Analyse von CASB-Anwendungen von Drittanbietern

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie über OAuth Anwendungen von Drittanbietern erkennen und bewerten, die mit Microsoft 365-Tenants verbunden sind.

Überblick

Die Erkennung von Drittanbieteranwendungen bietet umfassende Einblicke in Anwendungen, Erweiterungen und Plug-ins von Drittanbietern, denen über OAuth Zugriff auf einen Microsoft 365 (M365)-Tenant gewährt wird. Diese Funktion ermöglicht die Identifizierung verbundener Anwendungen und ein Verständnis der Bereiche für autorisierte Zugriffe, einschließlich einer Risikoeinschätzung, um potenziell riskante Berechtigungen hervorzuheben.

Bedeutung

Diese Funktion verbessert die Verwaltung und Sicherung von M365-Umgebungen, indem sie Einblicke in die Verbindungen von Drittanbieteranwendungen ermöglicht und riskante Zugriffsbereiche hervorhebt. Sie ermöglicht fundierte Entscheidungen und eine proaktive Eindämmung potenzieller Sicherheitsbedrohungen.

Risiken einer OAuth-basierten Integration

OAuth-basierte Integrationen verbessern die Produktivität und optimieren Arbeitsabläufe, können jedoch erhebliche Sicherheitsrisiken darstellen. Anwendungen von Drittanbietern fordern häufig verschiedene Berechtigungen oder Zugriffsbereiche an, die von einfachem schreibgeschütztem Zugriff bis zu vertraulichen Berechtigungen reichen, die eine Datenänderung oder administrative Kontrolle ermöglichen. Eine unsachgemäße Verwaltung dieser Berechtigungen kann zu Datensicherheitsverletzungen, nicht autorisierten Zugriffen und anderen Sicherheitslücken führen.

Berechnung der Risikobewertung

Das System stuft alle Autorisierungsbereiche in Abhängigkeit von den potenziellen Auswirkungen als gering, mittel oder hoch ein. Beispiele:

- Bereiche, die Zugriff auf grundlegende Benutzerdetails gewähren, sind risikoarm.
- Bereiche, in denen Daten geschrieben, bearbeitet oder konfiguriert werden können, sind mit hohem Risiko verbunden.

Es wird die höchste Risikostufe unter allen Zugriffsbereichen angezeigt, die einer App gewährt wurden. Mit diesem Ansatz wird sichergestellt, dass Sie sich der wichtigsten Risiken bewusst sind, die mit den Anwendungen von Drittanbietern verbunden sind.

Zugriff auf Erkennung von Drittanbieter-Anwendungen

Um auf diese Funktion im Umbrella Dashboard zuzugreifen, navigieren Sie zu Reporting > Additional Reports > Third-Party Apps (Berichte > Drittanbieter-Apps).

Zusätzliche Informationen

Informationen zur Verwendung von Drittanbieter-Apps finden Sie in der Umbrella-Dokumentation:

Bericht zu Drittanbieter-Apps

Cloud Access Security Broker für Microsoft 365-Tenants

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.