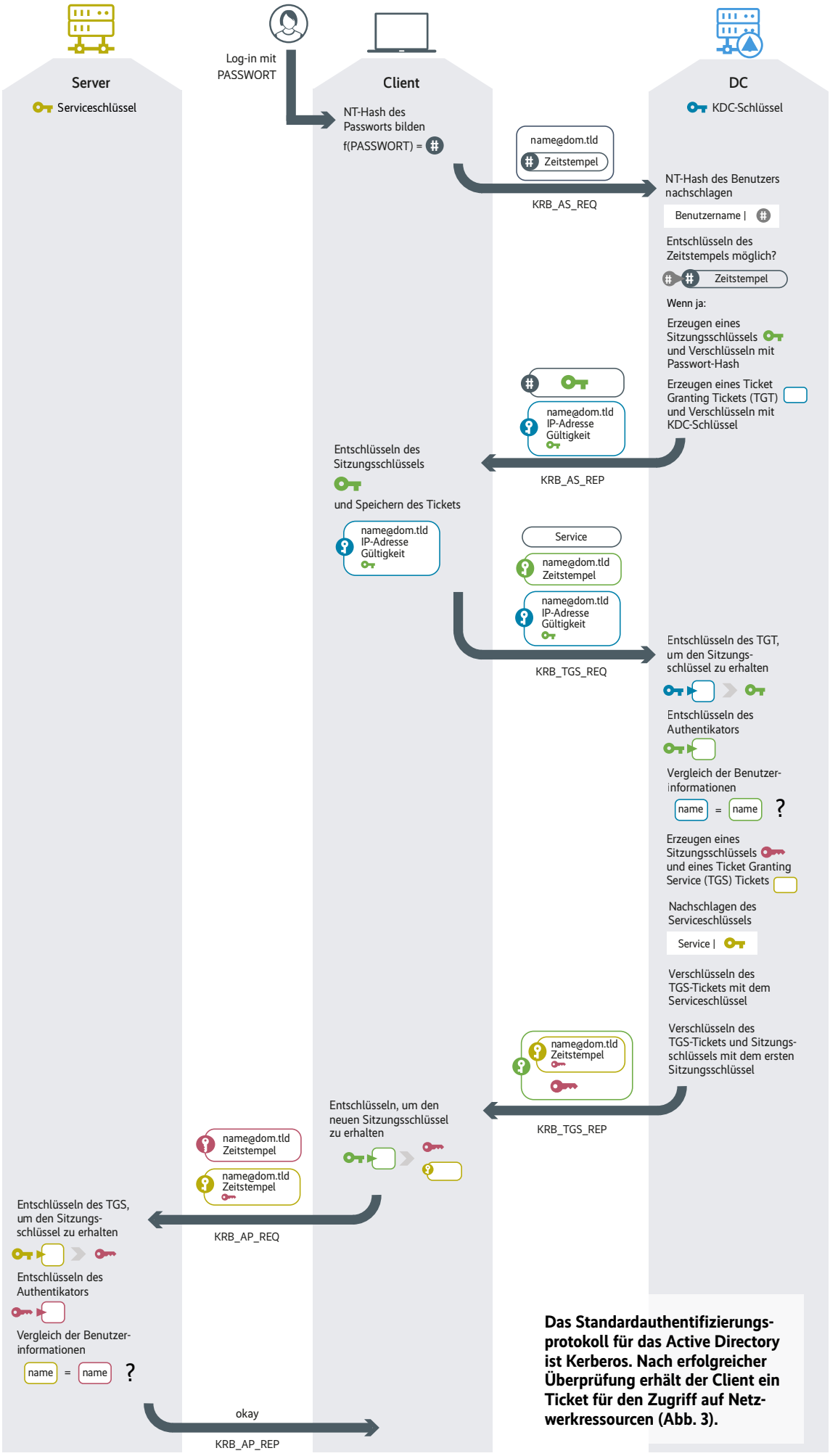
Den Zugriff steuern mit ACL

Bevor ein Benutzer Zugriff auf eine angeforderte Ressource erhält, muss der Domain-Controller prüfen, ob und in welchem Umfang er überhaupt dazu berechtigt ist. Dafür verfügt jedes Objekt über einen Security Descriptor, der zwei Arten von Zugriffskontrolllisten (Access Control List, ACL) enthält: Die Discretionary Access Control List (DACL) definiert die Berechtigungen, die ein Benutzer oder eine Gruppe für dieses Objekt haben; für Angreifer sind Fehlkonfigurationen in dieser Liste besonders interessant. Gemäß der System Access Control List (SACL) werden erfolgreiche und fehlgeschlagene Zugriffsversuche auf das Objekt in Windows-Ereignisprotokollen auf dem jeweiligen Rechner aufgezeichnet.

