« 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