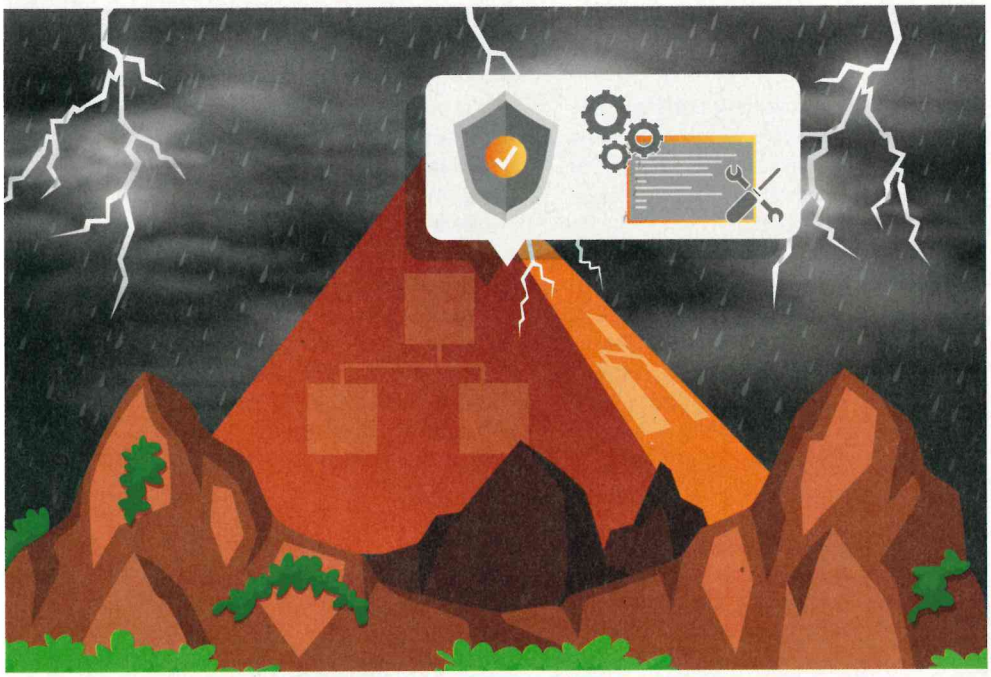


Tools für die Absicherung von Microsofts Active Directory

(Hilfs-)Mittel zum Zweck

Hagen Molzer

Das Active Directory sicher zu konfigurieren und zu härten ist bloß der erste Schritt. Nützliche Tools prüfen das AD auf Sicherheit und Kompromittierung, erkennen und verhindern Angriffe oder helfen im Ernstfall, Angriffsspuren zu verfolgen und die Daten wiederherzustellen.

iX-TRACT

- Zwar ist für die Absicherung eines Active Directory das Vermeiden von Fehlkonfigurationen und das Abschalten nicht benötigter Funktionen schon die halbe Miete. Ergänzend gibt es aber Softwarewerkzeuge, die durch Scans den Sicherheitsstatus ermitteln und Einfallstore offenlegen.
- Die von einigen Tools ausgegebenen Berichte zum Sicherheitsstatus können dabei helfen, Vorgesetzte von Maßnahmen zu überzeugen. Regelmäßig durchgeführt sind sie auch ein Beleg für kontinuierliche Sicherheitsbemühungen und -verbesserungen.
- Gelingt es Kriminellen, das Active Directory eines Unternehmens zu kompromittieren und zu manipulieren, helfen diese und weitere Werkzeuge den Systemverantwortlichen bei der Angriffsanalyse und der Wiederherstellung.

Die zahlreichen Angriffsvarianten auf das Active Directory, die in den vergangenen Monaten in verschiedenen *iX*-Artikeln im Detail vorgestellt wurden, lassen sich nicht immer durch Härtung und richtige Konfiguration des AD entschärfen. Manchmal sind zusätzlich spezielle Werkzeuge erforderlich.

Im Folgenden wird eine Auswahl an kostenlosen Open-Source- sowie kommerziellen Tools vorgestellt, die Administratoren bei der Absicherung und Verteidigung eines AD sowie bei der Wiederherstellung eines kompromittierten AD helfen. Insbesondere übernehmen sie folgende Aufgaben:

- Verringern der Angriffsfläche durch proaktives Schließen von Schwachstellen;
- Erkennung laufender Angriffe;
- Analyse und Aufarbeitung laufender und vergangener Angriffe;
- Entfernen von Angriffsspuren und Rückgängigmachen von Manipulationen;
- Disaster Recovery.

Die nachfolgenden Angaben basieren zum größten Teil auf öffentlich verfügbaren Informationen zu den jeweiligen Werkzeugen, teilweise auch auf Produktdemonstrationen durch die Hersteller. Außerdem flossen Erfahrungen des Autors aus dem praktischen Einsatz der Werkzeuge in Projekten ein. Eine Übersicht über die Tools nebst ihren wichtigsten Eigenschaften bietet die Tabelle.

Übersicht mit PingCastle

Bei PingCastle handelt es sich um ein Open-Source-Produkt, das eine Übersicht des Sicherheitsstatus eines AD liefert. In der eigenen Umgebung ist es kostenlos in fast vollem Funktionsumfang einsetzbar. Lediglich weniger wichtige Funktionen wie die Einordnung der Ergebnisse nach dem Maturity Level, also dem Reifegrad (inspiriert durch die französische Sicherheitsbehörde ANSSI – Agence nationale de la sécurité des systèmes d'information), und nach der MITRE-ATT&CK-Matrix sind nur in den Ergebnisberichten der kommerziellen, kostenpflichtigen Pro-Version enthalten.

