Vor- und Nachteile von Einschränkungen des Systemzugriffs

Inhalt

Einführung

Dieses Dokument beschreibt ein Problem, das bei der Einschränkung des Computerzugriffs (MAR) aufgetreten ist, und bietet eine Lösung für das Problem.

Angesichts der zunehmenden Anzahl privater Geräte ist es für Systemadministratoren wichtiger, den Zugriff auf bestimmte Teile des Netzwerks auf Unternehmensressourcen zu beschränken. Das in diesem Dokument beschriebene Problem betrifft die sichere Identifizierung dieser Problembereiche und deren Authentifizierung ohne Beeinträchtigung der Benutzerkonnektivität.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über 802.1x-Kenntnisse verfügen, um dieses Dokument vollständig verstehen zu können. In diesem Dokument wird davon ausgegangen, dass Benutzer mit der 802.1x-Authentifizierung vertraut sind. Außerdem werden die Probleme und Vorteile im Zusammenhang mit der Verwendung von MAR und generell der maschinellen Authentifizierung hervorgehoben.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie

die potenziellen Auswirkungen eines Befehls verstehen.

Problem

MAR versucht im Wesentlichen, ein gängiges Problem zu lösen, das bei den meisten der aktuellen und gängigen Extensible Authentication Protocol (EAP)-Methoden auftritt, nämlich dass die maschinelle Authentifizierung und die Benutzerauthentifizierung separate, voneinander unabhängige Prozesse sind.

Die Benutzerauthentifizierung ist eine 802.1x-Authentifizierungsmethode, die den meisten Systemadministratoren vertraut ist. Die Idee ist, dass jedem Benutzer Anmeldeinformationen (Benutzername/Passwort) gegeben werden und dass der Berechtigungssatz eine physische Person darstellt (er kann auch von mehreren Personen gemeinsam genutzt werden). Aus diesem Grund kann sich ein Benutzer von einem beliebigen Ort im Netzwerk mit diesen Anmeldeinformationen anmelden.

Eine Computerauthentifizierung ist technisch identisch, aber der Benutzer wird in der Regel nicht aufgefordert, die Anmeldeinformationen (oder das Zertifikat) einzugeben. der Computer oder die Maschine dies alleine tut. Dies erfordert, dass auf dem Computer bereits Anmeldeinformationen gespeichert sind. Der gesendete Benutzername lautet **host/<MyPCHostname>**, sofern auf Ihrem Computer **<MyPCHostname>** als Hostname festgelegt ist. Mit anderen Worten, es sendet **Host/**gefolgt von Ihrem Hostnamen.

Dieser Prozess ist zwar nicht direkt mit Microsoft Windows und Cisco Active Directory verknüpft, aber er wird einfacher wiedergegeben, wenn der Computer dem Active Directory hinzugefügt wird, da der Computer-Hostname der Domänendatenbank hinzugefügt wird und Anmeldeinformationen verhandelt (standardmäßig alle 30 Tage erneuert) und auf dem Computer gespeichert werden. Dies bedeutet, dass die Authentifizierung von Geräten von jedem Gerätetyp aus möglich ist. Sie wird jedoch wesentlich einfacher und transparenter wiedergegeben, wenn der Computer mit Active Directory verbunden ist, und die Anmeldeinformationen bleiben dem Benutzer verborgen.

MAR als Lösung

Es lässt sich leicht sagen, dass die Lösung für das Cisco Access Control System (ACS) bzw. die Cisco Identity Services Engine (ISE) zum Abschließen der MAR geeignet ist. Vor der Implementierung dieser Lösung müssen jedoch Vor- und Nachteile beachtet werden. Wie dies implementiert wird, wird am besten in den ACS- oder ISE-Benutzerhandbüchern beschrieben. In diesem Dokument wird daher lediglich beschrieben, ob und welche Hindernisse zu berücksichtigen sind.

