Verwalten von GPOs mit einem mehrschichtigen Sicherheits-Framework

Von Alvaro Vitta, Principal Solutions Consultant, Quest

Einführung

Eine Gruppenrichtlinie ermöglicht die zentralisierte Verwaltung und Konfiguration von Betriebssystemen, Anwendungen und Benutzereinstellungen in einer Microsoft Active Directory-Umgebung. Die Gruppenrichtlinie steuert mit, was für Benutzer welche Aktionen auf einem Computersystem durchführen dürfen. Sie setzt ein System für die Komplexität von Kennwörtern durch, das verhindert, dass Benutzer allzu simple Kennwörter wählen können, erlaubt oder verbietet nicht identifizierten Benutzern von Remote-Computern aus eine Verbindung zu einer Netzwerkfreigabe herzustellen und schränkt den Zugriff auf bestimmte Ordner ein. Ein einzelner Satz solcher Konfigurationen wird als Gruppenrichtlinienobjekt (Group Policy Object, GPO) bezeichnet.

GPOs sind eigentlich dafür gedacht, um IT-Vorgänge zu vereinfachen und als zentralisierte Sicherheitsrichtlinien über die gesamte Active Directory-Umgebung hinweg zu dienen. Allerdings können sie wie jedes andere leistungsfähige System auch missbräuchlich genutzt oder speziell dafür eingespeist werden, um Sicherheitskontrollen zu umgehen und Zugriff auf vertrauliche Daten zu erhalten. In manchen mittleren und größeren Organisationen werden hunderte oder sogar tausende GPOs in weit verteilten Umgebungen eingesetzt, wodurch sie nicht nur eine riesige Insider-Bedrohung bilden sondern auch eine große Angriffsfläche bieten, wenn keine geeigneten Sicherheitskontrollen vorhanden sind.

In diesem Whitepaper wird beschrieben, wie GPOs missbräuchlich verwendet oder ausgenutzt werden können, wenn keine geeigneten Sicherheitskontrollen vorhanden sind. Außerdem wird erklärt, wie eine mehrschichtige Sicherheitsarchitektur implementiert werden kann, die es Ihnen ermöglicht, unbefugte Zugriffe auf GPOs zu erkennen, zu melden und zu verhindern.

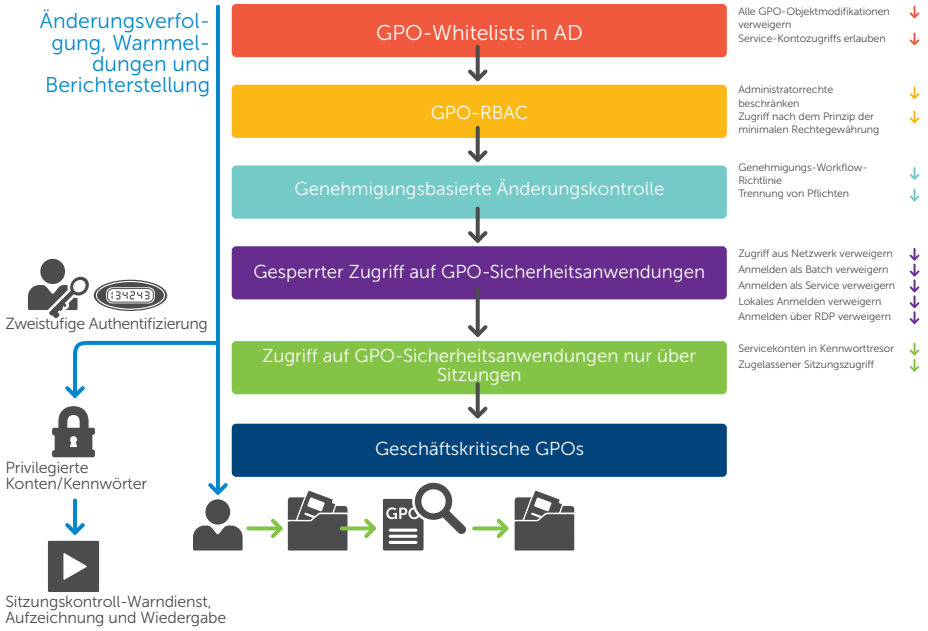

Abb. 1. Mehrschichtiges Sicherheits-Framework mit GPOs

Bei 55 % der Sicherheitsvorfälle sind interne Akteure involviert, die ihre Zugriffsberechtigungen missbrauchen.[1]