PingCastle benötigt zur Ausführung lediglich die Rechte regulärer Domänenbenutzer. Denn auch diese sind in der Lage, große Mengen an Informationen aus dem Active Directory auszulesen, die PingCastle 156 Prüfungen (Stand: Februar 2022) unterzieht. Eine detaillierte Liste der Prüfpunkte ist online einsehbar (siehe ix.de/zd6b). Während der Ausführung generiert das Werkzeug einen Ergebnisbericht im HTML-Format, in dem alle

Werkzeuge für das Absichern des Active Directory

Hersteller	Attivo Networks		Microsoft	PingCastle	Semperis			Silverfort	SpecterOps		Stealthbits (Netwrix)		Tenable
Werkzeug	ADAssessor	ADSecure	Defender for Identity	PingCastle	Purple Knight	DSP	ADFR	Silverfort	Blood-Hound	BloodHound Enterprise	Stealth-DEFEND	Stealth-INTERCEPT	Tenable.AD
Angriffe verhindern													
Indicators of Exposure (IOE): Erkennung/Behebung von Schwachstellen	✓ (ongoing*)		✓ (ongoing)	✓ (Point in Time**)	✓ (Point in Time)	✓ (ongoing)			✓ (Point in Time)	✓ (ongoing)			✓ (ongoing)
MFA								✓					
Angriffe erkennen													
Indicators of Attack (IOA): Erkennung von Angriffen	✓		✓					✓			✓		✓
User Behavior Analytics			✓					✓			✓		
Deception		✓	✓								✓		
Incident Response / Unterstützung im AD-Betrieb													
Logging von Änderungen im AD						✓						✓	✓
Rollback von Änderungen im AD						✓							
Incident Response			✓			✓		✓			✓	✓	✓
Disaster Recovery							✓						

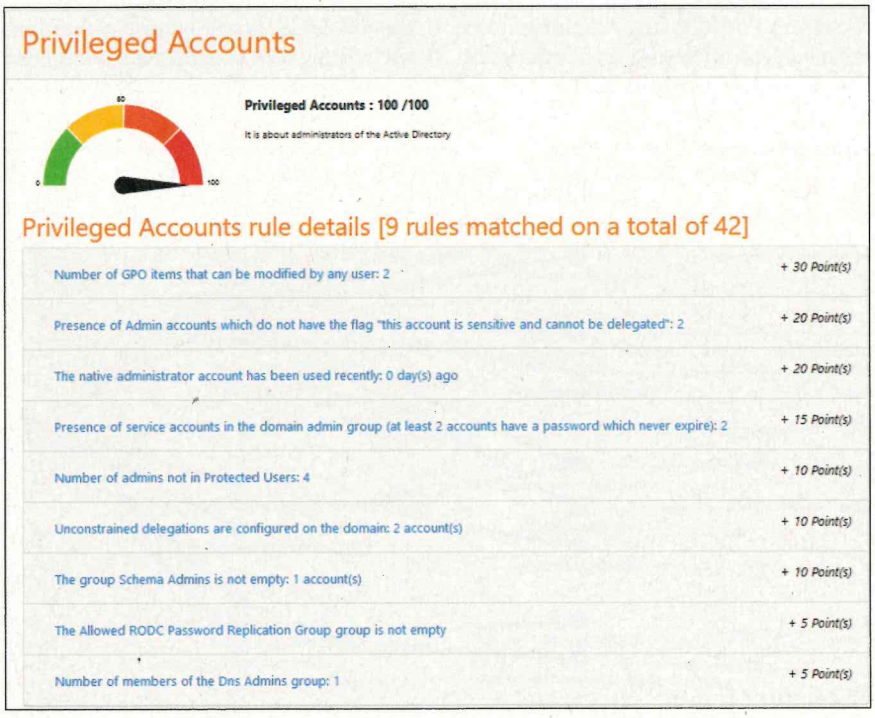
*kontinuierlich; ** zu einem bestimmten Zeitpunkt (Momentaufnahme)

Befunde und weitere interessante Konfigurationsdetails aufgelistet sind. Zu jedem einzelnen Befund liefert das interaktive HTML-Dokument eine genaue Beschreibung der Schwachstelle oder Fehlkonfiguration – die sogenannten Indicators of Exposure (IoE) –, eine Empfehlung zu ihrer Behebung und gegebenenfalls eine Übersicht der betroffenen Objekte (Abbildung 1).

Prinzipbedingt führt PingCastle Point-in-Time-Analysen durch, hält also nur den augenblicklichen Zustand der Umgebung fest. Um eine historische Auswertung des Zustands der Domäne zu erhalten, beispielsweise um dem Management die Verbesserung der Sicherheit im AD nahezulegen, ist die kostenpflichtige Professional- oder Enterprise-Lizenz oder eine manuell erstellte Visualisierung der Daten notwendig.

BloodHound wittert Seitwärtsbewegungen

BloodHound ist ebenfalls Open Source und sogar in vollem Funktionsumfang kostenlos einsetzbar. Seine Einrichtung wurde in [1] kurz vorgestellt. Während PingCastle im Allgemeinen nach Schwachstellen im AD sucht, konzentriert sich BloodHound auf Schwachstellen, die ein Lateral Movement erlauben [2] – also das Sich-Bewegen eines Hackers durch das Netzwerk, in das er eingedrungen ist.



PingCastle zeigt hier unter anderem, welche privilegierten Konten welche Schwachstellen aufweisen (Abb. 1).

Dazu untersucht es beispielsweise Berechtigungsvergaben und Beziehungen zwischen Objekten im AD, aber auch Informationen der domänenintegrierten Systeme wie die Windows-Clients und -Server selbst. Durch die Darstellung der Daten in einem Graphen werden auch lange und komplexe Angriffspfade einfach auffindbar.

Durch die anschließende Analyse lassen sich für den in Abbildung 2 gezeigten Fall beispielsweise folgende Schwachstellen finden und beheben:

- Gruppenverschachtelungen, die dazu führen, dass eine große Anzahl an Benutzern das Recht hat, die Passwörter hochprivilegierter Benutzer zurückzusetzen;
- administrative Berechtigungen oder Zugriffsberechtigungen für domänenintegrierte Systeme, die Gruppen wie „Jeder", „Authentifizierte Benutzer" oder „Domänenbenutzer" zugewiesen sind;
- Delegierung sensibler Rechte auf sicherheitskritische AD-Objekte (sogenannte High-Value Targets) wie Computer, die zur Public-Key-Infrastruktur (PKI) gehören, oder Systeme mit aktivierter uneingeschränkter Kerberos-Delegierung;
- Besitzer (Owner) von Computerkonten, bei denen es sich um Domänencontroller handelt, deren Besitzer aber nicht Mitglied der Gruppe der Domänenadministratoren sind;
- minderprivilegierte Administratoren mit der Rolle Helpdesk, die über Gruppenmitgliedschaften administrative Rechte in der Virtualisierungsumgebung haben, in der die Domänencontroller betrieben werden;
- administrative Berechtigungen eines regulären Benutzers auf einem System, auf dem ein hochprivilegierter Benutzer (zum Beispiel Domänenadministrator) angemeldet ist.

