

**ACE (Access Control Entries):** einzelne Einträge der Zugriffskontrolllisten

**ACL (Access Control List):** Zugriffskontrollliste

**Active Directory (AD):** Microsofts Verzeichnisdienst, der Informationen zu Objekten in Netzwerken (Geräte, Dienste, Benutzer etc.) verwaltet.

**AD CS (Active Directory Certificate Services):** Die Zertifikatsdienste sind eine optionale Rolle des AD, mit der sich unter anderem Unternehmenszertifikate erstellen und verwalten lassen.

**AD DS (Active Directory Domain Services):** Kernrolle des AD und oft synonym verwendet; sie stellt Authentifizierungs- und Autorisierungsdienste bereit und ist Basis für viele andere Microsoft-Produkte wie Exchange oder SharePoint.

**AD FS (Active Directory Federation Services):** Optionale Rolle des AD, die Benutzern nach einmaliger Anmeldung Zugriff auf Systeme und Anwendungen über Unternehmensgrenzen hinweg ermöglicht. Erlaubt etwa die Anmeldung am lokalen und am Azure Active Directory.

**Admin on Behalf of (AOBO):** Administrator im Auftrag von; AOBO ermöglicht Serviceprovidern RBAC-Besitzerzugriff auf Azure-Abonnements in Kundenmandanten.

**AGDLP-Modell (Account, Global, Domain Local Permissions):** Microsofts Empfehlungen zur Umsetzung einer rollenbasierten Zugriffssteuerung mit AD-Gruppen

**AMSI (Anti Malware Scan Interface):** Schnittstelle ab Windows 10, die Malwarescannern unter anderem besseren Einblick in PowerShell-Skripte und .NET-Programme zur Laufzeit verschafft. Mit ihr lassen sich dateilose Angriffe im Arbeitsspeicher erkennen.

**AS (Authentication Service):** Logische Komponente des KDC, bestätigt die Identität des Benutzers und stellt ihm ein **Ticket Granting Ticket** aus.

**AS-REP Roasting:** analog zu **Kerberoasting** funktionierender Angriff gegen normale Benutzerkonten bei deaktivierter Kerberos-Präauthentifizierung

**ATA:** Microsofts Advanced Threat Analytics, kann in AD-Umgebungen verdächtige Aktivitäten und Angriffe auf Konten entdecken. Wird noch bis Januar 2026 unterstützt, Nachfolger ist **MDI**.

**Azure Active Directory (Azure AD, AAD):** zentrale Identitäts- und Zugriffsverwaltung für die Dienstplattform Azure und für SaaS-Angebote in der in der Microsoft-Cloud. Im Juli 2023 wurde Azure AD in **Entra ID** umbenannt.

**Azure AD B2C (Business to Consumer):** Dienst, der in einem Azure-Abonnement aktiviert werden kann, um Identitätsverwaltung für Kunden bereitzustellen.

**Azure AD Connect:** Lokale Microsoft-Anwendung, mit der sich eine AD-Hybridumgebung synchronisieren lässt. Dazu wird Azure AD Connect auf einem lokalen Server, dem Azure AD Connect Server, betrieben.

**Azure AD DS (Domain Services):** Stellen in Azure eine klassische AD-Domäne mit Domänencontrollern und Protokollen wie LDAP und Kerberos bereit, die Microsoft verwaltet und in AAD integriert.

**Azure CLI (Command-Line Interface):** auf Python basierende Azure-Befehlszeilenschnittstelle mit mitgeliefertem Interpreter

**Azure Mandant (auch Azure Tenant):** Azure AD einer Organisation, Äquivalent zur Gesamtstruktur (Forest) im klassischen AD; enthält alle Benutzer, Gruppen, Geräte und Anwendungen der Organisation.

**Azure Monitor:** Azure-Dienst, der Telemetriedaten aus Azure- und lokalen Umgebungen sammelt und analysiert in Bezug auf Verfügbarkeit und Leistung.