Ausnutzung von GPO-Berechtigungen

Sam Smith, ein neuer IT-Administrator bei einem Fertigungsunternehmen, muss auf einem Windows-basierten Datenbankserver, auf dem sich eine wichtige SQL-Datenbank mit vertraulichen Kundendaten befindet, einen Patch installieren. Sam ist ein Domänenadministrator und kann sich aufgrund eines vorhandenen GPOs (**Lokal anmelden verweigern**) bei diesem SQL-Server nicht anmelden. Dieses GPO dient speziell dazu, zu verhindern, dass sich Domänenadministratoren bei diesem SQL-Server, auf dem sich die persönlichen Daten von Kunden befinden, anmelden können. Sam könnte nun eine Genehmigung für die Installation des Patches einholen und diesen Vorgang dann während des Zeitfensters durchführen, der für das Änderungsmanagement am Samstag vorgesehen ist. Stattdessen beschließt Sam jedoch, lieber die GPO-Einstellung **Lokal anmelden verweigern** so zu ändern, dass er Zugriff auf den Server erhält. Dazu deaktiviert er das GPO, das verhindert, dass sich Administratoren anmelden können, und meldet sich dann an, um den Patch zu installieren. Während er Zugriff auf den Server hat, wird er neugierig und stöbert etwas in den vertraulichen Kundendaten herum. Er kopiert sogar einige dieser Informationen in einen separaten Ordner!

Zum Schluss stellt er die ursprüngliche GPO-Einstellung wieder her. Und da Änderungen an GPO-Einstellungen nicht in systemeigenen Sicherheitsprotokollen nachverfolgt werden, wird der unbefugte Zugriff erst sechs Wochen später im Rahmen eines Datenbank-Audits bemerkt.

Wie kann solch ein Sicherheitsvorfall möglich sein?

Leider kommen ähnliche Szenarien öfter vor, als man denkt – manchmal aus Bequemlichkeit, manchmal jedoch auch mit böser Absicht. Aufgrund der Art und Weise, in der Sicherheitsberechtigungen bei GPOs angeordnet sind, kann eine GPO-Sicherheitseinstellung von jedem beliebigen Domänenadministrator geändert werden – sogar die Einstellungen, die eigentlich verhindern sollen, dass jemand eine bestimmte Aufgabe durchführt. Außerdem können GPO-Änderungen auch nicht überwacht werden, während sie gerade erfolgen – nicht einmal mithilfe von SIEM-Lösungen (Security Information and Event Management, Verwaltung von Sicherheitsinformationen und -ereignissen) – da GPO-Änderungen nicht im systemeigenen Sicherheitsprotokoll nachverfolgt werden. Und es lässt sich auch nicht verhindern, dass so etwas zukünftig wieder passiert, da sich nicht genau bestimmen lässt, welche GPO-Einstellung eigentlich geändert wurde

(d. h. keine Vorher-/Nachher-Werte). So steht es Domänenadministratoren jederzeit frei, lästige GPO-Einstellungen einfach zu ändern.

Mehrschichtiges Sicherheits-Framework

Eine Möglichkeit, solche Sicherheitsverletzungen (und viele andere) zu verhindern, bietet die Wahl eines mehrschichtigen Sicherheitsansatzes. Dazu ist eine in sich geschlossene Zusammenstellung von Sicherheitskontrollen erforderlich, die es Administratoren erlaubt, Änderungen an GPO-Einstellungen vorzunehmen, und gleichzeitig unbefugte Änderungen unterbindet – ganz egal, von wem diese versucht werden (selbst von Domänenadministratoren).

Die folgenden Sicherheitsschichten stellen gemeinsam sicher, dass die passenden Sicherheitsausgleichskontrollen für die Verwaltung von Zugriffen auf geschäftskritische GPO-Einstellungen vorhanden sind:

- GPO-Whitelists in Active Directory
- Auf GPO-Rollen basierende Zugriffssteuerung (Role-Based Access Control, RBAC)
- Genehmigungsbasierte Änderungskontrolle
- Gesperrter Zugriff auf GPO-Sicherheitsanwendungen
- Zugriff auf GPO-Sicherheitsanwendungen nur über Sitzungen

GPO-Whitelists in Active Directory

Alle wichtigen GPOs – wie domänenweite GPOs, Domänencontroller-GPOs, GPOs für geschäftskritische Anwendungen usw. – werden der Schutzliste einer von einem Drittanbieter stammenden Sicherheitsanwendung hinzugefügt, die über Whitelist-Funktionalität für GPO-Berechtigungen verfügt (z. B. Change Auditor for Active Directory). Diese Sicherheitslösung für Windows stellt Funktionen bereit, mit denen Berechtigungen in Whitelists in Echtzeit überprüft und unbefugte Zugriffsversuche auf GPO-Einstellungen überwacht werden können.