Insbesondere der letzte Punkt ist ein gutes Beispiel dafür, wie sich nach der Einführung von Maßnahmen des Enterprise Access Model von Microsoft (ehemals AD-Tiering-Modell; siehe ix.de/zd6b) deren Einhaltung und Wirksamkeit mithilfe von BloodHound überprüfen lässt.

PingCastle und BloodHound ergänzen einander gut und helfen Administratoren und auch professionellen Auditoren, den Großteil an Sicherheitslücken im Active Directory und der darin eingebundenen Systeme zu erkennen und zu schließen.

In großen Umgebungen mit sehr vielen Objekten und Beziehungen im Active Directory stößt BloodHound allerdings gelegentlich an seine Grenzen. So kann es, abhängig von der konkreten Abfrage, einige Minuten oder sogar Stunden dauern, bis das Tool die Daten analysiert hat und den Graphen anzeigt. Unter anderem dieses Problem soll mit dem Produkt BloodHound Enterprise gelöst werden.

Größer dimensioniert: BloodHound Enterprise

Dabei handelt es sich um eine kostenpflichtige Software as a Service (SaaS). Wie das freie Tool verfolgt auch die Enterprise-Version das Ziel, Schwachstellen aufzudecken, die Lateral Movement und Privilege Escalation im AD ermöglichen. BloodHound Enterprise soll jedoch mehrere Unzulänglichkeiten von BloodHound in großen Umgebungen beheben.

Bediener des regulären BloodHound-Werkzeugs in Active-Directory-Domänen mit sehr vielen Objekten benötigen viel Erfahrung und Know-how zu den verschiedenen Angriffspfaden und deren Ursachen, um unter der Vielzahl von Beziehungen und Pfaden die wichtigsten Schwachstellen zu priorisieren und die richtigen Schlüsse daraus zu ziehen.

Dem gegenüber steht die automatische Priorisierung der Schwachstellen und Maßnahmen von BloodHound Enterprise. Sie basiert auf der Grundidee, sich bei der Analyse der Angriffspfade auf den letzten Schritt der jeweiligen Pfade zu konzentrieren und so mit nur wenigen Anpassungen die Angriffsketten zu unterbrechen, die von vielen kompromittierbaren Objekten ausgehen (siehe Abbildung 3).

Das schon angesprochene Performanceproblem soll dadurch gelöst werden, dass BloodHound Enterprise in der Cloud betrieben und eine Graph-Rendering Library eingesetzt wird, die die Berechnungen auf GPUs auslagert und so deutlich performanter arbeitet.

Mit der historischen Übersicht über die Anzahl der Objekte mit Angriffspfaden zu High-Value Targets kann man beispielsweise die Effektivität der umgesetzten Maßnahmen messen und sicherstellen, dass zukünftige administrative Maßnahmen die Angreifbarkeit nicht wieder erhöhen. Abbildung 4 zeigt weitere vom Hersteller aufgelistete Unterschiede.

Semperis: vor und nach dem Angriff

Der Anbieter Semperis hat drei Produkte in seinem Portfolio, die Administratoren bei unterschiedlichen Aufgaben unterstützen. Bei allen dreien handelt es sich um On-Premises-Produkte ohne Cloud-Komponenten.

Das erste, Purple Knight, ist ein Auditierungswerkzeug für Active-Directory-Domänen, das ähnlich wie PingCastle das Active Directory in seinem aktuellen Zustand auf Schwachstellen untersucht (siehe Abbildung 5). Purple Knight lässt sich kostenlos herunterladen, nachdem über die Website (siehe ix.de/zd6b) Zugriff auf das Werkzeug angefragt wurde.

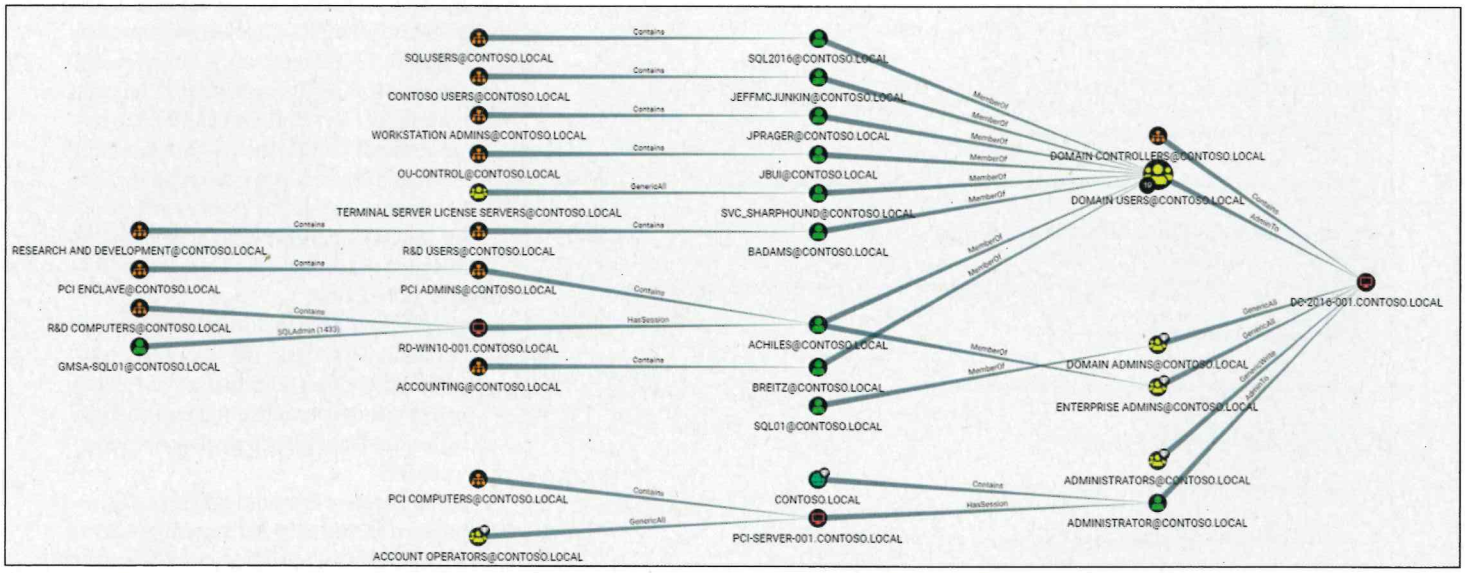
Die Ausführung erfolgt im Kontext eines regulären AD-Benutzers. Die gefundenen Schwachstellen werden von Purple Knight in zwei Kategorien aufgeteilt:

- IOE: Indicators of Exposure (Pre-Attack) – also Schwachstellen im klassischen Sinne;
- IOC: Indicators of Compromise (Post-Attack) – also Schwachstellen, die auf eine bereits erfolgte Kompromittierung hindeuten.

Anschließend werden die Ergebnisse als HTML- oder PDF-Bericht ausgegeben. Hierbei handelt sich also auch um eine Point-in-Time-Analyse.

Änderungen anzeigen und bearbeiten

Das Werkzeug DSP (Directory Services Protector) von Semperis ist kostenpflichtig und hat zwei wichtige Funktionen. Zum einen prüft es das Active Directory auf Schwachstellen wie Purple Knight auch. DSP führt diese Analyse jedoch nicht als Point-in-Time-Überprüfung, sondern fortlaufend durch. Somit können sich Administratoren sehr schnell über eine neue Schwachstelle informieren, zum Beispiel



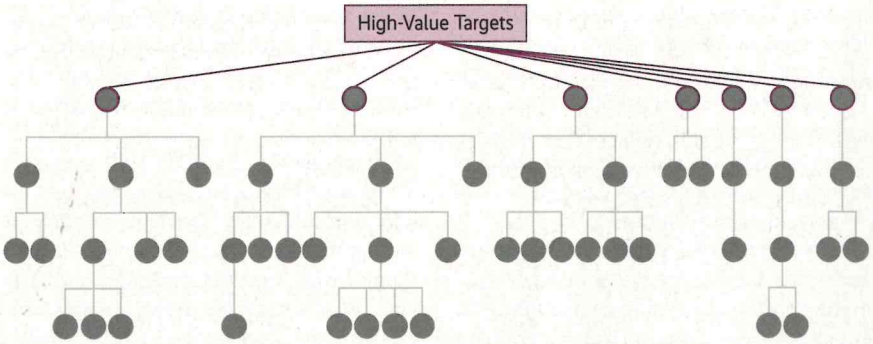
Der „Bluthund" zeigt hier mögliche Angriffspfade zur Kompromittierung eines Domänencontrollers (Abb. 2).

wenn sie gerade erst durch eine Änderung eines Administrators eingebracht wurde oder Semperis die Liste der Schwachstellenchecks erweitert hat.

Technisch besteht DSP aus zwei Agenten, die auf Domänencontrollern installiert werden und hierüber zum einen den Replikationsdatenstrom des Active Directory konsumieren (Was wurde geändert?) und zum anderen das Audit-Log der Domänencontroller auslesen (Wer hat es geändert?). Die über die Agenten ausgelesenen Daten werden in einer Datenbank archiviert und sind anschließend über die DSP-Website auswertbar.

Das befähigt DSP zu seiner zweiten Hauptaufgabe: Es bietet Administratoren eine Oberfläche, auf der sich sämtliche Änderungen an Objekten im AD zusammen mit den Details, etwa wer sie durchgeführt hat, nachvollziehen lassen. Sie können nach spezifischen Änderungen suchen, die Einstellung davor und danach vergleichen und diese sogar direkt über die DSP-Oberfläche rückgängig machen.

Alternativ lässt sich im Rahmen eines Incident-Response-Szenarios auch nach Änderungen suchen, die ein bestimmter Benutzer in der Vergangenheit durchgeführt hat, wenn beispielsweise der Verdacht besteht, dass der Benutzer kompromittiert wurde. Der Administrator kann auch Regeln anlegen, damit DSP warnt, wenn jemand vorher definierte Änderungen durchführt. Optional kann DSP diese auch sofort rückgängig machen.



Modellhaft sieht man hier, wie das Beheben von nur sieben Schwachstellen (farbig markiert) eine Kompromittierung verhindert, die von zahlreichen Objekten im AD ausgehen kann (Abb. 3).

Alles auf Anfang mit ADFR

ADFR (Active Directory Forest Recovery) ist das dritte Produkt von Semperis. Es ist ebenfalls kostenpflichtig und dient der Wiederherstellung des Active Directory nach einem Katastrophenfall. Hierzu wird auf den betreffenden Domänencontrollern der ADFR-Agent installiert, der nach erfolgter Konfiguration die Active-Directory-Daten sichert.

Falls dann in der Zukunft eine Wiederherstellung nach einem Katastrophenfall (Disaster Recovery) erforderlich wird, zum Beispiel wenn die Domäne vollständig kompromittiert wurde oder wenn eine Ransomware auch das Active Directory mitverschlüsselt hat, kann der Forest mithilfe von ADFR laut Hersteller in unter einer Stunde wiederhergestellt werden. Die manuelle Wiederherstellung eines Forest ohne ADFR umfasst laut Semperis circa 28 Schritte und ist sowohl zeitaufwendig als auch fehleranfällig.

