On-Premises-Active-Directory: Schlaraffenland für Angreifer und Ransomware

Für Admins ist Active Directory (AD) ein Segen. Weil der Verzeichnisdienst so zentral für On-Premises ist, nutzen ihn auch Kriminelle. Ransomware-Gruppen missbrauchen AD-Fehlkonfigurationen und eingebaute Funktionen, um sich im Netzwerk ihrer Opfer auszubreiten – und dort volle Kontrolle zu gewinnen.

DER AUTOR

Frank Ully
Head of Research, Oneconsult Deutschland

Lange legten IT-Verantwortliche ihr Augenmerk auf klassische Netz- und Clientsicherheit, zum Beispiel durch Firewalls und Malwarescanner. Danach rückten Webanwendungen in den Fokus. Die Sicherheit des AD als zentraler Verzeichnisdienst im Herzen der Organisation fristet oft ein Schattendasein.

Auf der einen Seite fehlen Kenntnisse über dessen wesentliche sicherheitsrelevanten Eigenschaften. Zum Beispiel: Jeder Benutzer kann zahlreiche Informationen über die Domäne abrufen, etwa die Gruppenmitgliedschaften anderer Nutzer oder deren Beschreibungsfeld, in dem manchmal Kennworthinweise hinterlegt sind. Schwache Passwörter von Dienstkonten knackt ein Angreifer beim «Kerberoasting» offline. Und: Ist eine Domäne kompromittiert, sind sämtliche Domänen derselben Gesamtstruktur betroffen – der Forest, nicht die Domäne ist eine Sicherheitsgrenze.

AD aus der Sicht von Angreifern

Auf der anderen Seite ist moderne Ransomware auf ein AD angewiesen. Sie bricht die Infektion ab, wenn sie auf einem Rechner landet, der nicht Teil davon ist. In einer Domäne dagegen verbreitet sich die Schadsoftware automatisiert von einem System zum nächsten. Sie nutzt Schwachstellen und Fehlkonfigurationen selbstständig aus: etwa wegen zu weitreichender Rechtedelegierung entstandene Lücken in Zugriffskontrolllisten, durch die ein normaler Benutzer das Passwort eines Administrators zurücksetzen kann.

Wesentlich für Angreifer ist die laterale Bewegung, bei der sie sich schrittweise vom zunächst infizierten Rechner über weitere Systeme hin zu den Kronjuwelen wie einem Datenbankserver oder Domänencontroller bewegen. Dazu müssen sie das nächste Ziel auf Netzebene erreichen und ein Konto kompromittiert haben, das sich dort etwa als lokaler Administrator anmelden darf.

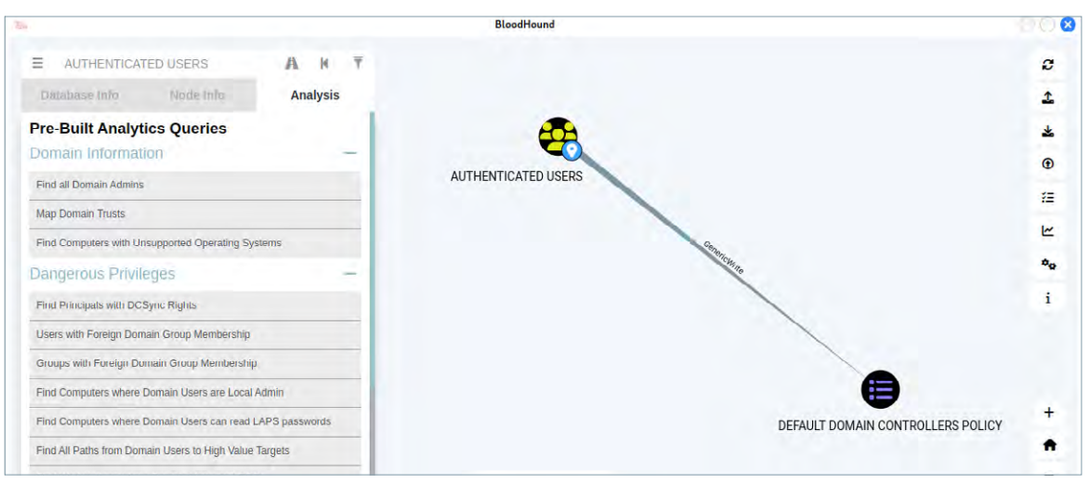
Grafische Angriffswerkzeuge wie «BloodHound» visualisieren Beziehungen zwischen AD-Benutzern und Computern und finden den schnellsten Weg zu einem Domänenadministrator, auch über viele Zwischenschritte. Ein solches Adminkonto ist leichte Beute, wenn Systemverwalter es nutzen, um sich an normalen Servern oder Clients anzumelden, oder wenn sie es bei Windows-Systemdiensten eintragen.

Haben Angreifer einen Domänenadmin kompromittiert, ist das AD gefallen. Ihre Verschlüsselungssoftware verteilen sie über Gruppenrichtlinien auf sämtliche verbundene Rechner. In schlecht gehärteten Umgebungen vergehen teils weniger als 24 Stunden von der Erstinfektion bis zum Lahmlegen aller Systeme, einschliesslich Backup-Servern – nachzulesen in Vorfallberichten auf thedfirreport.com. Fehlen dem Opfer verlässlich wiederherstellbare Offline-Backups, wird der Erpressungsversuch zum existenziellen Risiko.

