Ein praktischer Ansatz für Cyber Resilience

Sichern Sie die kritischen Assets in Ihrem hybriden Active Directory effizient mit Angriffspfadverwaltung.

Quest

Einführung

Unternehmen sind sich heute sehr bewusst, dass sie ihre Cybersicherheit verbessern müssen. Die Suche nach einer effektiven und effizienten Strategie zur Erreichung dieses Ziels erscheint jedoch oft schwierig. Angreifer erfinden ständig neue Taktiken und Techniken, sodass die IT-Abteilung kaum noch in der Lage ist, jeden neuen Brand zu bekämpfen.

Es gibt jedoch eine praktische Möglichkeit, dem Ansturm von Cyberangriffen einen Schritt voraus zu sein: Denken Sie wie ein Angreifer. Seit Jahren verwenden Hacker ein kostenloses Open-Source-Tool namens BloodHound, um den schnellsten Weg zur Übernahme einer Umgebung zu finden, sobald sie ein normales Benutzerkonto kompromittiert haben. Um mithalten zu können, müssen IT-Teams proaktiv all diese Angriffspfade aufzeigen, die Hacker ausnutzen könnten, und – was besonders wichtig ist – die wichtigsten Bereinigungsmaßnahmen ermitteln, die Hunderte oder Tausende dieser Angriffspfade auf einmal abschalten.

Jetzt haben sie ein Tool, das die effektive Verwaltung von Angriffspfaden leicht macht: SpecterOps BloodHound Enterprise. Dieses Whitepaper erklärt, wie die Angriffspfadverwaltung funktioniert und warum es ein praktischer Ansatz für moderne Cybersicherheit ist. Anschließend wird erläutert, wie Sie die Verwaltung von Angriffspfaden mit anderen wichtigen Strategien ergänzen können, um nicht nur Cybersicherheit, sondern auch Cyber Resilience zu erreichen.

Verschaffen Sie sich einen Überblick über Ihre kritischen Assets

Klassifizierung kritischer Assets in einer On-Premises-Umgebung

Ein wichtiger erster Schritt zum Schutz Ihrer IT-Umgebung ist die Kenntnis Ihrer wichtigsten IT-Assets. In einer On-Premises-Umgebung teilen IT-Experten die Assets in die folgenden Ebenen ein, die in Abbildung 1 dargestellt sind:

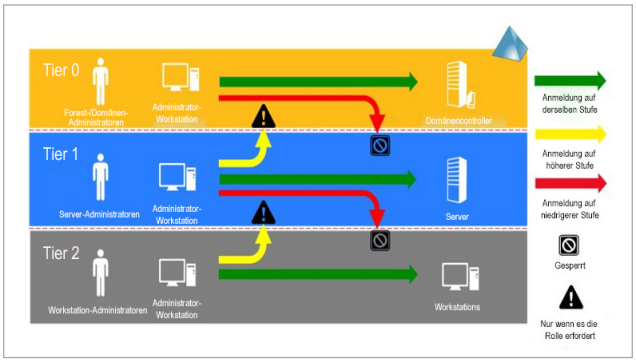

Abbildung 1: Klassifizierung kritischer Assets in einer On-Premises-Umgebung (Bildnachweis: Microsoft).

Tier 0 (die Steuerungsebene) umfasst Ihre sensibelsten Assets, z. B. Domänen-administratoren, Domänencontroller und administrative Workstations.

- **Tier 0:** Tier 0 (die Steuerungsebene) umfasst Ihre sensibelsten Assets, z. B. Gesamtstrukturen, Domänenadministratoren, Domänencontroller und administrative Workstations.
- **Tier 1:** Die nächste Stufe umfasst Ihre etwas weniger sensiblen Assets, z. B. Serveradministratoren und deren Workstations. Ganz allgemein besteht sie aus den folgenden zwei Ebenen:
  - **Verwaltungsebene –** für unternehmensweite IT-Verwaltungsfunktionen
  - **Daten-/Workload-Ebene –** für die Verwaltung der einzelnen Workloads, die entweder von IT-Mitarbeitern oder Geschäftseinheiten durchgeführt werden kann
- **Tier 2:** Tier 2 umfasst Assets wie Workstation-Administratoren und ihre Workstations. Sie kontrolliert sowohl den Benutzer- als auch den Anwendungszugriff.