Diesen Vorgang automatisiert ADFR auf einfache Weise. Es sind lediglich die IP-Adressen des neuen Servers (zukünftiger Domänencontroller) mit installiertem ADFR-Agenten anzugeben und die Wiederherstellung auf diesem Server beginnt. Da ADFR ausschließlich die Active-Directory-Daten sichert, ist das Backup

Category	BLOODHOUND	BLOODHOUND ENTERPRISE
Objective	• Identify Attack Paths from target principal(s) to an objective (e.g., "How can I get from Bob's laptop to Domain Admin")	• Continuously identify all Attack Paths risks • Prioritize risks by quantifiable exposure • Provide prescriptive, practical remediation guidance • Visualize Attack Path risk posture over time
Target User	• Penetration Testers • Red Teams	• Security Operations Teams • IT Operations Teams • Active Directory Administrators and Architects
Delivery	• Electron Application installed on a computer • Dark Mode support	• Software-as-a-Service (SaaS) web application • Full REST APIs • User Management with RBAC
Support	• Robust and active BloodHound Slack community	• Enterprise Support Model
Data Collection	• Manual operation for data collection • Stealth options to avoid defensive teams • May require additional steps to evade antivirus • Support for Azure	• Distributed collectors with health monitoring • Scheduled data collection • Signed binaries
Data Reconciliation	• Data must be manually deleted and re-collected to display current Attack Paths	• Data reconciled automatically to display "current state" of Active Directory with active Attack Path risks
Analytics	• Pre-built Analytic Queries used in search (e.g., "Find Shortest Paths to Domain Admins")	• Automatically identifies all Attack Path risks • Prioritizes Attack Path risks based on quantifiable Tier Zero and critical asset exposure
Remediations	• Not Applicable	• Prescriptive remediations with step-by-step instructions • Exportable full scope remediation plans • Logging Guidance to protect against breaking changes
Trend Reporting	• Not Applicable	• Attack Path risk trend reporting over time (e.g., Tier Zero exposure %, active risks, etc.)
Search	• Pathfinding across assets • Free-form search • Support for graphing hundreds of nodes	• Pathfinding across assets • Support for graphing hundreds of thousands of nodes

Mit der kostenlosen Version lässt es sich schon gut arbeiten, die Enterprise-Version von BloodHound setzt noch einen drauf (Abb. 4).

deutlich kleiner, als wenn beispielsweise über Windows-Bordmittel der Systemstatus gesichert wird. Somit kann die Backup-Frequenz problemlos erhöht werden und es besteht nicht die Gefahr, dass im Rahmen der Wiederherstellung ein gegebenenfalls mit Schadsoftware infiziertes Betriebssystem zurückgespielt wird.

Voraussetzung für eine sichere Wiederherstellung ist, dass zweifelsfrei festgestellt werden kann, wann die Kompromittierung erfolgte, und ein Backup der Daten vor diesem Zeitpunkt existiert.

Häufige Angriffe erkennen mit Tenable.ad

Das kommerzielle Produkt Tenable.ad des nahezu gleichnamigen Anbieters ist als Cloud- oder On-Premises-Variante erhältlich. In der On-Premises-Form besteht es aus mehreren virtuellen Maschinen, die im internen Netzwerk betrieben werden. Bei der Cloud-Variante wird die Verbindung über einen Site-to-Site-VPN-Tunnel zum Anbieter realisiert.

Das Werkzeug unterstützt Administratoren in drei verschiedenen Bereichen. Zunächst durchsucht auch Tenable.ad das Active Directory laufend nach vorhandenen Schwachstellen, berichtet darüber in einer Webapplikation und gibt Empfehlungen aus, wie diese behoben werden können. Die historische Entwicklung dieser Indicators of Exposure ist einsehbar; weitere Metriken geben Auskunft über den sicherheitstechnischen Zustand des Active Directory.

Die Trail-Flow-Funktion archiviert jegliche Änderung an Objekten im Active Directory. Dazu werden die Daten des AD bei der initialen Einrichtung einmal vollständig eingelesen und ab dann erhält Tenable.ad durch die Kommunikation mit der Replikations-API Kenntnis von allen durchgeführten Änderungen im Active Directory.

Prinzipbedingt lassen sich somit in Tenable.ad sämtliche Änderungen an Objekten im AD analysieren und mit den jeweiligen Einstellungen davor und danach vergleichen. Wer was verändert hat, lässt sich jedoch nicht erkennen, da diese Informationen nicht in den Replikationsdaten enthalten sind.

Im Bereich der Angriffserkennung (Indicators of Attack) ist Tenable.ad laut Hersteller in der Lage, sieben häufig durchgeführte Angriffe zu erkennen:

- DCSync
- Golden Ticket
- OS Credential Dumping: LSASS Memory
- DCShadow
- Password Guessing
- Password Spraying
- PetitPotam

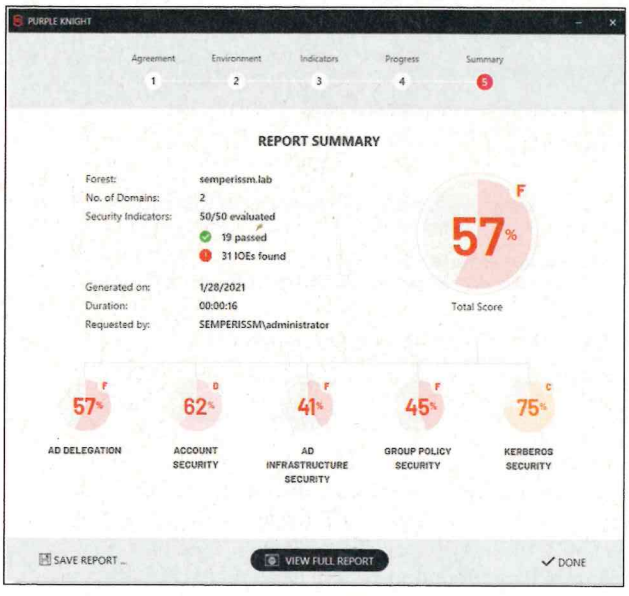
Attivo Networks – den Angreifer täuschen

Die beiden kostenpflichtigen Produkte ADAssessor und ADSecure von Attivo Networks helfen bei der Absicherung von Active Directorys und bei der Erkennung laufender Angriffe. ADAssessor analysiert das Active Directory fortlaufend auf Sicherheitslücken und gibt Empfehlungen, um diese proaktiv zu schließen.

