Informazioni sull'individuazione di applicazioni di terze parti CASB

Sommario

Introduzione

Questo documento descrive come individuare e valutare applicazioni di terze parti collegate a tenant Microsoft 365 tramite OAuth.

Panoramica

L'individuazione di applicazioni di terze parti fornisce informazioni complete su applicazioni, estensioni e plug-in di terze parti a cui è concesso l'accesso a un tenant Microsoft 365 (M365) tramite OAuth. Questa funzionalità consente l'identificazione delle applicazioni connesse e la comprensione degli ambiti di accesso autorizzati, incluso un punteggio di rischio per evidenziare le autorizzazioni potenzialmente rischiose.

Importanza

Questa funzionalità migliora la capacità di gestire e proteggere gli ambienti M365 fornendo visibilità sulle connessioni delle app di terze parti e mettendo in evidenza gli ambiti di accesso a rischio. Consente di prendere decisioni informate e di ridurre in modo proattivo le potenziali minacce alla sicurezza.

Rischi delle integrazioni basate su OAuth

Le integrazioni basate su OAuth migliorano la produttività e semplificano i flussi di lavoro, ma possono comportare rischi significativi per la sicurezza. Le app di terze parti spesso richiedono diverse autorizzazioni o ambiti di accesso, che vanno dall'accesso di sola lettura di base alle autorizzazioni riservate che consentono la modifica dei dati o il controllo amministrativo. La gestione scorretta di queste autorizzazioni può esporre l'organizzazione a violazioni dei dati, accessi non autorizzati e altre vulnerabilità.

Calcolo del punteggio di rischio

Il sistema classifica tutti gli ambiti di autorizzazione come a basso, medio o alto rischio in base all'impatto potenziale. Ad esempio:

- Gli ambiti che concedono l'accesso ai dettagli utente di base sono a basso rischio.
- Gli ambiti che consentono la scrittura, la modifica o la modifica dei dati sono ad alto rischio.

Viene visualizzato il livello di rischio più alto tra tutti gli ambiti di accesso concessi a un'app. Questo approccio garantisce la consapevolezza dei rischi più significativi associati a ciascuna applicazione di terze parti.

Accesso all'individuazione di applicazioni di terze parti

Per accedere a questa funzione nel dashboard Umbrella, passare a Report > Report aggiuntivi > Applicazioni di terze parti.

Ulteriori informazioni

Per istruzioni sull'utilizzo del report delle app di terze parti, fare riferimento alla documentazione di Umbrella:

Report app di terze parti

Abilita Cloud Access Security Broker per tenant Microsoft 365

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).