**Azure Resource Manager (ARM):** Erstellt, verändert und löscht Ressourcen entsprechend einem rollenbasierten Berechtigungsmodell (Azure Role-based Access Control, Azure RBAC).

**CES (Certificate Enrollment Web Service):** Webdienst für Zertifikatsregistrierung; Teil von **AD CS**, der es Benutzern und Computern ermöglicht, die Zertifikatsregistrierung über HTTPS durchzuführen.

**CIFS (Common Internet File System):** veraltete Implementierung des Protokolls **SMB** für Datei-, Druck- und weitere Dienste

**Conditional Access (bedingter Zugriff):** Mit Conditional Access lässt sich der Zugriff auf das Azure AD und andere Azure-Dienste granular reglementieren und kontrollieren.

**Container, Nicht-Container:** Objekte in der hierarchischen Struktur des AD. Container können weitere Objekte enthalten. Nicht-Container enthalten keine weiteren Objekte und werden daher auch als Endknoten oder Leaf (Blatt) bezeichnet.

**Credential Stuffing:** Angriff, bei dem ein Angreifer versucht, sich mit gestohlenen oder geleakten Zugangsdaten an Diensten oder Anwendungen anzumelden.

**DACL (Discretionary Access Control List):** Teil der **ACL**, definiert die Berechtigungen, die ein Sicherheitsprinzipal wie ein Benutzer oder eine Gruppe für ein Objekt hat.

**DCE/RPC (Distributed Computing Environment/Remote Procedure Call):** Spezifikation für einen Remote-Procedure-Call-Mechanismus (Aufruf entfernter Prozeduren). Sie vereinfacht das Schreiben und die Nutzung von verteilter Software.

**DCShadow:** Angriffsgegenstück zu **DCSync**, hier schreibt der Angreifer neue Objekte in die Domäne oder verändert Daten.

**DCSync:** Angriff, bei dem der Angreifer den Domänencontroller zum Replizieren von Daten wie Passwort-Hashes aller Konten auffordert und sie





ausliest. Der Angreifer muss dazu nicht selbst am DC angemeldet sein, aber die Rechte eines Domänenadministrators besitzen.

**Delegierung (eingeschränkt, uneingeschränkt, RBCD):** In Kerberos ergänzter Mechanismus zur Rechteübertragung, der einer Anwendung (beispielsweise einem Webserver) ermöglicht, im Namen eines Benutzers auf einen anderen Dienst (beispielsweise einen Datenbankserver) zuzugreifen.

**DFSR (Distributed File System Replication):** Repliziert Freigaben wie SYSVOL auf verschiedenen Domänencontrollern, um sie synchron zu halten.

**DHCP (Dynamic Host Configuration Protocol):** Protokoll zur dynamischen Zuweisung von IP-Adressen in einem Netzwerk sowie weiterer Verbindungsparameter wie dem DNS-Server

**Dienstkonto (Service Account):** Benutzerkonto, das keinen echten Benutzer, sondern Dienste wie SQL-Server oder automatisierte Abläufe wie Backups an einer Domäne authentifiziert. Daneben existieren reguläre Benutzer- und Computerkonten.

**Dienstprinzipal (Service Principal):** Identität, die in den einzelnen Azure ADs für eine mandantenfähige Anwendung erstellt wird, damit sie auf dieses AAD oder auf Azure-Ressourcen zugreifen darf.

**DN (Distinguished Name):** Bezeichnet den eindeutigen Pfad eines Objekts innerhalb des AD bei Abfragen über LDAP.

**Domäne:** Verwaltungsebene und Replikationsgrenze; Sammlung von Objekten (beispielsweise Benutzer oder Benutzergruppen) innerhalb des AD. Jede Domäne muss über einen eindeutigen Domänennamen entsprechend den Konventionen des DNS (Domain Name System) verfügen.

**Domänencontroller (Domain Controller, DC):** Das Herz einer Domäne; verantwortlich für die Authentifizierung, die Zugriffskontrolle auf AD-Ebene sowie das Verwalten von Objekten und Attributen innerhalb einer Domäne. Der DC sollte auf einem eigenen Server betrieben werden.