ADSecure ist die Active-Directory-Komponente der größeren Endpoint Detection Net Suite (EDN) von Attivo Networks, die einen Angreifer durch das Manipulieren von Daten und das Auslegen von Ködern in die Irre führen soll. Hierzu werden Agenten auf den Arbeitsplatzcomputern und Servern installiert, die die Antworten auf Anfragen des lokalen Betriebssystems an Domänencontroller manipulieren und gefälschte Daten zurückliefern.

Auf diese Weise erhält ein Angreifer, der eines dieser Systeme kompromittiert hat und Informationen über die Domäne sammeln möchte, Daten, die ihn entweder verwirren oder auf Systeme locken, die ausschließlich für ihn bestimmt sind und nicht zur produktiven Infrastruktur gehören, um dort seine Aktivitäten zu beobachten. Eine Anfrage, auf welchem System gerade Domänenadministratoren angemeldet sind, liefert dann beispielsweise nicht die tatsächlichen Namen oder IP-Adressen der Systeme zurück, sondern andere.

Einen anschließenden Zugriff des Angreifers auf die Systeme aus den manipulierten Antworten meldet ADSecure. Die Administratoren werden so über den potenziellen Angriff informiert.



Purple Knight sortiert die gefundenen Schwachstellen in Gruppen. Details liefert der Report (Abb. 5).

Silverfort – eine zweite Meinung

Das kostenpflichtige Silverfort dient der Absicherung des AD auf eine etwas andere Art und Weise. Das Produkt integriert sich in den Authentifizierungs-Workflow und kann eine „zweite Meinung" abgeben, nachdem ein Domänencontroller seine Entscheidung über einen Authentifizierungsversuch getroffen hat. Hierzu werden Silverfort-Agenten auf allen Domänencontrollern installiert. Die zweite Meinung von Silverfort kann im Erlauben oder Verbieten des Zugriffs bestehen oder darin, eine zweite Form der Authentifizierung anzufordern (Mehr-Faktor-Authentifizierung, MFA).

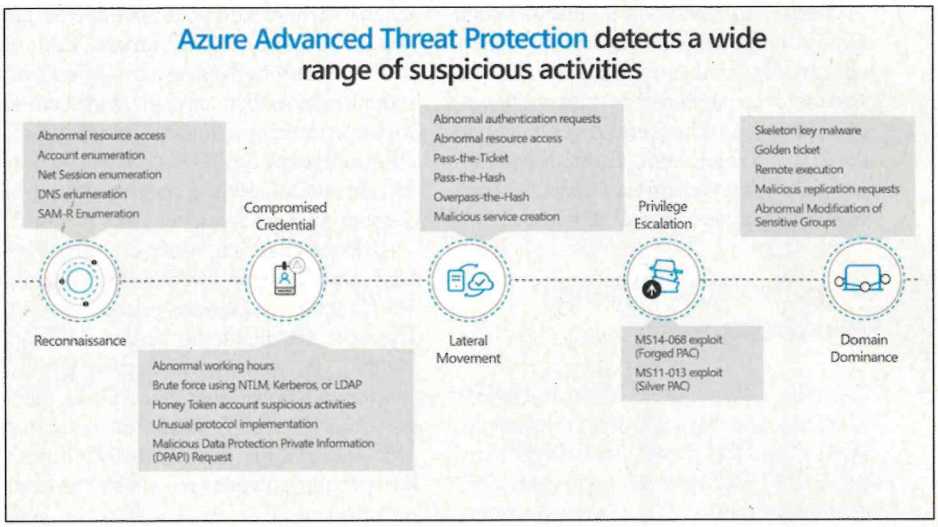
Auf welcher Basis Silverfort seine Entscheidung treffen soll, können die Administratoren detailliert konfigurieren. Es lässt sich beispielsweise festlegen, dass beim Zugriff auf Netzwerkfreigaben, beim Ausführen des Fernzugriffstools PsExec oder bei einem Zugriff via RDP ein zweiter Faktor erforderlich ist. Eine Unterscheidung dieser Zugriffe ist möglich, da Silverfort die Entscheidungen zum Beispiel auf Basis des angefragten Kerberos SPN (Service Principal Name) treffen kann.

Außerdem bezieht Silverfort bei jeder Entscheidung weitere Parameter mit ein, um risikoreiche Authentifizierungsversuche oder ein auffälliges Verhalten von Benutzerkonten durch das Erfordernis eines zweiten Faktors abzusichern oder die Administratoren über das Verhalten zu alarmieren. So können Dienstkonten etwa Brute-Forcing-Versuche oder auffälliges Verhalten bemerken.

Als zweiten Faktor unterstützt Silverfort viele verschiedene Möglichkeiten: Microsoft Authenticator, DUO, Yubico oder RSA. Darüber hinaus lassen sich neben dem Active Directory auch weitere sogenannte Identity-Provider anbinden, zum

Beispiel ADFS-Server (Active Directory Federation Services), Azure Active Directory, Okta, Ping oder generische Geräte und Produkte, die RADIUS (Remote Authentication Dial-In User Service) verwenden.

Diese zu den Authentifizierungsvorgängen im AD von Silverfort erhobenen und archivierten Daten lassen sich auch zur Incident Response heranziehen, um etwa herauszufinden, wie sich ein Benutzerkonto verhalten hat, wenn bekannt ist, dass es beispielsweise um 8:54 Uhr kompromittiert wurde. Die Information, dass sich der kompromittierte Benutzer um 9:03 Uhr vom System Client4872 aus via Kerberos über CIFS (Netzwerkfreigabe) am Server Fileserver1 angemeldet hat, kann für die Aufarbeitung des Vorfalls hilfreich sein.



In einem Video (hier ein Snapshot daraus) demonstriert Microsoft, welche verdächtigen Aktivitäten entlang der verschiedenen Angriffsphasen sein Defender for Identity aufdecken kann (Abb. 6).

Microsofts Defender for Identity

Defender for Identity (vormals Azure Advanced Threat Protection) ist der Teil der kostenpflichtigen Microsoft-Defender-Cloud-Security-Produkte, der sich mit dem Active Directory beschäftigt. Im Rahmen der Implementierung wird der Defender-for-Identity-Agent auf allen Domänencontrollern und neuerdings auch auf allen ADFS-Servern installiert. Die Agenten sammeln anschließend Daten (Eventlog), analysieren den Netzwerkverkehr (NTLM, Kerberos, LDAP, RPC, DNS, SMB) oder lesen den Inhalt des Active Directory aus.