Klassifizierung kritischer Assets in einer hybriden Umgebung

Dieses Modell lässt sich von lokalem Active Directory auf Hybrid-Umgebungen mit Azure AD ausweiten, wie in Abbildung 2 dargestellt. Wie Sie sehen, umfasst das Modell dieselben Komponenten wie oben beschrieben: Steuerungsebene, Verwaltungsebene, Daten-/Workload-Ebene, Benutzerzugriff und Anwendungszugriff.

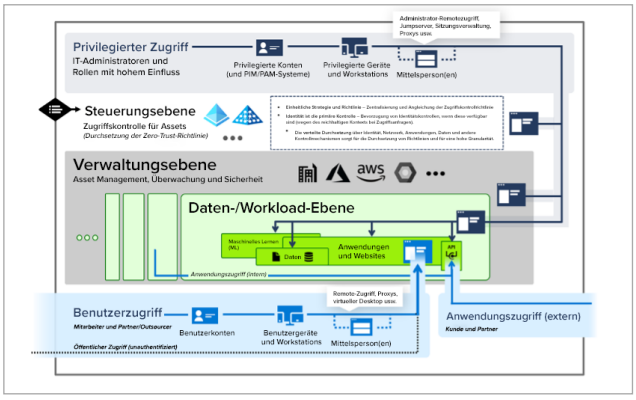

Abbildung 2: Klassifizierung kritischer Assets in einer On-Premises-Umgebung (Bildnachweis: Microsoft).

Wichtig ist, dass einige kritische Sicherheitsgrundsätze für beide Modelle gelten. In erster Linie sollte nichts in der Lage sein, irgendetwas auf einer höheren Ebene zu kontrollieren. Insbesondere sollten Assets in der Steuerungsebene niemals von Assets in der Verwaltungs- oder der Daten-/Workload-Ebene kontrolliert werden. Darüber hinaus sollte der Benutzer immer dann, wenn ein legitimer Bedarf für den Zugriff auf Ressourcen mit privilegiertem Zugriff besteht, ein spezielles privilegiertes Benutzerkonto und eine spezielle Workstation mit privilegiertem Zugriff (Privileged Access Workstation, PAW) verwenden.

> **Assets in der Steuerungsebene sollten niemals von Assets in der Verwaltungs- oder Daten-/Workload-Ebene kontrolliert werden.**

Wichtige Beispiele für kritische Assets

Es ist wichtig zu verstehen, dass kritische Assets nicht auf hochprivilegierte Konten wie Domänen- und Server-Administratoren beschränkt sind. Andere Beispiele sind:

- Domänencontroller (DCs), die alle Anmeldeinformationen für alle AD-Benutzerkonten enthalten
- Gruppenrichtlinienobjekte (Group Policy Objects, GPOs), die Tier-0-Assets betreffen
- Ihr Azure AD Connect-Server und das zugehörige Dienstkonto
- ADFS
- Server von Zertifizierungsstellen (Certificate Authority, CA) und PKI-Servern (Public Key Infrastructure), da ein Angreifer, der diese kompromittiert, Zertifikate generieren kann, mit denen er sich als beliebiger Benutzer anmelden kann, ohne dessen Kennwort zu kennen
- Sicherungen von Active Directory
- Workstations mit privilegiertem Zugriff

Aufdecken der Angriffspfade, die Ihre kritischen Assets gefährden

Angreifer sind natürlich erpicht darauf, sich Zugang zu Ihren kritischen Assets zu verschaffen. Wenn sie diese Assets kompromittieren, können sie ihr ultimatives Ziel erreichen – sei es, Ihre wertvollsten Daten zu stehlen, Ransomware in der gesamten Umgebung zu verbreiten, Ihre AD-Sicherungen zu beschädigen, um die Wahrscheinlichkeit zu erhöhen, dass Sie das Lösegeld zahlen, Hintertüren für zukünftige Zugriffe einzubauen oder etwas anderes.

