White paper

Host Access Management and Security Server (MSS)
Add-on MSS Advanced Authentication

Utilizzo dell'autenticazione multifattori per autorizzare l'accesso al mainframe

MICRO FOCUS

Le password sono inefficaci

Ad essere sinceri, l'autenticazione degli utenti con nomi utente e password non è più efficace. Per quale motivo? Perché gli utenti non gestiscono le password in modo attento. Scelgono le password più ovvie. Utilizzano la stessa password più volte. E annotano le password su post-it che chiunque può trovare.

Ma gli utenti non sono l'unico problema

Utilizzare nomi utente e password, praticamente è come consegnare agli hacker le chiavi del vostro regno. I cyber criminali più scaltri scrivono algoritmi avanzati per trovare modi di aggirarli. Quindi, se viene utilizzata la stessa password per più applicazioni, gli hacker che hanno violato una password possono intrufolarsi ovunque vogliano. Ad esempio, un hacker potrebbe rubare la password di Facebook di un utente e in questo modo ottenere accesso alla vostra infrastruttura aziendale nella sua interezza. Questo problema è grande motivo di preoccupazione.

La conclusione è che i nomi utente e le password sono cose che un utente deve conoscere e saper utilizzare correttamente. E queste cose possono essere acquisite o rubate con relativa facilità. in sintesi, questi dati non sono abbastanza sicuri.

Le vecchie password per mainframe sono decisamente inefficaci

I problemi relativi alle password appena descritti si applicano anche alle password per mainframe. La differenza è che le password per mainframe delle applicazioni precedenti (quelle a supporto del vostro business e che contengono tutti i vostri dati più sensibili) sono protette solo da otto caratteri, senza distinzione tra maiuscole e minuscole. Scritte decenni fa, in periodi più sicuri, le applicazioni mainframe erano codificate con deboli password di otto caratteri perché ritenute alquanto efficaci. Ora non è più così.

Che cos'è l'autenticazione multifattori (MFA)?

L'autenticazione MFA combina più fonti di identità come modo per autorizzare l'accesso. Le soluzioni MFA più efficaci combinano almeno due dei tre seguenti tipi di fonti di identità:

- Qualcosa che l'utente *sa*, come un codice PIN o una password.
- Qualcosa che l'utente possiede, come una chiave elettronica, un telefono o un token.
- Una caratteristica fisica *dell'utente*, come le impronte digitali, la retina, la voce o il viso.

Richiedendo almeno due di queste fonti di identità, è possibile rafforzare notevolmente i requisiti di autenticazione e ridurre il rischio di una violazione alla sicurezza.

Che cosa non è l'autenticazione MFA?

Se la vostra banca vi chiede di inserire il PIN e il codice fiscale, non si tratta di autenticazione MFA. PIN e codici fiscali sono cose che voi *conoscete*. L'autenticazione MFA combina due di tre *sorgenti diverse* tra le cose che voi sapete, avete o siete.

La crescente necessità dell'autenticazione MFA

Le organizzazioni sono sempre più consapevoli dei rischi associati ad un'autenticazione a singolo fattore per le transazioni online. "Il rapporto del 2013 di Verizon sulle violazioni di dati, che ha individuato nell'autenticazione a singolo fattore il responsabile primario delle violazioni alla sicurezza, riferisce che il 76% delle intrusioni nella rete avvenute nel 2012 ha sfruttato credenziali deboli o rubate." Questo costoso problema può essere evitato grazie all'autenticazione MFA, rendendo i pagamenti elettronici veloci e affidabili come quelli in contanti.

La proliferazione di nuove leggi governative, quali HIPAA, sta anche favorendo l'adozione dell'autenticazione MFA. Il 26 marzo 2013 sono stati approvati nuovi regolamenti da parte del Dipartimento della Salute e dei Servizi Umani degli Stati Uniti d'America, che estendono i requisiti HIPAA di sicurezza e privacy a tutte le controparti del dipartimento, come appaltatori e fornitori, nonché provider di servizi, chi offre servizi per conto di un provider di servizi sanitari o chi fornisce soluzioni che integrano i dati relativi a medici o pazienti. Viste le ingenti multe per mancata conformità, molte organizzazioni stanno passando all'autenticazione MFA.

Se l'autenticazione multifattori risolve così tanti problemi, perché non è stata utilizzata?

Cambiare spesso va di pari passo con la resistenza e la migrazione all'autenticazione MFA non è diversa. La resistenza all'autenticazione MFA è solitamente collegata ad uno o più dei seguenti motivi:

- **Mancanza di informazioni**: i metodi di autenticazione biometrica (ad esempio, scanner di impronte digitali) sono già stati integrati in smartphone e PC. Ma molte aziende semplicemente non sanno come incorporare questa nuova tecnologia nelle loro consolidate infrastrutture di sicurezza.