**Domänenfunktionsebene (Domain Functional Level):** Bestimmt, welche AD-Funktionen in der Domäne genutzt werden können. Neuere Funktionsebenen bringen häufig Sicherheitsfunktionen mit.

**DSRM (Directory Service Restore Mode):** Der Wiederherstellungsmodus für Verzeichnisdienste ist eine Funktion auf Domänencontrollern, mit der der Server für die Notfallwartung offline geschaltet wird, insbesondere für die Wiederherstellung von Sicherungen.

**Enumeration/enumerieren:** Eine der wichtigsten Angriffsphasen; Durchforsten der Unternehmensinfrastruktur, in diesem Fall der Domäne, nach wertvollen oder angriffsrelevanten Daten.

**ESAE (Enhanced Security Administrative Environment):** „Red Forest“, separate Gesamtstruktur mit Administratorkonten, PAWs und dafür nötigen Gruppen

**Explicit Mapping:** Zertifikatsinformationen an Benutzer- oder Computerobjekt im AD anheften.

**Forest:** Als Gesamtstruktur oberste Verwaltungsebene im AD, bildet die Sicherheitsgrenze in AD-Umgebungen.

**Forest-Funktionsebene (Forest Functional Level):** Bestimmt, welche AD-Funktionen im Forest genutzt werden können.

**Globaler Leser (Global Reader):** Rolle im Azure AD, die auf (fast) alles Lesezugriff, aber keine Schreibrechte wie der globale Administrator hat.

**GMSA (Group Managed Service Accounts):** Gruppenverwaltete Dienstkonten, deren Passwort mit dem Domänencontroller synchronisiert wird.

**Goldenes Ticket:** gefälschtes TGT, Ticket Granting Ticket, „Generalschlüssel“

**GPC (Gruppenrichtliniencontainer):** Speichert allgemeine Informationen zur Gruppenrichtlinie in der Domänendatenbank NTDS.dit, verweist auf die GPT, Teil der Gruppenrichtlinien.

**GPO (Gruppenrichtlinien, Group Policy Object):** Sammlung von Richtlinien für Benutzer und Computer; zentral ausrollbar

**GPP (Group Policy Preferences, Gruppenrichtlinieneinstellungen):** Funktion der Gruppenrichtlinien, die Einstellungen verwaltet.

**GPT (Gruppenrichtlinientemplate):** Speichert spezifische Informationen zur Gruppenrichtlinie in der SYSVOL-Freigabe auf Domänencontrollern, Teil der Gruppenrichtlinien.

**GUID (Globally Unique Identifier):** 128-Bit-Kennung für verteilte Computersysteme

**KDC (Key Distribution Center):** Zentrale Komponente von Kerberos, Schlüsselverwaltungszentrale für angemeldete Nutzer in einem Netzwerk, besteht logisch aus AS und TGS.

**Kerberoasting:** Angriffstechnik, bei der schwache Passwörter von Dienstkonten mit SPN via Brute Force oder Passwortlisten offline „gebraten“ oder „geröstet“ werden.

**Kerberos:** Standardauthentifizierungsprotokoll für das AD, bestehend aus den Komponenten Client, Server und KDC

**krbtgb-Hash:** zentrales AD-Geheimnis und Vertrauensanker für Kerberos; Passwort-Hash des Kerberos-Dienstkontos

**LAPS (Local Administrator Password Solution):** Verwaltet Kennwörter lokaler Administratorkonten für in eine Domäne eingebundene Computer auf Domänencontrollern und schützt ihren Abruf durch ACLs.

**Lateral Movement:** Techniken, mit denen sich Angreifer schrittweise durch ein Netzwerk bewegen und nach lohnenden Daten und Zielen suchen.