Allerdings können Gegner in der Regel Ihre Tier-0-Assets bei ihrem ersten Angriff nicht gefährden. Stattdessen verwenden sie in der Regel Phishing, kennwortbasierte Angriffe und andere Techniken, um ein normales Benutzerkonto zu übernehmen. Wenn sie erst einmal Fuß gefasst haben, können sie ein Open-Source-Tool namens BloodHound verwenden, um eine Reihe von Schritten zu entdecken, mit denen sie die Kontrolle über Tier-0-Assets erlangen können. Eine solche Reihe von Schritten wird als **Angriffspfad** bezeichnet.

> **Ein Angriffspfad ist eine Reihe von Schritten, die es einem Angreifer, der ein normales Benutzerkonto kompromittiert hat, ermöglichen, Zugang zu Ihrer Steuerungsebene zu erhalten.**

Ein Angriffspfad ist nicht einfach ein fehlendes Sicherheitsupdate oder eine suboptimale Konfiguration, die durch effektives Patching und Schwachstellenverwaltung behoben werden kann. Vielmehr ist ein Angriffspfad eine Reihe von Schritten, die eine Kombination von Faktoren wie versteckte Berechtigungen, verschachtelte Gruppenmitgliedschaften, falsch konfigurierte Gruppenrichtlinien, inhärente Sicherheitslücken in der AD-Architektur und komplexe Beziehungen in Active Directory und Azure ausnutzt.

Am besten lassen sich Angriffspfade anhand eines Beispiels erklären. Abbildung 3 veranschaulicht einen Angriffspfad. Sein Ausgangspunkt ist ein normales Benutzerkonto, Alex. Dieses Benutzerkonto ist jedoch Mitglied der Gruppe HelpDesk, die wiederum Mitglied einer anderen Gruppe ist, dem Tier-2-Support. (Solche Gruppenverschachtelungen sind in AD sehr üblich.) Und die Tier-2-Supportgruppe hat lokale Administratorrechte auf dem Computer „Payment-01“. Demnach hat Alex – oder

ein Angreifer, der das Konto von Alex kompromittiert – lokale Administratorrechte auf diesem Rechner, auf dem ein Dienstkonto (SVC_PAYADMIN) angemeldet ist.

Infolgedessen kann Alex (oder der Angreifer) die lokalen Admin-Rechte des Kontos „Alex“ nutzen, um sich auf dem Computer „Payment-01“ anzumelden und ein Tool wie mimikatz auszuführen und damit die Anmeldeinformationen des Dienstkontos auszulesen und im Namen dieses Kontos zu handeln. Und das Dienstkonto hat das Recht, Mitglieder zur Domänenadministratorengruppe hinzuzufügen, ein Tier-0-Asset, das die volle Kontrolle über die Umgebung gewährt.

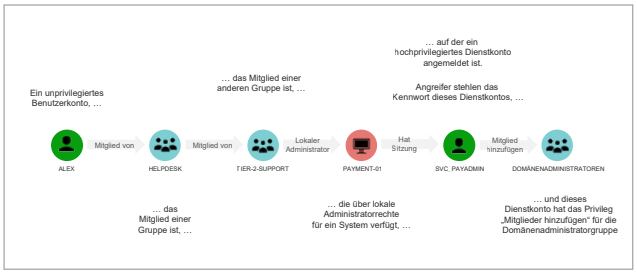

Abbildung 3: Ein Beispiel für einen Angriffspfad in Active Directory.

Verwaltung von Angriffspfaden

Angriffspfade kartieren

Das obige Beispiel veranschaulicht nur einen Angriffspfad in einer Umgebung – in den meisten Umgebungen gibt es Hunderte oder sogar Tausende von Angriffspfaden, die es einem Angreifer, der die Kontrolle über ein normales Benutzerkonto erlangt, ermöglichen, die Steuerungsebene zu kompromittieren.