Die gesammelten Daten werden vorgefiltert und in die Cloud von Microsoft hochgeladen. Nach der Analyse alarmiert Defender for Identity bei Angriffen oder Auffälligkeiten entlang der Phasen eines Angriffs: Informationssammlung, Kompromittierung der Zugangsdaten, Ausbreitung im Netzwerk, Erweiterung der Privilegien und vollständige Kompromittierung der Domäne.

Defender for Identity erkennt beispielsweise das Datensammeln mit BloodHound, das Durchführen von Brute-Force-Angriffen, Pass-the-Hash- oder Pass-the-Ticket-Angriffe sowie einen Golden-Ticket-Angriff.

Neben der Erkennung dieser technischen Angriffe kann Defender for Identity auch bei verdächtigem Verhalten von Benutzern alarmieren, beispielsweise beim Verbinden des VPN eines Benutzers aus einem ungewöhnlichen Land oder dem plötzlichen gehäuften Zugriff auf Systeme einer Abteilung, der der Benutzer nicht angehört. Außerdem können Benutzer als „Honeytoken" markiert werden: Alle Authentifizierungen solcher Benutzer lösen dann sofort einen Alarm aus.

Auch Defender for Identity analysiert den aktuellen Zustand der Active-Directory-Konfiguration, warnt vor sicherheitsrelevanten Fehlkonfigurationen und gibt Empfehlungen zur Behebung aus.

Das Tool liefert wichtige Daten bei der Aufarbeitung von Sicherheitsvorfällen, etwa um zu analysieren, auf welche Systeme ein Benutzer nach seiner Kompromittierung zugegriffen hat. Insbesondere wenn weitere Komponenten von Microsoft Defender Cloud Security zum Einsatz kommen, wird die „Advanced Hunting"-Funktion von Microsoft 365 schnell sehr mächtig. Mit ihr kann man beispielsweise die Logs der Computer (Defender for Endpoint) und die Logs von Defender for Identity gemeinsam in einem Arbeitsschritt und mit einer einheitlichen Abfragesprache (Kusto Query Language) durchsuchen und Ereignisse aus beiden Bereichen korrelieren. Dies liefert schnell ein umfassendes Bild mit viel Kontext über das, was in der Infrastruktur zum fraglichen Zeitpunkt vorgefallen ist.

Stealthbits lernt auch selbst

Stealthbits, mittlerweile Teil des Unternehmens Netwrix, bietet zwei kostenpflichtige Produkte (StealthINTERCEPT und StealthDEFEND) im Active-Directory-Security-Umfeld, die sich kombiniert einsetzen lassen und ergänzen. Zur Implementierung werden StealthINTERCEPT-Agenten auf den Domänencontrollern installiert. Sie liefern anschließend die Daten für beide Produkte auf jeweils getrennt voneinander zu installierenden On-Premises-Servern.

StealthDEFEND erkennt Angriffe auf das Active Directory oder auf Dateiserver und gibt einen Alarm aus. Mögliche Angriffe könnten sein: Informationsgewinnung über LDAP (zum Beispiel mit BloodHound), Pass-the-Ticket-, Golden-Ticket- oder DCSync-/DCShadow-Angriffe. Nach einer Einlernphase von 30 Tagen für jeden Benutzer meldet StealthDEFEND außerdem auch eine Bedrohung, wenn sich das Nutzerverhalten plötzlich signifikant verändert.

Darüber hinaus ist die Dateiserverkomponente von StealthDEFEND in der Lage, laufende Ransomware-Angriffe zu erkennen. Hierzu werden die Vorgänge in den Dateisystemen überwacht, entweder über einen Agenten auf Windows-Fileservern oder über Schnittstellen zu bekannten NAS-Systemen wie NetAPP oder EMC. Wird so eine bestimmbare Anzahl von Dateien mit bekannten Ransomware-Endungen oder Namensschemas von Ransomware-Hinweisen erkannt, meldet StealthDEFEND eine Bedrohung.

StealthDEFEND kann automatisiert auf erkannte Bedrohungen für AD- oder Fileserver reagieren: etwa Gruppenmitgliedschaften von AD-Objekten ändern, Konten deaktivieren oder Endgeräte (Clients oder Server) umkonfigurieren. Für die zuletzt genannte Maßnahme wird in StealthDEFEND ein Benutzer mit administrativen Rechten auf den Endgeräten hinterlegt und StealthDEFEND kann als Reaktion auf eine Bedrohung dann beispielsweise eine Windows-Firewallregel erstellen, um einen Angriff zu stoppen, oder ein PowerShell-Skript ausführen.

StealthDEFEND kann Administratoren beim Aufarbeiten einer Bedrohung unterstützen. Es durchsucht die gesammelten und archivierten Daten und filtert diejenigen heraus, mit denen man den Ablauf und die Auswirkungen erfolgter Angriffe nachvollziehen und weitere betroffene Systeme oder Benutzer identifizieren kann.

Angriffe nachvollziehen und untersuchen

Dazu loggt StealthDEFEND aber nicht jede einzelne Änderung an den Objekten im Active Directory. Dies ist die Aufgabe von StealthINTERCEPT: Es archiviert jegliche Änderung im AD, mit den Informationen, was genau sich geändert hat, wer die Änderung vorgenommen hat und von wo aus. Auch Authentifizierungsvorgänge werden protokolliert. So kann man beispielsweise analysieren, woher nicht erfolgreiche Anmeldeversuche stammen, wenn ein Benutzerkonto gesperrt wurde.

Eine weitere Funktion von StealthINTERCEPT ist es, Änderungen im Active Directory auf der Basis von Regeln zu verbieten. Damit lässt sich beispielsweise konfigurieren, dass nur zwei Mitglieder der eigentlich zehn Benutzer beinhaltenden Domänenadministratorengruppe weitere Benutzer zur Gruppe der Domänenadministratoren hinzufügen dürfen.