Versucht nun jemand, auf das Objekt zuzugreifen, sieht das System die einzelnen Einträge (Access Control Entries, ACE) der DACL durch und prüft, ob der Zugriff erlaubt oder verweigert wird. Falsche Einträge in Zugriffskontrolllisten in der Domäne können einem Angreifer den Weg zu deren Kontrolle ebnen.

Mit Gruppenrichtlinien Vorgaben zentral verwalten

Über Gruppenrichtlinien können Administratoren Richtlinien (Policies) und Einstellungen (Preferences) für Computer und Benutzer zentral verwalten. Eine Gruppenrichtlinie kann beispielsweise festlegen, dass das Benutzerpasswort mindestes 12 Zeichen lang sein muss und der Account nach dreimaliger Falscheingabe gesperrt wird. Auch kann sie für Computer die lokale Windows-Firewall konfigurieren oder Softwareinstallationen starten. Zur besseren Wartbarkeit sollte eine Richtlinie nur Einstellungen entweder für Be-



Das Standardauthentifizierungs-protokoll für das Active Directory ist Kerberos. Nach erfolgreicher Überprüfung erhält der Client ein Ticket für den Zugriff auf Netz-werkressourcen (Abb. 3).

nutzer oder für Computer enthalten, der nicht konfigurierte Teil kann komplett deaktiviert werden.

Die Richtlinieninhalte werden in sogenannten Gruppenrichtlinienobjekten (Group Policy Object, GPO) gespeichert und können mit Domänen, Organisationseinheiten oder Standorten (Sites) verknüpft werden.

Ein Gruppenrichtlinienobjekt hat im Wesentlichen zwei Bestandteile: Der Gruppenrichtliniencontainer (GPC) speichert allgemeine Informationen zur Gruppenrichtlinie, zum Beispiel den Anzeigenamen oder den Pfad zur Gruppenrichtlinienvorlage. Er ist in jedem AD unter CN=Policies, CN=System Container zu finden. Die Gruppenrichtlinienvorlage (GPT) enthält Dateien und Ordner, in denen die Einstellungen definiert werden. Sie liegt in der Freigabe SYSVOL\<domain>\Policies auf dem Domänencontroller. Der GPC auf dem Controller verweist auf die GPT in der SYSVOL-Freigabe.

SYSVOL wird von allen Domänencontrollern gemeinsam genutzt und zwischen den Controllern mit Distributed File System Replication (DFSR) repliziert. Außerdem kann in typischen AD-Konfigurationen jeder angemeldete Benutzer viele Gruppenrichtlinien abfragen und ihre jeweiligen Einstellungen aus der SYSVOL-Freigabe lesen.

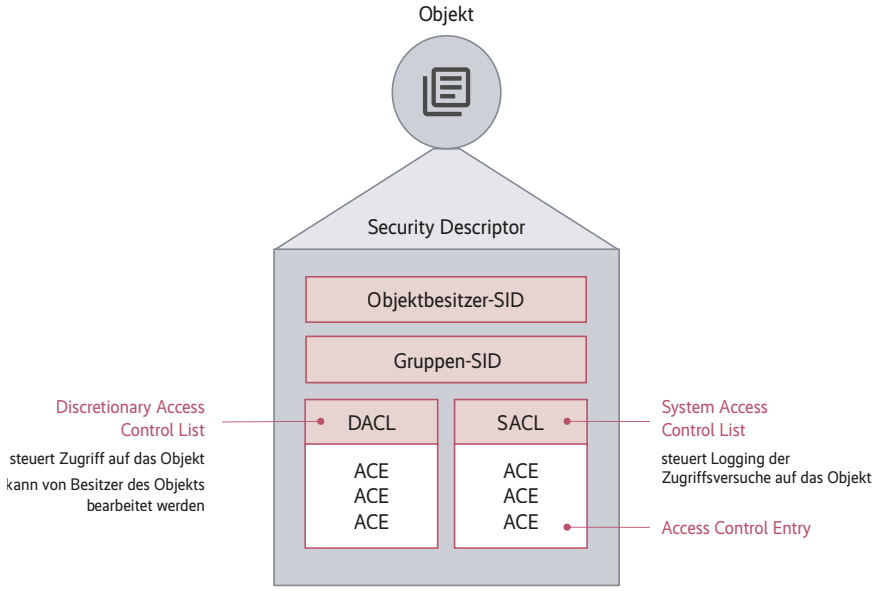
Schließlich sind auf den einzelnen Windows-Clients die Client-Side Extensions (CSE) dafür verantwortlich, diese Einstellungen anzuwenden. Bei den mit dem Windows Server mitgelieferten Gruppenrichtlinien sind die meisten sicherheitsrelevanten Einstellungen nicht oder nur unzureichend konfiguriert.