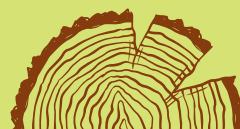
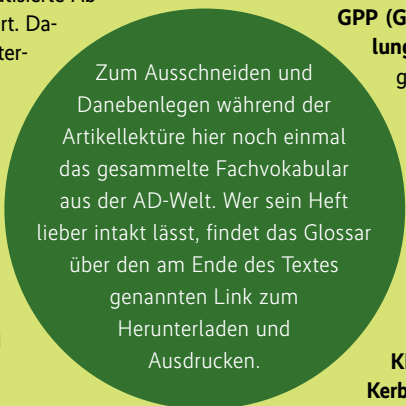
**LDAP (Lightweight Directory Access Protocol):** Protokoll für Abfragen und Änderungen in einem verteilten Verzeichnisdienst

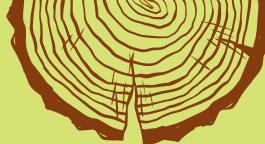
**Least Privilege:** Vergabe des niedrigsten benötigten Rechts

**LLMNR (Link-Local Multicast Name Resolution):** Protokoll, um bei Ausfall der DNS-Server einen Rechner im Netzwerk zu identifizieren.

**LSA Secret:** Von der LSA (Local Security Authority) lokal gespeichertes Geheimnis, darunter Passwörter von Domänenkonten, mit denen ein Windows-Dienst gestartet wird.

**LSASS-Prozess:** Der Windows-Prozess LSASS (Local Security Authority Subsystem Service) der lokalen Sicherheitsautorität LSA ist wesentlich an





der Authentifizierung von lokalen und Domänenbenutzern beteiligt. Er hält Passwort-Hashes im Arbeitsspeicher vor.

**Microsoft 365:** Software-as-a-Service-Angebot von Microsoft, etwa mit Exchange Online

**MDI (Microsoft Defender or Identity):** Vormalig Azure Advanced Threat Protection (Azure ATP), leitet Daten aus verschiedenen Quellen an die Azure-Cloud weiter und wertet sie dort nach verdächtigem Verhalten aus. Nachfolger von **ATA**.

**mDNS (Multicast DNS):** Protokoll zum Auflösen von Rechnernamen in IP-Adressen in Computernetzwerken ohne lokalen DNS-Server

**MS-DRSR (Microsoft Directory Replication Service Remote Protocol):** Protokoll, mit dem Domänencontroller untereinander Daten austauschen.

**MS-KILE:** Microsoft-eigene Kerberos-Implementierung, basiert auf dem offenen **Kerberos**-Standard Version 5.

**NBT-NS (NetBIOS-Nameservice):** Teilprotokoll des ursprünglichen NetBIOS-Stacks von Windows zur Identifizierung eines Rechners im Netzwerk, auch heute noch Fallback bei Ausfall der DNS-Server

**NDES (Network Device Enrollment Service):** Microsofts Implementierung des SCEP-Protokolls (Simple Certificate Enrollment Protocol)

**Netlogon-Dienst:** Anmeldedienst, überprüft Domänenanmeldungen.

**Net-NTLM (NT LAN Manager):** Challenge-Response-Authentifizierungsprotokoll, oft auch nur als NTLM bezeichnet.

**Net-NTLM-Relaying:** Man-in-the-Middle-Angriff, bei dem **Net-NTLM**-Anmeldungen an einen vom Angreifer ausgesuchten Rechner oder Dienst weitergeleitet werden.

**NTDS.dit:** Zentrale Datenbankdatei auf Domänencontrollern, die alle Daten einer Domäne enthält, einschließlich der Passwort-Hashes der Benutzer.

**NT-Hash/NTLM-Hash:** Passwort-Hash bei Nutzung von **Net-NTLM**

**OAuth2 (Open Authorization):** Autorisierungsprotokoll für APIs. Das auf OAuth2 aufbauende OpenID Connect nutzen viele Internetdienste auch zur Authentifizierung von Benutzern.

**OU (Organizational Unit):** Organisationseinheit innerhalb einer Domäne

**Overpass the Hash:** Authentifizierung eines Angreifers über Kerberos mit einem NT-Hash.

**PAM (Privileged Access Management):** Produkt zum Absichern privilegierter (administrativer) Zugriffe innerhalb einer Organisation.