Die Open-Source-Version von BloodHound zeigt normalerweise nur die kürzesten Angriffspfade in der Umgebung an. Es ist wie bei Google Maps – wenn Sie von Seattle nach Manhattan fahren, zeigt Ihnen Google Maps die zwei oder drei besten Routen für Ihre Reise an. Aber auch wenn es in der Regel ausreicht, nur die wichtigsten Routen von Google Maps abzurufen, müssen Sicherheitsteams über alle Angriffspfade in ihrer Umgebung Bescheid wissen, und nicht nur über die einfachsten.

Glücklicherweise gibt es jetzt eine Version des Tools, die speziell für Sicherheitsteams entwickelt wurde: SpecterOps BloodHound Enterprise. Es zeigt automatisch alle Angriffspfade auf, die zu Ihren kritischen Assets führen. BloodHound Enterprise analysiert alle Beziehungen in Ihrer Domäne und identifiziert jeden Weg, den ein Angreifer ausnutzen könnte, um in Ihre Steuerungsebene zu gelangen, wie in Abbildung 4 dargestellt. Noch besser: Es stellt diese Angriffspfade in einem klaren grafischen Format dar.

SpecterOps BloodHound Enterprise erstellt automatisch eine Karte aller Angriffspfade, die zu Ihren kritischen Assets führen.

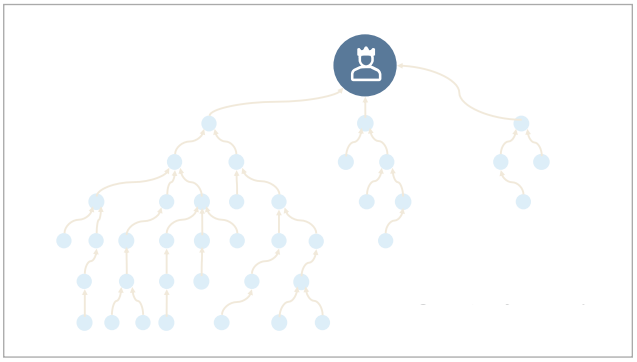

Abbildung 4: BloodHound Enterprise bildet alle Angriffspfade ab, die zu Ihrer Steuerungsebene führen.

Identifizierung und Entschärfung von Choke Points

Hunderte oder gar Tausende von Angriffspfaden einzeln zu entschärfen wäre natürlich selbst für das bestausgestattete IT-Team eine überwältigende Aufgabe. Das wäre so, als würde man versuchen, jede mögliche Route von Seattle nach Manhattan zu blockieren. Wenn Sie eine Route blockieren, werden die Gegner einfach eine andere wählen. Außerdem würden die Sperren, die Sie überall errichten, den legitimen Verkehr in Ihrer Umgebung stören und möglicherweise sogar das Geschäft praktisch zum Erliegen bringen.

Glücklicherweise bietet BloodHound Enterprise eine weitaus effektivere Option als eine derart verstreute Verteidigungsstrategie. Es fügt die aufgedeckten Angriffspfade zu einem einzigen kohärenten Bild zusammen, indem es alle Angriffspfade gruppiert, die den gleichen letzten Schritt (**Choke Point**) aufweisen. Selbst Unternehmen mit Tausenden von Angriffspfaden haben in der Regel nur eine Handvoll Choke Points.

BloodHound Enterprise quantifiziert sogar die Choke Points und sagt Ihnen mit hoher Sicherheit, welcher Prozentsatz Ihrer Konten der Ausgangspunkt für einen Angriffspfad ist, der von einem bestimmten Choke Point abhängt. Abbildung 5 zeigt zum Beispiel eine Umgebung mit drei Choke Points. Der linke ist der letzte Schritt in den Angriffspfaden, die 92 % aller Konten betreffen. Die Prozentsätze summieren sich auf mehr als 100 %, da ein bestimmtes Konto der Ausgangspunkt von mehr als einem Angriffspfad sein kann.

