Überprüfung der Funktion zur Umgehung des Verhaltens für sicheren Zugriff auf Microsoft 365-Kompatibilität

Inhalt

Problem

Bei der Konfiguration von Cisco Secure Access mit aktivierter Microsoft 365-Kompatibilitätsfunktion besteht Unsicherheit, ob bestimmte Microsoft-bezogene vollqualifizierte Domänennamen (FQDNs) automatisch von der SWG-Verarbeitung (Secure Web Gateway) und der TLS-Entschlüsselung umgangen werden. Insbesondere muss das Bypass-Verhalten für diese Domänen geklärt werden:

- do.dsp.mp.microsoft.com
- dl.delivery.mp.microsoft.com
- manage.microsoft.com

Die Hauptsorge gilt der Frage, ob diese Domänen manuell in die Liste "Nicht entschlüsseln" aufgenommen werden müssen oder ob sie automatisch ausgeschlossen werden, wenn die Microsoft 365-Kompatibilität aktiviert ist. Darüber hinaus besteht Verwirrung hinsichtlich der Interaktion zwischen den SWG-Level-Bypasses und den IPS-Level-Entschlüsselungseinstellungen, insbesondere für manage.microsoft.com, die in der Dokumentation aufgeführt ist, dass die manuelle Konfiguration der Do Not Decrypt List weiterhin erforderlich sein kann.

Umwelt

- Sicherer Zugriff von Cisco
- Microsoft 365-Kompatibilitätsfunktion aktiviert
- Konfiguration von SWG-Inspektion (Secure Web Gateway) und TLS-Entschlüsselung
- Verwendete IPS-Entschlüsselungsrichtlinien

- Microsoft Management- und Update-Services, die Konnektivität erfordern

Auflösung

Das Verhalten der Microsoft 365-Kompatibilitätsfunktion wurde durch Labortests mit folgenden Ergebnissen verifiziert:

Funktionsumfang der Microsoft 365-Kompatibilität

Die Microsoft 365-Kompatibilitätsfunktion befreit Microsoft 365-bezogene Domänen, die in den Endpunktkategorien von Microsoft als "Optimieren" und "Zulassen" gekennzeichnet sind, von der SWG-Überprüfung und Richtliniendurchsetzung. Auf diese Weise wird der Datenverkehr zu diesen Domänen unverändert auf SWG-Ebene weitergeleitet.

Ergebnisse der Labortests

Die Tests wurden in einer kontrollierten Laborumgebung mit aktivierter Microsoft 365-Kompatibilität durchgeführt. Dieses Verhalten wurde für die angegebenen FQDNs beobachtet:

Schritt 1: Kompatibilitätsfunktion für Microsoft 365 aktivieren

Die Microsoft 365-Kompatibilitätsfunktion wurde in der Konfiguration für sicheren Zugriff aktiviert.

Phase 2: Testen des Datenverkehrs zu Ziel-FQDNs

Der Web-Datenverkehr zu jedem der drei FQDNs wurde über einen Standard-Internetbrowser generiert:

- do.dsp.mp.microsoft.com
- dl.delivery.mp.microsoft.com
- manage.microsoft.com

Schritt 3: Überprüfen des Umgehungsverhaltens im Dashboard

Die Analyse des Dashboards für sicheren Zugriff bestätigte, dass bei Aktivierung der Microsoft 365-Kompatibilitätsfunktion für den Datenverkehr zu diesen Zielen keine Prüfung und Entschlüsselung des Webdatenverkehrs stattfand.

Schritt 4: DNS-Steuerungsverhalten bestätigen

Der DNS-Datenverkehr zu diesen Zielen wurde weiterhin über Secure Access gesteuert. Dieses Verhalten wird dokumentiert, es sei denn, eine spezifische DNS-Ausnahme wurde konfiguriert.

Wichtigste verhaltensbasierte Ergebnisse

Basierend auf Testergebnissen und Dokumentationsanalyse:

- SWG-Umgehung: Die drei angegebenen FQDNs werden von der Web-Datenverkehrsanalyse umgangen, wenn die Microsoft 365-Kompatibilität aktiviert ist.
- TLS-Entschlüsselung: Die Entschlüsselung wird auf der SWG-Ebene für diese Domänen umgangen.
- DNS-Steuerung: DNS-Abfragen werden weiterhin über Secure Access verarbeitet, es sei denn, sie sind ausdrücklich ausgenommen.
- Domänenabdeckung: Während "*.microsoft.com" als gesamte Domain nicht vollständig durch Spezifikation umgangen wird, werden die spezifischen getesteten URLs in der Praxis umgangen.

Überlegungen zum IPS-Layer

Die Microsoft 365-Kompatibilitätsfunktion wird auf der SWG-Ebene ausgeführt. Für die Umgehung der Entschlüsselung auf IPS-Ebene kann weiterhin eine manuelle Konfiguration erforderlich sein:

- Wenn auch für diese Domänen eine Umgehung der IPS-Entschlüsselung gewünscht wird, kann eine manuelle Ergänzung der Liste "Nicht entschlüsseln" erforderlich sein.
- Die Liste "Nicht entschlüsseln" wirkt sich primär auf die IPS-seitige Entschlüsselung aus, nicht auf die SWG-Verarbeitung.

- Dies erklärt, warum in der Dokumentation auch dann auf das Hinzufügen von manage.microsoft.com zur Liste "Nicht entschlüsseln" verwiesen werden kann, wenn die Microsoft 365-Kompatibilität aktiviert ist.

Ursache

Die Verwirrung rührt von der Layer-Architektur von Cisco Secure Access her, bei der die Kompatibilität mit Microsoft 365 die Verarbeitung auf SWG-Ebene beeinflusst, während die IPS-Entschlüsselung als separate Ebene mit eigenen Konfigurationsanforderungen funktioniert. Die Microsoft 365-Kompatibilitätsfunktion übernimmt automatisch die SWG-Umgehung für qualifizierte Microsoft-Domänen. IPS-Entschlüsselungsrichtlinien können jedoch eine separate Konfiguration über die Liste "Nicht entschlüsseln" erfordern.

Verwandte Inhalte

- Cisco Secure Access Kompatibilitätsdokumentation zu Microsoft 365
- Erstellung einer effektiven Liste "Nicht entschlüsseln" für Cisco Secure Access
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.