Die Firma ManageEngine hat mehrere Produkte im Portfolio, die den Administratoren beim Verwalten des Active Directory helfen. Zwar handelt es sich dabei nicht um dedizierte Sicherheitsprodukte, eines dieser Werkzeuge, „ADAudit Plus" für Change Management, kann dennoch in diesem Kontext nützlich sein. Es protokolliert und archiviert unter anderem Änderungen im Active Directory und Benutzeranmeldungen. Zu den gesammelten Daten lassen sich anschließend auch Berichte und E-Mail-Alarme erstellen.

Passwortfilter für Domänencontroller

Im Active Directory, genauer auf Domänencontrollern, fehlt standardmäßig die Möglichkeit, das Setzen häufig verwendeter und schwacher Passwörter wie „Sommer2021" oder „Password123!" zu verhindern, sofern sie der Passwortrichtlinie – Groß- und Kleinschreibung, Sonderzeichen et cetera – entsprechen. Gerade für das Active Directory ist die Wahl guter Passwörter jedoch elementar, denn der Angreifer kann sich beispielsweise eine Liste möglichst vieler AD-Benutzer erstellen und „sprayt" die Trivialpasswörter gegen diese Liste. Gegebenenfalls kann er so Benutzer kompromittieren, die interessante Rechte haben, die ihm beim Lateral Movement behilflich sind. Details sowie Hilfestellungen für Passwortsicherheit liefert der Artikel „Passwortsicherheit (nicht nur) im Active Directory" [3].

In Windows kann jedoch eine beliebige DLL-Datei in den LSASS.EXE-Prozess auf Domänencontrollern geladen werden. Dieser Prozess ist unter anderem für den Vorgang der Passwortänderung verantwortlich. Eine solche DLL-Datei kann diese Deny-Listing-Funktion enthalten und verhindern, dass Benutzer bereits kompromittierte oder schwache Passwörter setzen.

Eine Reihe von Open-Source-Projekten auf GitHub nutzt diese Schnittstelle zu LSASS.EXE, um verschiedene Prüfungen beim Ändern von Passwörtern im Active Directory hinzuzufügen. Sie prüfen dann etwa bei einer Passwortänderung, ob sich das neue, vom Benutzer gewünschte Passwort in der Liste der bereits kompromittierten Passwörter des von Troy Hunt initiierten Projekts „Have I Been Pwned" (siehe ix.de/zd6b) befindet, und verhindern, dass es auf diesen Wert gesetzt wird.

Der Administrator lädt hierzu eine Hashliste der in der Datenbank von Have I Been Pwned befindlichen Passwörter herunter und verteilt sie zum Abfragen mit der DLL auf allen Domänencontrollern. Mit einigen dieser Projekte lassen sich auch bestimmte Zeichenfolgen in einem Passwort verbieten. So kann man auch verhindern, dass ein Mitarbeiter das Passwort <FIRMENNAME>123$ setzt. Beispielhaft seien hier die Projekte ad-password-protection und PwnedPasswordsDLL genannt (beide siehe ix.de/zd6b).

Um ihre Aufgaben zu erfüllen, müssen die DLL-Dateien auf allen Domänencontrollern in den LSASS.EXE-Prozess geladen werden.

Kein Lerneffekt

Leider informieren die bekannten Implementierungen der Passwortkontrollfunktion den Benutzer nicht darüber, warum das von ihm gewählte Passwort abgelehnt wurde. Er erhält lediglich dieselbe generische Fehlermeldung, die er auch beim Versuch erhält, ein gegen die generelle Passwortrichtlinie verstoßendes Passwort zu wählen. Eine Einführung dieser DLLs sollte also mit einer Informationskampagne für die Benutzer einhergehen, um deren Frustration bei der Passwortwahl möglichst gering zu halten.

Die im Rahmen dieses Artikels vorgestellten Open-Source-Projekte wurden vom Autor nicht auf Unbedenklichkeit überprüft. Vor der produktiven Implementierung sollten daher ihre Stabilität und der Quellcode eingehend geprüft werden.

Fazit

Auch wenn die Gefahr, angegriffen zu werden, für das Active Directory groß ist und die Einfallstore zahlreich sind – machtlos sind die Verteidiger nicht. Viele Werkzeuge helfen dabei, die Sicherheit proaktiv zu erhöhen und Sicherheitslücken zu schließen, bevor sie ausgenutzt werden können. Im besten Fall reicht dies schon und Angreifer wenden sich stattdessen einfacheren Zielen zu. Im schlimmsten Fall verlängert es lediglich die Zeitspanne, die ein Angreifer im internen Netzwerk eines Unternehmens benötigt, um an sein Ziel zu gelangen. Doch auch für diese Phase stehen Werkzeuge zur Verfügung, die Angriffe erkennen und Alarm schlagen.

Sollte es einem kompetenten Angreifer dennoch gelingen, größere Teile der Infrastruktur oder sogar die gesamte Domäne zu kompromittieren, können einzelne Tools bei der Aufarbeitung des Sicherheitsvorfalls oder bei der Wiederherstellung (Disaster Recovery) wertvolle Dienste leisten. Dazu müssen die Werkzeuge aber bereits vor dem Vorfall implementiert worden sein. (ur@ix.de)

Quellen

[1] Marco Wohler; Mehr ist mehr; AD-Härtungsmaßnahmen jenseits von Group Policies; *iX* 6/2021, S. 92

[2] Frank Ully; Fette Beute; Passwörter und Hashes – wie Angreifer die Domäne kompromittieren; *iX* 11/2020, S. 94

[3] Sandro Affentranger; Schwierige Wahl; Passwortsicherheit (nicht nur) im Active Directory; *iX* 1/2022, S. 116

[4] Die im Text erwähnten Tools und Details sind über ix.de/zd6b zu finden.

Hagen Molzer

ist Senior-Berater bei der cirosec GmbH. Seine fachlichen Schwerpunkte liegen in den Bereichen Windows-Betriebssystem- sowie Active-Directory-Sicherheit, in denen er Penetrationstests, Beratungsprojekte sowie Red-Team-Assessments durchführt.