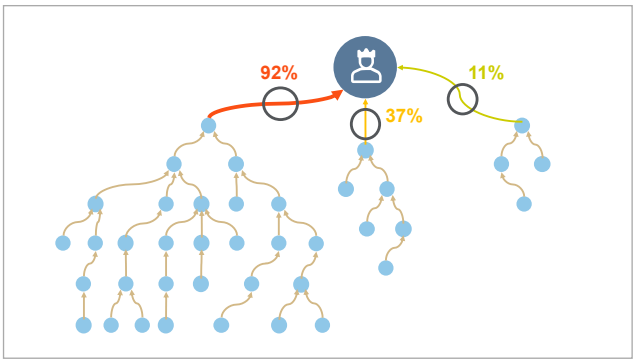

Abbildung 5: BloodHound Enterprise identifiziert die Choke Points, die Teil mehrerer Angriffspfade sind.

BloodHound Enterprise identifiziert die Choke Points, die von mehreren Angriffspfaden gemeinsam genutzt werden, so dass Sie Hunderte von ihnen auf einmal blockieren können.

Indem Sie einen Choke Point entschärfen, blockieren Sie jeden Angriffspfad, der auf diesen Punkt angewiesen ist. Und BloodHound Enterprise zeigt Ihnen die spezifischen Aktionen, die Sie durchführen müssen, z. B. das Entfernen einer bestimmten Berechtigung oder Instanz einer verschachtelten Gruppenmitgliedschaft.

Überwachung von Angriffspfaden

Manchmal können Unternehmen jedoch bestimmte Choke Points nicht schnell beheben, weil ihr Active Directory viele technische Altlasten aufweist – Beziehungen, Gruppenmitgliedschaften, Berechtigungen usw. sind so komplex, dass Änderungen das Risiko bergen, dass etwas kaputt geht, z. B. eine kritische Anwendung, die auf eine bestimmte Berechtigung angewiesen ist.

Daher ist es wichtig, die Verwaltung mit der **Überwachung von Angriffspfaden** zu kombinieren. So können Sie kontinuierlich beobachten, ob Angriffspfade, die Sie noch nicht entschärft haben, genutzt werden, sodass Sie umgehend reagieren können. Quest Change Auditor und On Demand Audit ergänzen BloodHound Enterprise durch:

- Überwachung von Active Directory in Echtzeit auf aktive Angriffe und Kompromittierungsindikatoren (Indicators of Compromise, IOCs)
- Hinderung von Angreifern daran, Angriffspfade zu nutzen, indem Änderungen an und der Zugriff auf kritische Assets verhindert werden, z. B. indem sie sich selbst zu Domänenadministratoren machen oder sich zu anderen privilegierten Gruppen hinzufügen
- Auditierung von Sicherheitsänderungen in Ihren AD- und Azure AD-Umgebungen

Es ist von entscheidender Bedeutung, dass Sie alle Angriffspfade, die Sie noch nicht entschärfen konnten, kontinuierlich überwachen.

Mehr als Cybersicherheit: Cyber Resilience

Die Verwaltung und Überwachung von Angriffspfaden kann die Cybersicherheit erheblich verbessern. Aber Unternehmen brauchen heute **Cyber Resilience**. Das heißt, sie müssen sowohl Cyberrisiken minimieren als auch sicherstellen, dass sie auch im Katastrophenfall schnell wieder einsatzbereit sind. Diese Quest-Lösungen können helfen:

GPOADmin

Gruppenrichtlinien (GPOs) verdienen besondere Aufmerksamkeit, da sie Einstellungen in der gesamten Domäne steuern können und daher ein wichtiger Angriffsvektor sind. GPOADmin® optimiert die Verwaltung und Sicherheit von GPOs, indem es Ihnen hilft:

- sicherzustellen, dass vorgeschlagene Änderungen an GPOs Ihren Sicherheitsrichtlinien entsprechen, bevor sie bereitgestellt werden
- GPOs durch automatische Attestierung kontinuierlich zu validieren
- nicht genehmigte GPO-Änderungen schnell auf eine genehmigte Konfiguration zurückzusetzen

Recovery Manager Disaster Recovery Edition und On Demand Recovery

Recovery Manager for Active Directory und On Demand Recovery bieten einen Mehrwert in mehreren Bereichen. Erstens erleichtern sie die Behebung von Choke-Point-Problemen, denn wenn eine Änderung der Konfiguration oder der Berechtigungen zu Problemen führt, kann das IT-Team diese sofort rückgängig machen und zu einem bekannten guten Zustand zurückkehren.

