White paper

Un nuovo approccio per le password per mainframe: l'eliminazione

opentext™

Un nuovo approccio per le password per mainframe: l'eliminazione

Le password sono una necessità per l'azienda. Il loro compito è quello di assicurare che solo gli utenti autorizzati accedano al vostro bene più prezioso: le informazioni. Data questa importanza fondamentale, non basta una password qualsiasi. La password ideale è lunga e complessa. È diversa per ogni applicazione e richiede aggiornamenti regolari.

Anche le password possono rappresentare una minaccia per l'azienda. Dover creare password, doverle ricordare e modificare di continuo sono fattori che pesano sulle spalle degli utenti. Il tentativo di gestione e applicazione delle policy sulle password rappresenta una responsabilità per l'IT. Fortunatamente, i moderni sistemi NetIQ IAM (Identity and Access Management), insieme a quelli SSO (Single Sign-On), hanno contribuito a migliorare le cose. Gli utenti hanno bisogno di accedere una sola volta per avere a disposizione la maggior parte delle proprie risorse aziendali.

La maggior parte, ma non *tutte*. Purtroppo, i sistemi IAM e SSO non sono compatibili con i sistemi più importanti, quelli che effettivamente utilizza la vostra azienda. I vostri sistemi mainframe.

"Fornire l'accesso al mainframe ovunque e in qualsiasi momento"

Oggi gli utenti si aspettano di poter accedere alle loro risorse aziendali, compreso il mainframe, ovunque, in qualsiasi momento e da qualsiasi dispositivo. Ma concedere un accesso illimitato al mainframe vuol dire turbare il sonno degli amministratori di rete IT e di quelli dei sistemi mainframe.

Per quale motivo? Perché, quando si tratta di fornire un accesso sicuro, la rete e il mainframe sono come due isole autonome. Ognuna delle due utilizza il proprio sistema di controllo degli accessi. Ciascuna ha il proprio sovrano e nessuno dei due sovrani è disposto a rinunciare al controllo del proprio dominio per favorire l'altro.

Nonostante le dipendenze e i vantaggi comuni, ottenibili collaborando, i sovrani di ciascuna isola non vedono alcuna soluzione agli ostacoli posti dall'integrazione.

L'isola della rete

Gli amministratori della rete IT hanno un legittimo interesse a rafforzare la sicurezza di accesso al mainframe, perché gestiscono le applicazioni di emulazione di terminali, che rendono possibile l'accesso. Ma non vi è alcun modo per estendere la solida sicurezza della rete, dotata di password complesse facilitate dal sistema IAM, all'isola del mainframe.

La maggior parte delle applicazioni mainframe è stata scritta decine di anni fa, in tempi più sicuri. Non esistevano reti aperte, architetture orientate ai servizi e pirati informatici. Le applicazioni mainframe erano codificate con deboli password di otto caratteri, perché ritenute alquanto efficaci. Ora non è più così.

Riscrivere le applicazioni mainframe adesso è rischioso, disagevole e costoso, anche se ci si imbatte in programmatori mainframe ancora impiegati. L'unico altro modo per imporre una sola password per l'accesso a tutte le risorse di rete, compreso il mainframe, è semplificare le password aziendali a otto caratteri. Nessuno vuole muoversi in questa direzione.

L'isola del mainframe

Gli amministratori dei sistemi mainframe sanno che, dopo decenni di relativa disattenzione da parte della comunità di hacker, i mainframe si ritrovano improvvisamente presi di mira. Non hanno un sistema IAM, ma hanno un sistema RACF o Top-Secret per l'autenticazione e l'autorizzazione degli accessi al mainframe. Il che va bene, però purtroppo sono ancora obbligati all'uso di password da otto caratteri.

Per quanto vorrebbero rafforzare le proprie password e controllare gli accessi, gli amministratori dei sistemi mainframe sono irremovibili su una cosa: in nessun caso compromettono il 99,999 percento di affidabilità dei mainframe. Ma nella loro mente, questo è esattamente ciò che farebbero se cercassero di integrare l'accesso ai mainframe con i server di rete sull'isola della rete. Semplicemente, non possono permettersi i costanti tempi di inattività comunemente associati ai problemi di sicurezza della rete.

Problemi con le password dei mainframe

Dotati di grandi capacità, i mainframe hanno alcune peculiarità che li rendono degli intrusi nelle aziende moderne. Una di queste è la password per le applicazioni mainframe. Ecco perché questo è un problema:

- **Autenticazione debole**
  Provate a chiedere a qualsiasi esperto di sicurezza se pensa che una password di otto caratteri, senza distinzione maiuscole/minuscole, sia in grado di fornire un adeguato livello di protezione per i dati sensibili. La risposta sarà un sonoro "No!". Le password aziendali devono seguire delle rigorose policy. Ma per i motivi summenzionati, queste policy non possono essere applicate agli accessi ai mainframe.

Difesa in profondità con MSS

È possibile aggiungere anche ulteriori livelli di protezione associando MSS a questi componenti aggiuntivi:

- **MSS Security Proxy Add-On**
  Ottenete una cifratura end-to-end e applicate il controllo degli accessi al perimetro tramite una tecnologia di sicurezza brevettata.
- **MSS Advanced Authentication Add-On**
  Consentite l'autenticazione multifattori e autorizzate l'accesso ai vostri preziosi sistemi host.
- **MSS Automated Sign-On for Mainframe Add-On**
  Consentite l'accesso automatizzato alle applicazioni IBM 3270 tramite il sistema Identity & Access Management.
- **MSS PKI Automated Sign-On Add-On**
  Consentite l'accesso automatizzato PKI delle applicazioni ai vostri sistemi aziendali di importanza critica.
- **MSS Terminal ID Management Add-On**
  Allocate in modo dinamico gli ID dei terminali in base a nome utente, nome DNS, indirizzo IP o pool di indirizzi.