**Password-Hash-Synchronisierung (PHS):** Eine von drei Anmeldemethoden für Hybrididentitäten in Azure AD, bei der Azure AD Connect einen Hash eines Benutzerkennwort-Hashes aus dem lokalen AD mit Azure AD synchronisiert.

**Pass the Hash:** Authentifizierung eines Angreifers über **Net-NTLM** mit einem **NT-Hash**

**Pass the Key:** Authentifizierung eines Angreifers über **Kerberos** mit einem Kerberos-Schlüssel

**Pass the Ticket:** Authentifizierung eines Angreifers mit einem Kerberos-Ticket, ohne Passwort oder Hash zu benötigen.

**Pass-Through-Authentifizierung (PTA):** Weitere Möglichkeit zur Anmeldung für Hybrididentitäten in Azure AD, bei der ein Anmeldeversuch von der Cloud zur Prüfung ins lokale AD weitergeleitet wird.

**Password Spraying:** Variante des Brute-Forcing, bei der eine kurze Liste mit wahrscheinlichen Passwörtern bei vielen oder allen Benutzern durchprobiert wird.

**PAWs (Privileged Access Workstations):** Speziell gesicherte Rechner zur Administration, die gehärtet und nicht mit allen Netzwerken verbunden sind.

**Persistenz:** Angriffsphase, in der ein Angreifer versucht, sich dauerhaften Zugriff zu verschaffen. Bezieht sich einerseits auf ein einzelnes kompromittiertes System, andererseits über Änderungen an der Domäne auf die komplette Umgebung.

**PetitPotam:** Auslösemechanismus, um eine Net-NTLM-Authentifizierung über einen Remote-Aufruf des Encrypting File System zu erzwingen, als Vorstufe für einen Net-NTLM-Relaying-Angriff. Die Bezeichnung wird oft fälschlich für das Net-NTLM-Relaying zu nicht gehärteten AD-Webdiensten verwendet.

**PKINIT:** Kerberos-Präauthentifizierungsverfahren mit Zertifikaten in Domänenumgebungen mit **ADCS**

**Printer-Bug:** Auslösemechanismus, um eine Net-NTLM-Authentifizierung über einen Remote-Aufruf des Druckerspoolers zu erzwingen, als Vorstufe für einen Net-NTLM-Relaying-Angriff.

**Protected Users:** Benutzergruppe im Active Directory, für deren Mitglieder verschiedene Härtingsmaßnahmen im AD sowie auf Windows-Systemen aktiviert werden.

**RBCD (Resource Based Constrained Delegation):** Jüngste Variante der Kerberos-Delegation, bei der an der Zielressource definiert wird, welchen Konten sie zur Delegation vertraut.

**RDP (Remote Desktop Protocol):** Microsofts Protokoll für Fernwartung; von Angreifern häufig genutztes Einfallstor

**RDP-Hijacking:** Angriff, bei dem eine bestehende Sitzung über das Remote Desktop Protocol übernommen wird.

**Red Forest:** Von Microsoft vorgeschlagene Architektur zum Absichern der Administration einer Organisation aus einem speziell abgesicherten Active Directory Forest heraus.

**RID (Relative Identifier):** Relative Kennung, die einem Objekt bei der Erstellung zugewiesen wird und Teil seiner Sicherheitskennung in einer Domäne wird.

**RODC (Read Only Domain Controller):** Domänencontroller ohne Schreibrechte

**SACL (System Access Control List):** Teil der **ACL**; bestimmt, ob erfolgreiche oder fehlgeschlagene Zugriffsversuche auf das Objekt protokolliert werden.

**SAM (Security Account Manager):** Speichert lokale Benutzerkonten und ihre Passwort-Hashes.

**Sicherheitsleser (Security Reader):** Rolle in Azure AD mit globalem Lesezugriff auf alle sicherheitsrelevanten Funktionen

**SD (Security Descriptor):** Enthält die Sicherheitsinformationen, die mit einem zu sichernden Objekt verbunden sind, darunter die **SID** seines Besitzers sowie **DACL** und **SACL**.