Ganz allgemein ermöglichen es Ihnen diese Lösungen, Ihr Unternehmen im Falle eines erfolgreichen Angriffs oder einer anderen Art von Katastrophe so schnell wie möglich wieder zum Laufen zu bringen. Sie können:

- Änderungen an AD und Azure AD sofort rückgängig machen, wenn Bereinigungsmaßnahmen unbeabsichtigte Folgen haben
- nicht genehmigte oder anderweitig unerwünschte Änderungen an beliebigen Objekten, einschließlich Benutzern, GPOs und AD-Konfiguration, rückgängig machen
- AD-Domänen oder einen gesamten AD-Forest nach einem Angriff schnell wiederherstellen

Konzentrieren Sie sich auf die Cyber Resilience: Stellen Sie sicher, dass Sie Ihr Unternehmen im Falle eines erfolgreichen Angriffs oder einer Katastrophe schnell wieder zum Laufen bringen können.

Fazit

Microsoft berichtet, dass jeden Tag 95 Millionen Active Directory-Benutzerkonten angegriffen werden. Jetzt wissen Sie auch, warum: Wenn ein Angreifer ein normales Benutzerkonto kompromittiert, ist er wahrscheinlich in der Lage, einen Angriffspfad zu nutzen, der ihn in nur wenigen Schritten zu Ihren Tier-0-Assets führt. Die Open-Source-Version von BloodHound wird ihm diesen Weg schnell aufzeigen. Glücklicherweise haben IT-Teams jetzt eine Lösung, die eine praktische Möglichkeit bietet, Hunderte oder sogar Tausende von Angriffspfaden auf einmal zu unterbrechen. SpecterOps BloodHound Enterprise kartiert die Angriffspfade in Ihrem AD, priorisiert sie nach dem Risiko und bietet klare Anleitungen zur Bereinigung.

Für eine robuste Strategie, die nicht nur Cybersicherheit, sondern auch Cyber Resilience bietet, sollten Sie BloodHound Enterprise mit folgenden Komponenten ergänzen: Quest Change Auditor und On Demand Audit für eine effektive Überwachung von Angriffspfaden, GPOADmin für eine optimierte Verwaltung und Sicherheit von Gruppenrichtlinien sowie Recovery Manager for Active Directory und On Demand Recovery für eine schnelle und zuverlässige Sicherung und Wiederherstellung.

Vereinbaren Sie einen Termin für unsere kostenlose Active Directory-Sicherheitsbewertung, bei der wir Ihr aktuelles Sicherheitsniveau sowie potenzielle Angriffspfade auf Ihre wichtigsten Assets überprüfen.

Über Quest

Quest stellt Softwarelösungen bereit, mit denen das Potenzial neuer Technologien in einer zunehmend komplexen IT-Landschaft voll ausgeschöpft werden kann. Von der Datenbank- und Systemverwaltung über die Migration zu und Verwaltung von Active Directory und Microsoft 365 bis hin zur Cyber Resilience: Quest hilft Kunden, bereits heute ihre IT-Herausforderungen von morgen zu bewältigen. Weltweit vertrauen mehr als 130.000 Unternehmen und 95 % der Fortune 500 Quest die proaktive Verwaltung und Überwachung der nächsten Unternehmensinitiative an. Quest soll außerdem die nächste Lösung für komplexe Microsoft-Herausforderungen finden, um für die nächste Bedrohung gewappnet zu sein. Quest Software. Where Next Meets Now. Weitere Informationen finden Sie auf www.quest.com.

Sollten Sie Fragen hinsichtlich der potenziellen Nutzung des Materials haben, wenden Sie sich bitte an: www.quest.com/de-de/company/contact-us.aspx