Ein sicheres AD ist möglich

Zentrale Komponenten von Windows, Domänendiensten sowie den eng verwandten Active Directory Certificate Services (ADCS) sind gelegentlich von Schwachstellen betroffenen – sie sollte man zügig patchen. Einige schwerwiegende Fehlkonfigurationen, die Admins manuell beheben, decken kostenfreie Auditwerkzeuge wie «PingCastle» oder «Purple Knight» auf.

Eine wesentliche Strategie gegen laterale Bewegung ist das stärkere Segmentieren des Netzwerks; das kann schon mit der eingebauten Windows-Firewall gelingen. Clients müssen nicht andere Clients erreichen, und auch nicht die meisten Server. Als zweites sollten Organisationen privilegierte Konten besser schützen: durch das schrittweise Umsetzen des Least-Privilege-Prinzips und weitere Massnahmen wie regelmässige Passwortaudits, Passwortfilter und Mehr-Faktor-Authentifizierung.



Grafische Angriffswerkzeuge wie «BloodHound» visualisieren Beziehungen zwischen AD-Benutzern, Computern und anderen Objekten wie Gruppenrichtlinien.

« Am häufigsten sind alte, unsichere Konfigurationsstandards anzutreffen »

Gezielte Angriffssimulationen zeigen auf, welche Schwachstellen im Active Directory ausgenutzt und welche Konfigurationsstandards am meisten betroffen sind. Mit einem Sicherheitsaudit der Active-Directory-Konfiguration können Unternehmen ihren Schutz optimal anpassen. Interview: Tanja Mettauer

Welche Services bietet Oneconsult seinen Kunden, um sich vor Angriffen auf das Active Directory zu schützen?
Fabian Gonzalez: Bei einem Sicherheitsaudit der Active-Directory-Konfiguration wird die Sicherheit einer AD-Umgebung umfassend geprüft. Dabei verwenden wir Programme wie «BloodHound», «PingCastle» und «PowerView». Mithilfe des Tools «BloodHound» können Beziehungen zwischen angemeldeten Domänenbenutzern, Gruppen und Geräten in der Domäne analysiert und als Graph visualisiert werden. Das Audit kann etwa mit Fokus auf hoch privilegierte Benutzergruppen oder auf Server durchgeführt werden. Zusätzlich können Referenz-Windows-Installationen, Gruppenrichtlinien-Einstellungen oder Active Directory Certificate Services (ADCS) auditiert werden. Der Kunde gewährt uns dazu Lesezugriff auf alle Einstellungen, was uns erlaubt, sicherheitsrelevante Fehlkonfigurationen effizient zu erkennen. Kunden, die bereits einen höheren Sicherheitslevel besitzen, können durch gezielte Angriffssimulationen – einem sogenannten Red Teaming – prüfen, ob die vorhandenen Sicherheitsmechanismen ausreichen, um einen Angriff auf das AD zu verhindern oder ihn zumindest stark erschweren.

Wie funktioniert eine Incident Response, wenn ein Kunde ein kompromittiertes Active Directory bei Ihnen meldet?
Ein kompromittiertes AD ist oft eine «Begleiterscheinung» in einem weit grösseren Cyberangriff, etwa in einem Ransomware-Fall. Ist das AD kompromittiert, muss man davon ausgehen, dass die Angreifer die Kontrolle über das gesamte Netzwerk haben und somit im schlimmsten Fall das Passwort jedes Benutzers kennen. Um den Angriff einzudämmen, ist daher eine der ersten Massnahmen, die Kennwörter aller Benutzer zu ändern. Administrative Benutzerkonten, einschliesslich Servicekonten, sollten zwingend priorisiert werden. Aktuell nicht benötigte Konten können temporär deaktiviert werden. Des Weiteren wird das AD mit einem Scan auf mögliche Änderungen und Schwachstellen überprüft und abgesichert. Es ist schwierig, das ganze Schadensausmass und sämtliche Aktivitäten der Angreifer bei einer AD-Kompromittierung zu bestimmen. Wir raten in solchen Fällen zur kompletten Neuerstellung des Active Directorys. Nur so ist gewährleistet, dass die Angreifer vollständig ausgesperrt werden.

Welche sicherheitsrelevanten Fehlkonfigurationen treffen Sie im Active Directory am häufigsten an?
Am häufigsten sind alte, unsichere Konfigurationsstandards anzutreffen, die bei der Ersteinrichtung des AD oder bei der Installation zusätzlicher Anwendungen wie Microsoft Exchange gesetzt wurden. Diese Einstellungen werden beim Einspielen von Updates weiterhin übernommen und können Systeme beeinträchtigen, die auf dem neuesten Stand sind. Ein Beispiel sind ältere Microsoft-Exchange-Installationen, bei denen die Exchange-Objekte erhöhte Berechtigungen im AD besitzen. Ein Angreifer, der einen Exchange-Server erfolgreich kompromittiert hat, könnte aufgrund der Standardeinstellungen Domänenadmin-Rechte erlangen. Weitere Beispiele sind das Forcieren der LDAP- und SMB-Signierung. Hier wird standardmässig zwar die Signierung unterstützt, aber nicht in jedem Fall erzwungen. So werden dennoch unsichere Verbindungen akzeptiert.

« Ein kompromittiertes AD ist oft eine ‹Begleiterscheinung› in einem weit grösseren Cyberangriff, etwa in einem Ransomware-Fall. »

Fabian Gonzalez, Team Leader Red Teaming & Penetration Testing, Oneconsult

Das Dossier finden Sie auch online
www.netzwoche.ch