Vorteile

MAR wurde erfunden, weil Benutzer- und Computerauthentifizierungen völlig getrennt sind. Aus diesem Grund kann der RADIUS-Server keine Überprüfung durchsetzen, bei der sich Benutzer von unternehmenseigenen Geräten anmelden müssen. Mit MAR erzwingt der RADIUS-Server (ACS oder ISE auf der Cisco-Seite) für eine bestimmte Benutzerauthentifizierung, dass innerhalb der X Stunden (in der Regel 8 Stunden, dies ist jedoch konfigurierbar) vor der Benutzerauthentifizierung für denselben Endpunkt eine gültige Maschinenauthentifizierung vorhanden sein muss.

Aus diesem Grund kann eine Computerauthentifizierung erfolgreich durchgeführt werden, wenn

der RADIUS-Server die Anmeldeinformationen des Computers kennt, in der Regel, wenn der Computer der Domäne beigetreten ist. Der RADIUS-Server überprüft dies anhand einer Verbindung zur Domäne. Es liegt in der alleinigen Sache des Netzwerkadministrators zu bestimmen, ob eine erfolgreiche Computerauthentifizierung vollständigen Zugriff auf das Netzwerk oder nur eingeschränkten Zugriff bietet. Dies öffnet in der Regel zumindest die Verbindung zwischen dem Client und dem Active Directory, sodass der Client Aktionen wie die Verlängerung des Benutzerkennworts oder das Herunterladen von Group Policy Objects (GPOs) durchführen kann.

Wenn eine Benutzerauthentifizierung von einem Gerät stammt, auf dem in den letzten Stunden keine Computerauthentifizierung stattgefunden hat, wird dem Benutzer der Zugriff verweigert, selbst wenn der Benutzer normalerweise gültig ist.

Der uneingeschränkte Zugriff wird nur dann gewährt, wenn die Authentifizierung gültig ist und von einem Endpunkt aus abgeschlossen ist, auf dem in den letzten Stunden eine Computerauthentifizierung stattgefunden hat.

Nachteile

In diesem Abschnitt werden die Nachteile der MAR-Verwendung beschrieben.

MAR und Microsoft Windows Supplicant

Die Idee hinter MAR ist, dass für eine Benutzerauthentifizierung nicht nur ein Benutzer mit gültigen Anmeldeinformationen, sondern auch eine erfolgreiche Computerauthentifizierung von diesem Client protokolliert werden muss. Sollte dies ein Problem darstellen, kann der Benutzer sich nicht authentifizieren. Das Problem besteht darin, dass diese Funktion manchmal versehentlich einen legitimen Client sperren kann, wodurch der Client zum Neustart gezwungen wird, um wieder Zugriff auf das Netzwerk zu erhalten.

Microsoft Windows führt eine Computerauthentifizierung nur beim Booten durch (wenn der Anmeldebildschirm angezeigt wird). Sobald der Benutzer die Benutzeranmeldeinformationen eingegeben hat, wird eine Benutzerauthentifizierung durchgeführt. Wenn sich der Benutzer abmeldet (kehrt zum Anmeldebildschirm zurück), wird auch eine neue Computerauthentifizierung durchgeführt.

Im folgenden Beispielszenario wird veranschaulicht, warum MAR manchmal Probleme verursacht:

Benutzer X arbeitete den ganzen Tag auf seinem Laptop, der über eine Wireless-Verbindung verbunden war. Am Ende des Tages schließt er einfach den Laptop und verlässt die Arbeit. Dadurch wird der Laptop in den Ruhemodus versetzt. Am nächsten Tag kommt er wieder ins Büro und öffnet seinen Laptop. Jetzt kann er keine Wireless-Verbindung herstellen.

Wenn Microsoft Windows in den Ruhezustand wechselt, wird ein Snapshot des Systems in seinem aktuellen Zustand erstellt, der den Kontext der angemeldeten Benutzer enthält. Über Nacht läuft der MAR-Cache-Eintrag für den Benutzer-Laptop ab und wird gelöscht. Wenn der Laptop eingeschaltet ist, führt er jedoch keine Authentifizierung durch. Stattdessen geht es direkt in eine Benutzerauthentifizierung, da das die Ruhephase aufgezeichnet hat. Die einzige Möglichkeit, dies zu beheben, besteht darin, den Benutzer abzumelden oder seinen Computer neu zu starten.