Änderungen an Ihren wichtigsten GPOs können dann nur noch über ein spezielles "GPO-Dienstkonto" vorgenommen werden, das von einer Drittanbieter-Sicherheitslösung (Proxy) für GPOs (z. B. GPOAdmin) verwendet wird und Änderungen an Ihren wichtigsten GPOs vornehmen darf. Allen anderen Konten (inklusive den Domänenadministratoren) wird der Bearbeitungszugriff auf GPOs automatisch verweigert. Autorisierte Änderungen können nur noch über die Benutzeroberfläche von GPOAdmin erfolgen, die über ein Zugriffsmodell nach dem Prinzip der minimalen Rechte ("Least-Privilege-Prinzip") und geeignete Steuerelemente für die Regelung von GPO-Änderungen verfügt. Durch die Verwendung einer Sicherheitslösung mit GPO-Whitelist-Funktionalität werden die Risiken beseitigt, die mit ständigen unbefugten Änderungen verbunden sind.

GPO-RBAC

Obwohl systemeigene GPO-Berechtigungen eigentlich dazu dienen, Berechtigungen an GPOs zu delegieren, können diese Berechtigungen manchmal einen Interessenkonflikt verursachen. So kann zum Beispiel ein Mitglied der Administratorgruppe ganz nach seinem Belieben Änderungen an GPO-Einstellungen vornehmen, die eigentlich genau das verhindern sollen. Aus genau diesem Grund empfiehlt sich die Implementierung eines rollenbasierten Zugriffssteuerungsmodells, damit GPO-Berechtigungen aus dem Active Directory ausgelagert und von einer GPO-Sicherheitslösung (Proxy) kontrolliert werden, die von einem Drittanbieter stammt (z. B. GPOAdmin). GPOAdmin ist eine Lösung, die GPOs über ihren ganzen Lebenszyklus hinweg regelt. GPOAdmin verfügt über ein Modell nach dem Prinzip der minimalen Rechte ("Least-Privilege-Prinzip"). So können Sie die Anzahl der Administratoren reduzieren, die allzu großzügige Zugriffsberechtigungen für GPO-Einstellungen besitzen.

Genehmigungsbasierte Änderungskontrollen

Nach der Einrichtung von GPO-Whitelist-Funktionalität und einem GPO-RBAC-Modell müssen Sie einen automatisierten Prozess einrichten, der die Trennung von Pflichten durch den Einsatz von Genehmigungs-Workflows erlaubt. So wird verhindert, dass derjenige, der eine GPO-Einstellung bearbeitet, nicht mit demjenigen identisch ist, der die Übernahme dieser Änderung in die Produktionsumgebung genehmigt. Das mag offensichtlich klingen, ist aber ein Punkt, der sorgfältig geklärt und implementiert werden muss.

> 69 % der berechtigten Benutzer sagen, dass Sicherheitstools nicht genügend Informationen zu Vorfällen bereitstellen.[2]

Mithilfe einer mehrschichtigen Sicherheitsarchitektur können unbefugte Zugriffe auf GPOs erkannt, gemeldet und verhindert werden.

Sperren des Zugriffs auf GPO-Sicherheitsanwendungen

Wenn Sie GPO-Sicherheitsanwendungen von Drittanbietern einsetzen (z. B. Change Auditor for Active Directory oder GPOAdmin), um Änderungen an GPOs zu steuern, dann müssen Sie diese Anwendungen auch als geschäftskritisch betrachten. Daher müssen Sie diese Sicherheitsanwendungen vor unbefugten Zugriffen schützen. Um diese Sicherheitsschicht zu implementieren, müssen Sie Ihrer Whitelist einfach eine GPO-Sicherheitsrichtlinie hinzufügen und diese dann auf die Server anwenden, die als Host für Ihre Sicherheitsanwendungen dienen. Verwenden Sie dabei die folgenden Einstellungen:

