SCIRGE
UNVEIL + CONTROL ALL BUSINESS WEB APP REGS & LOGINS

MIÉRT FONTOS A

SAAS MENEDZSMENT

A cégek sok esetben támaszkodnak különböző külsős webalapú alkalmazásokra és szolgáltatásokra. Tömegével kerülnek felhasználásra nap mint nap online fiókok különböző felhőben futó SaaS (Software as a Service) platformokon a munkával járó feladatok elvégzése céljából. A marketing osztály hozzáfér hírlevélküldő rendszerekhez, közösségi portálok menedzsmentjéhez; a HR részleg állásportálokhoz; a kereskedők CRM rendszerekhez, lead generáló oldalakhoz - csak néhány példát említve. A legtöbb ilyen fiók ad-hoc jelleggel kerül létrehozásra a munkavállalók által, aminek köszönhetően ezek nem kezeltek központilag, rendkívül magas biztonsági kockázatot és menedzsment nehézségeket okozva.

TUDTAD?

Átlagosan többszáz SaaS appot használnak a vállalatok. A felhasználók egyenként tucatnyi ilyen hozzáféréssel rendelkeznek. Ez akár több ezer nem menedzselt fiókot is jelenthet.

A "Shadow IT" kifejezés az IT részleg tudta nélküli erőforrások használatát jelenti. Ez magában foglalhat hardvert és szoftvert egyaránt, de általában a szoftveres felhőalapú SaaS alkalmazások használatát jelenti. A Shadow IT a vállalati erőforrások elleni rosszindulatú aktivitások melegágya.

- ✕ A vállalati fiókokkal - mint az Active Directory (AD) - szemben az IT számára többnyire ismeretlenek.
- ✕ A munkavállalók távozása után a hozzáférések továbbra is működhetnek.
- ✕ A felhasználók kerülik a komplex jelszavakat, ezért gyakori a gyenge vagy az AD jelszó használata.
- ✕ A különböző riportok alapján fiókok milliárdjai kompromittálódnak évente.
- ✕ A kiszivárgott fiókok és jelszavak illetéktelen hozzáférést jelenthetnek vállalati erőforrásokhoz.
- ✕ A jelszavak újrafelhasználása és kompromittálódása az ATO támadások leggyakoribb okozója.
- ✕ Gyakran ezek a fiókok megosztásra kerülnek a munkavállalók között nehezítve a felelősség kérdését.
- ✕ Audit esetén gyakorlatilag lehetetlen kézzel összegyűjteni a használt online fiókok listáját.
- ✕ Az ilyen fiókok jelentős része rövid élettartamú, hátramaradva használatlanul és változatlanul örökre.
- ✕ Az elhagyott vagy átfedésben levő fiókok szükségtelen kiadásokat eredményezhetnek.

A Scirge platform egyedi megközelítést biztosít a nem menedzselt webes felhasználói fiókok felderítésére és kezelésére. Segít felfedni, mely weboldalakon és webes szolgáltatásoknál regisztrálnak az alkalmazottak céges email címekkel. Centralizált szabályok segítségével kontrollálhatók és monitorozhatók a hozzáférések. A felfedezett fiókokról készült központi leltár segít csökkenteni az olyan biztonsági kockázatokat, mint pl. az "account takeover" vagy a "password reuse", valamint elősegíti a GDPR és egyéb audit elvárásokkal szembeni követelményeknek való megfelelést.

SCIRGE

A nem menedzselt webalapú fiókok felderítője.

Felderítés

Segít felfedni milyen webes alkalmazások és szolgáltatások vannak használatban. Új regisztrációk és meglévő fiókok bejelentkezései egyaránt detektálhatók.

Leltározás

A felfedezett fiókok központi nyilvántartása segít nyomonkövetni a hozzáféréseket és elősegíti a megfelelőséget a GDPR és egyéb auditok esetén.

Kontroll

Központilag menedzselt és terített szabályok határozhatják meg, hogy egy adott email cím használható-e regisztrációhoz vagy bejelentkezéshez egy weboldalon.

Szabályzás

Szabályok definiálják mi kerül monitorozásra vagy blokkolásra különböző, akár szabályonként eltérő paraméterek alapján.

Tudatosság

A munkavállalók biztonságtudatosságának növelése érdekében találat esetén központilag konfigurált üzenetek jeleníthetők meg.

Analízis

A központi felületen megjelenített adatok felfedhetik a webes alkalmazásokhoz tartozó fiókokkal kapcsolatos hozzáféréseket és szokásokat.

HOGYAN MŰKÖDIK?

A Scirge telepítése és menedzselése egyszerű. A vállalati SaaS fiókok felderítése pillanatok alatt elindítható.

Végponti böngészőkiegészítő

A böngészőkiegészítő komponenst a végpontokra szükséges telepíteni, ami történhet manuálisan vagy automatikusan (pl. GPO segítségével). A bővítmény begyűjti az aktív konfigurációt és szabályokat, amelyek alapján a webes fiókok regisztrációja és a bejelentkezések monitorozhatók. A szabályoktól függően lehetőség van blokkolásra, figyelmeztetésre, vagy a háttérben történő naplózásra vagy ignorálásra.

Központi szerver

A kliens-oldali böngésző bővítmény iparági sztenderdeknek megfelelő titkosított csatornán kommunikál a központi szerverrel a szabályok és a konfiguráció frissítéséhez, valamint a logok visszaküldéséhez. A központi szerver begyűjti és tárolja az adatokat, a feldolgozás után pedig részletes naplóbejegyzéseket és hasznos információkat biztosít. A központi szerver webes felületén az adminisztrátorok és az IT biztonság képviselői könnyedén és auditált módon kezelhetik és ellenőrizhetik a szabályokat.

Kiértékelés és frissítés

Ahogy az adatok begyűjtése és analizálása történik, úgy a szabályok könnyedén finomhangolásra kerülhetnek a környezet és az üzleti igények alapján. Többféle lehetőség biztosított a szabályok létrehozásához a kivételektől az általános megközelítésig. A biztonságtudatosság folyamatos növeléséhez figyelemfelkeltő üzenetek jeleníthetők meg a felhasználóknak.

WEB www.scirge.com

EMAIL info@scirge.com

SCIRGE