MAR ist zwar eine gute Funktion, kann jedoch zu Netzwerkstörungen führen. Diese

Unterbrechungen lassen sich nur schwer beheben, wenn Sie die Funktionsweise von MAR verstehen. Wenn Sie MAR implementieren, ist es wichtig, die Endbenutzer darüber aufzuklären, wie sie Computer ordnungsgemäß herunterfahren und sich am Ende jedes Tages von jedem Rechner abmelden können.

MAR und verschiedene RADIUS-Server

Häufig werden im Netzwerk mehrere RADIUS-Server für Lastenausgleich und Redundanz eingesetzt. Allerdings unterstützen nicht alle RADIUS-Server einen gemeinsamen MAR-Sitzungscache. Nur die ACS-Versionen 5.4 und höher und die ISE-Version 2.3 und höher unterstützen die Synchronisierung des MAR-Cache zwischen den Knoten. Vor diesen Versionen ist es nicht möglich, eine Computerauthentifizierung für einen ACS/ISE-Server durchzuführen und eine Benutzerauthentifizierung für einen anderen Server durchzuführen, da diese nicht miteinander übereinstimmen.

MAR- und kabelgebundene/Wireless-Switching

Der MAR-Cache vieler RADIUS-Server basiert auf der MAC-Adresse. Es handelt sich einfach um eine Tabelle mit der MAC-Adresse der Laptops und dem Zeitstempel der letzten erfolgreichen Computerauthentifizierung. Auf diese Weise kann der Server wissen, ob der Client in den letzten X Stunden maschinell authentifiziert wurde.

Was passiert jedoch, wenn Sie Ihren Laptop mit einer kabelgebundenen Verbindung booten (und daher eine Computerauthentifizierung von Ihrer kabelgebundenen MAC-Adresse aus durchführen) und dann tagsüber auf das Wireless-Netzwerk umschalten? Der RADIUS-Server hat keine Möglichkeit, Ihre Wireless-MAC-Adresse mit Ihrer kabelgebundenen MAC-Adresse zu korrelieren und zu wissen, dass Sie in den letzten X Stunden automatisch authentifiziert wurden. Die einzige Möglichkeit besteht darin, sich abzumelden und Microsoft Windows dazu zu veranlassen, eine andere Authentifizierung über Wireless durchzuführen.

Lösung

Cisco AnyConnect bietet unter anderem die Möglichkeit, vorkonfigurierte Profile zu erstellen, die eine Computer- und Benutzerauthentifizierung auslösen. Es bestehen jedoch dieselben Einschränkungen wie bei Microsoft Windows Supplicant, was die Authentifizierung des Computers betrifft, die nur beim Abmelden oder Neustart auftritt.

Mit AnyConnect Version 3.1 und höher ist es außerdem möglich, EAP-FAST mit EAP-Verkettung auszuführen. Hierbei handelt es sich im Grunde um eine einzige Authentifizierung, bei der Sie gleichzeitig zwei Paare von Anmeldeinformationen senden, den Benutzernamen/das Kennwort des Computers und den Benutzernamen/das Kennwort des Benutzers. Die ISE kann daher leichter überprüfen, ob beide Lösungen erfolgreich sind. Da kein Cache verwendet wird und keine vorherige Sitzung abgerufen werden muss, ist dies zuverlässiger.

Wenn der PC bootet, sendet AnyConnect nur eine Computerauthentifizierung, da keine Benutzerinformationen verfügbar sind. Bei der Anmeldung beim Benutzer sendet AnyConnect jedoch sowohl die Computer- als auch die Benutzeranmeldeinformationen gleichzeitig. Wenn Sie das Kabel abziehen oder trennen/entfernen, werden die Anmeldeinformationen für den Computer und den Benutzer erneut in einer einzigen EAP-FAST-Authentifizierung gesendet, die sich von den früheren Versionen von AnyConnect ohne EAP-Verkettung unterscheidet.

EAP-TEAP ist die langfristig beste Lösung, da es speziell zur Unterstützung dieser Authentifizierungstypen entwickelt wurde. EAP-TEAP wird jedoch von vielen Betriebssystemen bis heute nicht in der nativen Komponente unterstützt