**Sicherheitsprinzipal:** Entität, der Berechtigungen zugewiesen werden, etwa Benutzer oder Gruppen, in Azure AD auch **Dienstprinzipale**.

**SID (Security Identifier):** Sicherheitskennung eines AD-Sicherheitsprinzipals mit einem domänenspezifischen Präfix sowie der **RID**



**SID-Historie/SID-Verlauf:** Attribut an Domänenobjekten, damit die Sicherheitskennung migriert werden kann. Wird bei Varianten des **goldenen Tickets** missbraucht.

**SIEM (Security Information and Event Management):** System, das alle sicherheitsrelevanten Informationen in einem Netzwerk zusammenführt und interpretiert und bei erkannten Sicherheitsvorfällen Alarm schlägt.

**Silbernes Ticket:** gefälschtes Serviceticket (**TGS, Ticket Granting Service**), unauffälliger einsetzbar als das **Goldene Ticket**

**SMB (Server Message Block):** Dateiübertragungsprotokoll

**SOC (Security Operations Center):** Zentrum für IT-Sicherheitsdienstleistungen. Es sammelt und analysiert Bedrohungsinformationen (Threat Intelligence) aus verschiedenen Quellen und leitet im Bedarfsfall erste Schritte zur Bewältigung eines Sicherheitsvorfalls ein (Incident Response).

**SPN (Service Principal Name):** Dienstprinzipalname, über den ein Client eine Instanz eines Diensts eindeutig identifiziert. Wesentlich für die Funktionsweise von **Kerberos**.

**SRV-Eintrag (Service Resource Records):** Eintragsart im DNS, die dazu dient, AD-Dienste wie den Domänencontroller zu finden.

**Stammdomäne:** Containerobjekt, das die Basis der Domänenhierarchie bildet. Unterhalb der Stammdomäne können zusätzliche Domänen angelegt werden. Eine solche Hierarchie wird als Domänenbaum bezeichnet.

**SYSVOL:** Freigabe von Dateien und Ordnern auf jedem Domänencontroller in einer Domäne, enthält etwa die **GPT**.

**TGS (Ticket Granting Service):** Logische Komponente des **KDC**, gibt Tickets für Zugriff auf Netzwerkressourcen an Benutzer aus.

**TGT (Ticket Granting Ticket):** Authentifizierungsticket bei Kerberos, belegt die Identität eines Sicherheitsprinzipals, enthält unter anderem Informationen zum Benutzer und einen Gültigkeitszeitraum.

**Tiers:** Verwaltungsebenen

**Tier-Modell:** Verschiedene voneinander getrennte und unterschiedlich geschützte Ebenen, um **Lateral Movement** zu verhindern.

**Trusts:** Vertrauensbeziehungen zwischen Domänen innerhalb eines Forests und zu Domänen in anderen Forests

**UPN (User Principal Name):** Benutzerprinzipalname als Gegenstück zu **SPN** für Benutzer

**Verwaltete Identität (Managed Identity):** Bestimmter Typ von **Dienstprinzipal** in Azure, der an spezifische Ressourcen angehängt werden kann; Anmeldeinformationen werden dabei automatisch gehandhabt.

**WEF (Windows Event Forwarding):** Mechanismus, um Windows-Ereignisprotokolle zu einem zentralen Server weiterzuleiten.

**Windows-Ereignisprotokoll:** Sammlung von Logdateien in Windows-Systemen. Kann über die Ereignisanzeige eingesehen werden. Die sicherheitsrelevante Teilmenge, das Windows-Sicherheitsereignisprotokoll, hilft beim Nachvollziehen von Angriffen.

**WinRM (Windows Remote Management):** Modernes Fernwartungsprotokoll; wird bei PowerShell Remoting genutzt.

**WMI (Windows Management Instrumentation):** Älteres Fernwartungsprotokoll, das etwa Informationen über den Systemzustand abfragen kann.

---

Das Glossar kann über den [Link ix.de/zxw2](https://ix.de/zxw2) heruntergeladen und ausgedruckt werden.



