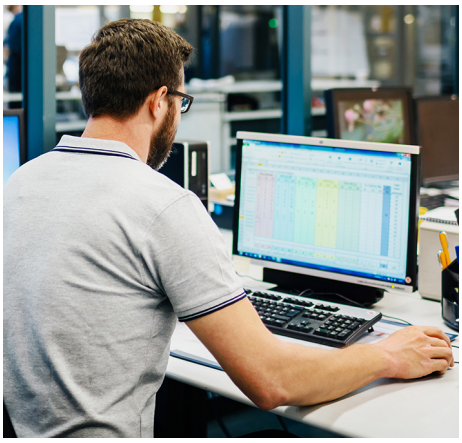
opentext™



Date equilibrio all'accesso mainframe con il sign-on automatizzato

Albert Einstein diceva: "Follia è fare sempre la stessa cosa aspettandosi risultati diversi". Analogamente, applicare anno dopo anno lo stesso livello di sicurezza all'accesso mainframe e aspettarsi che diventi magicamente più sicuro, in effetti, è folle.

Se da una parte la sicurezza nelle procedure di accesso alle applicazioni aziendali si è evoluta per far fronte a nuove minacce alla sicurezza, quella per l'accesso alle applicazioni mainframe è rimasta allo stesso livello per decenni. Questa stasi si è verificata per tre motivi principali:

- In primo luogo, le applicazioni mainframe esistenti fanno ancora il grosso del lavoro nella maggior parte delle aziende. Modificarle è rischioso, difficile e costoso. Anche la ricerca delle risorse umane per aggiornare i controlli di sicurezza degli accessi per queste applicazioni è quasi impossibile.
- Le aziende di grandi dimensioni, in secondo luogo, spesso non sono disposte a immergersi nel "vaso di Pandora" del mainframe. Il dialogo sull'IT ristagna spesso su domande di questo tipo: e se si rompe qualcosa? E se si rivela molto più complicato di quanto pensassimo? E se il nostro business subisse un arresto? Non possiamo mettere il mainframe al riparo e risolvere i problemi durante lo svolgimento delle nostre attività. I costi per duplicare tale ambiente, inoltre, sono troppo elevati in termini di tempo e denaro.
- In terzo luogo, vi è la percezione che il mainframe sia al sicuro all'interno del firewall e che solo gli utenti autorizzati possano accedervi, ma non vi è alcuna garanzia che non si verifichino violazioni delle credenziali di accesso al mainframe altrui da parte di un malintenzionato.

  Le applicazioni meno recenti utilizzano password deboli di otto caratteri, che non fanno distinzione tra maiuscole e minuscole. Non vi è amministratore di rete al mondo che ritenga che tali password siano sufficientemente complesse da proteggere qualsiasi informazione, soprattutto quelle relative ai clienti e alla proprietà intellettuale.

La questione è: come si fa a scardinare uno schema folle quando alcuni dei motivi di un dato comportamento si basano su paure molto reali e logiche?

L'incompatibilità dei sistemi di sicurezza aziendali

All'interno della maggior parte delle aziende vi sono due sistemi di sicurezza. Il primo è il sistema di Identity and Access Management (IAM) utilizzato per fornire accesso alle applicazioni e risorse aziendali. I sistemi IAM richiedono l'uso di una password di accesso complessa (di solito si tratta di una password con un minimo di 12 caratteri che include lettere maiuscole e minuscole, numeri e caratteri speciali). Le password complesse sono infinitamente più difficili da violare.

Anche i sistemi mainframe hanno la loro forma di "IAM", generalmente nota come RACF o Top-Secret. Tali sistemi forniscono autenticazione e autorizzazione alle risorse mainframe. Il problema è che, per loro "natura", le applicazioni che utilizzano questi sistemi richiedono solo password deboli di otto caratteri.