"Deny logon as a batch" (Anmelden als Batch verweigern), "Deny access from network" (Zugriff aus Netzwerk verweigern), "Deny logon as service" (Anmelden als Dienst verweigern), "Deny logon locally" (Lokales Anmelden verweigern) und "Deny logon via RDP" (Anmelden über RDP verweigern)

Zugriff auf GPO-Sicherheitsanwendungen nur über Sitzungen

Um Ihren Serveradministratoren einen sicheren Zugriff für ihre regelmäßigen Wartungsarbeiten an den GPO-Sicherheitsanwendungen einzurichten, müssen Sie einen kontrollierten Zugriff bereitstellen. Dieser erfolgt über eine verschlüsselte Remotedesktopverbindung von einem "Jump-Server (z. B. TPAM, The Privileged Appliance and Modules) aus. Außerdem ist als Frontend auch ein System für zweistufige Authentifizierung möglich (z. B. Quest Defender), um die Sicherheit noch weiter zu erhöhen. Nach Genehmigung der zeitbasierten Sitzung durch einen zuständigen Genehmiger kann ein autorisierter Mitarbeiter dann eine Verbindung von dem speziell geschützten Jump-Server zu dem Server herstellen, auf dem sich die von einem Drittanbieter stammende GPO-Sicherheitsanwendung befindet, um die jeweilige Wartungsaufgabe durchzuführen. Alle Vorgänge in der Sitzung werden aufgezeichnet und können bei Bedarf nachvollzogen werden, um in Erfahrung zu bringen, was genau auf dem Server durchgeführt wurde.

Fazit

GPO-Sicherheitsvorfälle können, ob versehentlich oder böswillig, in jeder Organisation vorkommen. Angesichts der Tatsache, dass die integrierten Sicherheitsprotokolle nicht genügend Informationen bereitstellen und die systemeigenen Berechtigungen zu unflexibel sind, benötigen Sie ein mehrschichtiges Sicherheits-Framework, das auf GPO-Sicherheitslösungen von Drittanbietern zurückgreift, um GPO-Sicherheitsvorfälle zu erkennen, zu melden und zu verhindern. Dann sind die wertvollen Daten Ihrer Organisation nicht in Gefahr.

Informationen zum Autor

Alvaro Vitta ist einer der führenden Lösungsberater in puncto Sicherheit bei der Quest. Vitta befasst sich seit 15 Jahren mit der Bewertung, dem Entwurf, dem Testen und der Bereitstellung von Sicherheitslösungen in Großunternehmen für lokale und cloudbasierte Plattformen im privaten und öffentlichen Sektor in den Bereichen Identitäts- und Zugriffsmanagement, Active Directory und Governance, Risiko und Compliance in globalen Unternehmen. Vitta verfügt über verschiedene Branchenzertifizierungen, darunter CISSP, CISSO, MCSE und ITIL.

[1] *"2015 Data Breach Investigations Report" (Untersuchungsbericht zu unbefugten Datenzugriffen), Verizon, April 2015, http://www.verizonenterprise.com/DBIR/2015*

[2] *"Privileged User Abuse and the Inside Threat" (Missbräuchliche Verwendung durch privilegierte Benutzer und die Bedrohung durch Insider), Raytheon Company, Mai 2014, http://www.raytheoncyber.com/rtnwcm/groups/cyber/documents/content/rtn_257010.pdf.*

ÜBER QUEST

Quest hilft Kunden dabei, aufwendige Verwaltungsaufgaben zu reduzieren, damit sie sich auf die für Unternehmenswachstum erforderlichen Innovationen konzentrieren können. Die skalierbaren, erschwinglichen und benutzerfreundlichen Lösungen von Quest® ermöglichen eine beispiellose Effizienz und Produktivität. Quest lädt Benutzer dazu ein, Teil einer innovativen globalen Gemeinschaft zu werden, und unternimmt alle Anstrengungen, den Anforderungen seiner Kunden gerecht zu werden. Daher wird das Unternehmen auch weiterhin die Bereitstellung der umfassendsten Lösungen für Azure Cloud-Management, SaaS, Sicherheit, mobile Mitarbeiter und datenbasierte Einblicke vorantreiben.

Sollten Sie Fragen hinsichtlich der potenziellen Nutzung des Materials haben, wenden Sie sich bitte an:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Informationen zu unseren regionalen oder internationalen Büros finden Sie auf unserer Website (www.quest.com).