Con MSS e i suoi prodotti aggiuntivi, vi è infine un modo pratico per modernizzare la sicurezza mainframe senza alcuna ricodifica.

Come funziona MSS Automated Sign-On for Mainframe Add-On

Interagendo con la IBM z/OS Digital Certificate Access Service (DCAS), Automated Sign-On for Mainframe ottiene un PassTicket RACF per l'applicazione di destinazione da poter utilizzare una sola volta per un periodo di tempo limitato. Restituisce l'ID utente del mainframe e il passticket nella macro di accesso dell'emulatore del terminale, che invierà le credenziali al mainframe, per consentire all'utente di accedere all'applicazione.

- **Comportamento rischioso da parte degli utenti**
  In un'era come la nostra, costituita da accessi immediati, l'ulteriore passaggio di immissione delle credenziali per accedere al mainframe è visto come uno spreco di tempo da parte di molti utenti. Pensateci bene. Chi mai vorrebbe inserire una password diversa ogni volta che apre una nuova app, specialmente se la apre cinque o sei volte al giorno? Perciò, gli utenti cercano soluzioni convenienti, come quella di evitare di eseguire il logout o lasciare accese (e incustodite) le workstation quando se ne vanno.
- **Reimpostare la password del mainframe: non se ne parla!**
  Gli utenti che hanno accesso a più applicazioni su più mainframe hanno più password da ricordare. Nessuno può riuscirci, per cui ricorrono a metodi inaccettabili dal punto di vista della sicurezza: promemoria scritti su post-it o lievi modifiche alla password al momento dell'aggiornamento. Ma poi la dimenticano e quindi devono reimpostarla. A differenza delle password di rete, le password per mainframe non possono essere reimpostate dall'utente. Un addetto IT, ben pagato, dovrà interrompere ciò che sta facendo per eseguire questa attività ripetitiva e laboriosa.

Dai rischi per la sicurezza all'usabilità e alle problematiche di gestione dell'IT, l'accesso al mainframe tramite una password di otto caratteri è una prassi che necessita di un aggiornamento.

Il ponte verso una sicurezza serena

Le nostre due isole non si sono evolute in parallelo. Nell'isola della rete, la sicurezza per gli accessi alle applicazioni aziendali è stata potenziata per soddisfare le minacce sempre più sofisticate. Nell'isola del mainframe, la sicurezza prescritta per quelle applicazioni fondamentali, vecchie di decenni, è rimasta tale per decenni.

Per fortuna, finalmente esiste un metodo in grado di estendere una sicurezza solida e gestita a livello centrale alle vostre applicazioni mainframe senza mettere a repentaglio le attività aziendali, che si chiama OpenText™ Host Access Management and Security Server (MSS). La soluzione MSS integra il mainframe con il sistema IAM, realizzando così un ponte tra le due isole.

Più nello specifico, la soluzione MSS è compatibile con il sistema IAM per gestire e proteggere in modo centralizzato l'accesso al mainframe tramite gli emulatori di terminali Micro Focus. Posizionata tra l'utente e il mainframe, utilizza la struttura di autenticazione LDAP esistente per convalidare le credenziali di un utente prima di concedere l'accesso al mainframe. In altre parole, gli utenti non possono arrivare alla schermata di accesso host fino a quando non siano stati autenticati e autorizzati con solide credenziali IAM, ossia solide password complesse.

In combinazione con uno dei suoi componenti aggiuntivi (Automated Sign-On for Mainframe), la soluzione MSS elimina anche la necessità delle password per i mainframe. Avete capito bene. Gli utenti potranno saltare l'ulteriore passaggio di inserimento di una password per accedere alle proprie applicazioni mainframe dopo aver effettuato l'autenticazione per MSS. La soluzione MSS gestisce questo passaggio al posto loro. È una soluzione vincente per gli utenti (mai più rischiose password di otto caratteri da ricordare) e per il reparto IT attento alla sicurezza (che finalmente può liberarsi dalla gestione delle password).

MSS può essere installato su un server o sul mainframe, a seconda di quale sia la soluzione migliore per l'attività aziendale. Offre una soluzione flessibile, scalabile e altamente sicura per l'accesso al mainframe, che elimina il bisogno di password per i mainframe.

Sicuro, gestibile e conveniente

Una volta i vostri preziosi dati mainframe viaggiavano su un percorso protetto da e verso un terminale attendibile. Ora non è più così. Oggi, proteggere tali dati dai malintenzionati nell'autostrada di Internet richiede la protezione più avanzata possibile. È il momento di lasciare le deboli password di otto caratteri nel passato, nell'epoca alla quale appartengono. Costruite, invece, un ponte per il metodo di autenticazione più efficace che ci sia, per garantire che solo gli utenti autorizzati accedano ai vostri dati più importanti. MSS offre un metodo sicuro, gestibile e conveniente per poterlo fare.

Scoprite di più su
www.microfocus.com/opentext

Mettetevi in contatto con noi

Blog di Mark Barrenechea, CEO di OpenText

262-IT0080-001 | O | 09/23 | © 2023 Open Text

opentext™