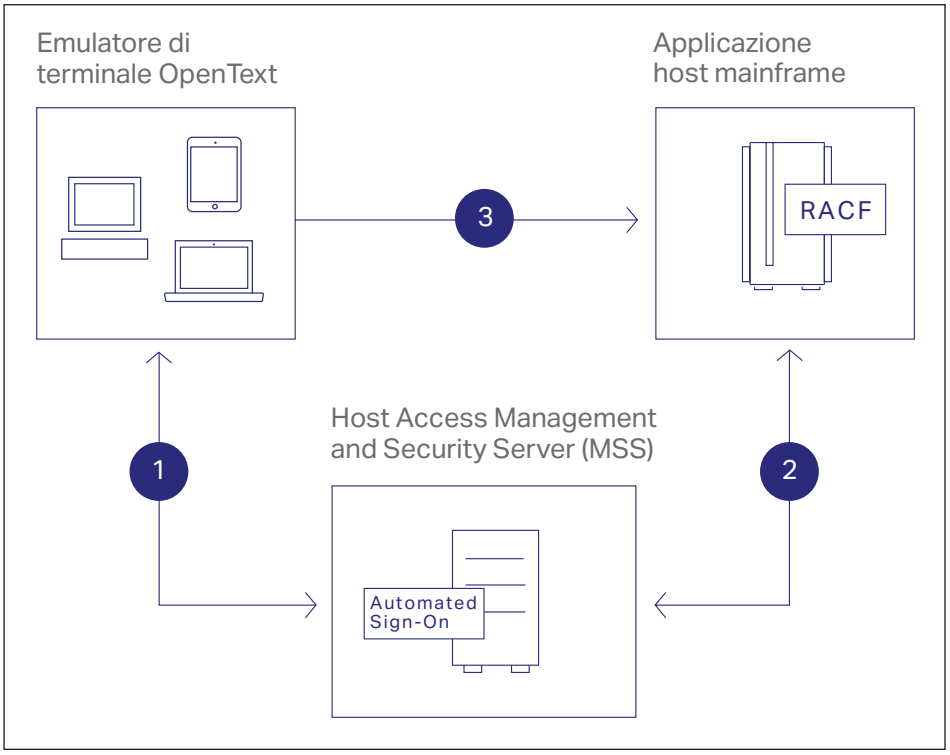
Abbiamo quindi a disposizione due sistemi separati che forniscono l'accesso alle risorse aziendali. A questo punto ci si deve domandare: perché è giusto richiedere un'autenticazione complessa per accedere alle applicazioni aziendali, ma solo un'autenticazione debole per accedere alle applicazioni mainframe di importanza critica, ossia quelle che consentono di gestire le vostre attività aziendali? È assurdo.

Questa follia deve cessare

E se ci fosse un modo per utilizzare il vostro sistema IAM per controllare e gestire l'accesso al vostro sistema host? In effetti c'è, si chiama OpenText™ Host Access Management and Security Server (MSS).

MSS porta finalmente equilibrio in azienda integrando il vostro mainframe con il sistema di Identity and Access Management (IAM) esistente. MSS offre un punto di controllo di sicurezza tra gli utenti che hanno bisogno di accedere al mainframe e ai sistemi host. Utilizza la vostra struttura IAM esistente, in particolare l'autenticazione complessa, per autorizzare l'accesso al mainframe.

MSS fornisce inoltre un prodotto aggiuntivo (Automated Sign-On for Mainframe) per garantire ulteriore equilibrio all'interno dell'ambiente. Automated Sign-On for Mainframe consente il sign-on automatizzato all'applicazione mainframe, eliminando la necessità per gli utenti di immettere eventuali ID o password. Provate a immaginare: niente più password per il mainframe.



1. L'emulatore avvia una sessione e richiede le credenziali utente per l'applicazione host da Automated Sign-On.
2. Automated Sign-On richiede un passticket utilizzabile una sola volta da RACF e lo invia nuovamente all'emulatore.
3. L'emulatore utilizza le credenziali di un passticket utilizzabile una sola volta per consentire all'utente di accedere automaticamente all'applicazione host.

Altri prodotti MSS aggiuntivi che forniscono un ulteriore livello di sicurezza critica per l'accesso host sono i seguenti:

- **Componente aggiuntivo MSS Security Proxy:** per ottenere una cifratura end-to-end e applicare il controllo degli accessi al perimetro tramite una tecnologia di sicurezza brevettata.
- **Componente aggiuntivo MSS Advanced Authentication:** per consentire l'autenticazione multifattore e autorizzare l'accesso ai vostri preziosi sistemi host.
- **Componente aggiuntivo MSS PKI Automated Sign-On:** per consentire l'accesso automatizzato PKI delle applicazioni ai vostri sistemi aziendali di importanza critica.
- **Componente aggiuntivo MSS Terminal ID Management:** per allocare dinamicamente gli ID dei terminali in base a nome utente, nome DNS, indirizzo IP o pool di indirizzi.

MSS e questi prodotti aggiuntivi sfruttano la vostra infrastruttura e le vostre risorse esistenti consentendovi di utilizzare gli strumenti di cui già disponete per proteggere e gestire l'accesso host. Sono, inoltre, in grado di offrire un valore aziendale duraturo, favorendo, al contempo, un TCO ridotto. In questo modo, garantiscono anche un riequilibrio dei livelli di sicurezza aziendale.

Scoprite di più su
www.opentext.com

Mettetevi in contatto con noi

261-IT0182-002 | O | 02/24 | © 2024 Open Text

opentext™