Nachhaltige Forest-Wirtschaft

Wie erläutert können Domänen zu hierarchischen Domänenbäumen strukturiert werden. Das Wurzelelement dieser Hierarchie ist die Stammdomäne.

Entgegen einer verbreiteten Annahme ist allerdings das für die Sicherheit entscheidende Element in einem Active Directory nicht die Domäne, sondern der Forest. Er bildet als eine Sammlung einer oder mehrerer Domänen oder Domänenbäume die Gesamtstruktur aller Objekte im AD. Alle Domänen eines Forest teilen sich unter anderem dasselbe Schema, das die Struktur der Active-Directory-Einträge definiert, und einen gemeinsamen globalen Katalog für die Suche nach Objekten.

IT-Verantwortliche nehmen oft irrtümlich an, dass die Domäne eine Sicherheitsgrenze im AD bildet. Aber Administratoren einer Domäne können sich administrativen Zugriff auf jede andere Domäne innerhalb der Gesamtstruktur verschaffen. Wird eine Domäne kompromittiert, führt dies zur Kompromittierung des gesamten Forest. Damit ist in Microsofts Active Directory der Forest die eigentliche Sicherheitsgrenze.



Den Zugriff auf ein Objekt regelt der Security Descriptor. Er enthält die Zugriffskontrolllisten mit den Berechtigungen (Abb. 4).

Welche Funktionen und Sicherheitsmechanismen in einer Domäne bereitstehen, bestimmen die Gesamtstruktur- und Domänenfunktionsebenen (siehe ix.de/zvnk).

Kein Zugriff ohne Vertrauen

Trusts stellen Vertrauensbeziehungen zwischen Domänen und Forests her. Sie ermöglichen Benutzern einer Domäne, auf Ressourcen anderer Domänen zuzugreifen.

Arten von Vertrauensbeziehungen können anhand ihrer Richtung und ihrer Transitivität unterschieden werden: Bei einseitigen Vertrauensstellungen vertraut eine Domäne B einer Domäne A. Dadurch können Benutzer aus Domäne A auf Ressourcen in Domäne B zugreifen; ein Zugriff von Domäne B zu A ist jedoch nicht möglich. Richtung des Vertrauens und Richtung des Zugriffs sind also genau gegensätzlich. Bei zweiseitigen Vertrauensstellungen vertrauen beide Domänen einander, sodass Benutzer einer Domäne auf die jeweils andere zugreifen können.

Eine transitive Vertrauensstellung erweitert das Vertrauen einer Domäne B zu einer Domäne A auf alle Domänen, denen Domäne A vertraut. Bei einer intransitiven Vertrauensstellung spielen andere Vertrauensbeziehungen keine Rolle, sondern bleiben auf die Ursprungsbeziehung von Domäne B zu Domäne A beschränkt.

Alle Vertrauensbeziehungen innerhalb eines Forest sind automatisch zweiseitig und transitiv, das heißt, jede Domäne in einem Forest vertraut jeder anderen Domäne desselben Forest. Zusätzlich können händisch weitere Trusts erstellt werden, beispielsweise externe Trusts, also intransitive Vertrauensbeziehungen zwischen Domänen zweier Forests.

Dabei können durch Trusts Authentifizierungsgrenzen womöglich unbeabsichtigt erweitert und ungewollt Informationen auch über den Forest hinaus preisgegeben werden.

Aufgrund mangelnder Kenntnis der Zusammenhänge und falscher Einstellungen kann man an vielen Schaltstellen des Active Directory Einfallstore für Angreifer schaffen. Ein grundlegendes Wissen ist für den sicheren Betrieb daher unumgänglich. (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] Details zu den Gesamtstruktur- und Domänenfunktionsebenen sowie weitere Informationen siehe ix.de/zvnk

Frank Ully

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