- **La paura di ciò che non si conosce**: ad esempio, l'autenticazione MFA può complicare l'esperienza dell'utente? Poiché la facilità di utilizzo si traduce spesso in efficienza, le organizzazioni sono riluttanti a modificare lo status quo per qualsiasi motivo, anche per una maggiore sicurezza.
- **La paura del fallimento**: al fine di beneficiare di tutti i vantaggi dell'autenticazione MFA, è necessario configurarla in modo uniforme. In caso contrario, si potranno ottenere solo risultati mediocri. L'ampiezza dell'implementazione richiesta può essere scoraggiante.

Quando si tratta di implementare la tecnologia MFA per autorizzare l'accesso al mainframe, la resistenza è ancora più difficile da superare.

L'autenticazione MFA e il mainframe

Mentre la sicurezza per l'accesso alle applicazioni aziendali è cresciuta rafforzandosi per rispondere alle minacce sempre più sofisticate, le procedure per la sicurezza scritte nelle applicazioni mainframe sono rimaste ferme da decenni. Provate a chiedere a qualsiasi professionista della sicurezza IT se pensa che una password di otto caratteri, senza distinzione tra maiuscole e minuscole, sia in grado di fornire un adeguato livello di autenticazione per i dati sensibili. La risposta sarà un deciso "No!". Anche in tal caso, il mainframe è tipicamente lasciato fuori dalle discussioni sulla tecnologia MFA.

Il problema è tutto qui: per quanto robusto e affidabile, il mainframe è tipicamente isolato dal resto dell'azienda. Gli amministratori IT lo considerano una zona che sia meglio lasciare agli esperti di mainframe. Gli esperti, ossia gli amministratori dei sistemi mainframe, sanno che la riprogettazione delle applicazioni mainframe per il supporto di password complesse e solide è rischioso, difficile e costoso. Non hanno alcun desiderio di mettere a repentaglio il record di affidabilità del mainframe pari al 99,999% dei casi. Per quanto siano preoccupati per la sicurezza, hanno la sensazione di non poter fare nulla.

Ciò che è necessario per superare la loro resistenza è un metodo in grado di estendere una sicurezza solida e gestita a livello centrale, alle applicazioni mainframe senza mettere a repentaglio le attività aziendali.

La soluzione Micro Focus

In effetti, esiste un metodo sicuro, gestibile ed economico per estendere una sicurezza solida e gestita a livello centrale alle applicazioni mainframe: si chiama Micro Focus® Host Access Management and Security Server (MSS). La soluzione MSS funziona integrando il mainframe con il sistema IAM (Identity and Access Management), gestendo e proteggendo l'accesso al mainframe tramite gli emulatori di terminale Micro Focus.

Posizionata tra l'utente e il mainframe, la soluzione MSS 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.

La soluzione MSS funziona insieme ad un add-on, denominato MSS Advanced Authentication, per fornire l'autenticazione più solida possibile per i sistemi mainframe. Insieme, questi due prodotti attualmente supportano 14 diversi metodi di autenticazione, dalle smart card e dai codici di verifica basati su testo per i dispositivi mobili fino alla scansione delle impronte digitali e della retina. Da questa gamma di opzioni, è possibile scegliere quelle che sono più semplici da adottare e supportare per ogni organizzazione.

I prodotti MSS e MSS Advanced Authentication possono essere installati su un server o sul mainframe, a seconda di quale sia la soluzione migliore per l'attività aziendale. Questi prodotti forniscono una soluzione flessibile e altamente sicura per l'accesso al mainframe che non mette in pericolo le attività aziendali.

Rivalutazione dell'autenticazione MFA per il mainframe

L'arrivo di nuove tecnologie è spesso segnato da fallimenti poiché non si valutano attentamente tutte le implicazioni. Per quanto riguarda l'autenticazione MFA, diverse sono le questioni da considerare prima di iniziare:

- Stabilire e attuare una policy di autenticazione globale (piuttosto che adottare un approccio frammentario con acquisizioni ad-hoc).
- Rendere l'autenticazione MFA facile da gestire (evitare diversi metodi di autenticazione per diversi sistemi).
- Rendere l'autenticazione MFA facile da usare (valutare la possibilità di implementare contemporaneamente la tecnologia Single Sign-On (SSO) per semplificare il processo di autenticazione.

Se configurata correttamente, l'autenticazione MFA facilita effettivamente la vita degli utenti. In fondo, passare il dito su uno scanner e inserire un PIN è più semplice che ricordare nome utente e password.

Aspetti da considerare nella scelta di un fornitore MFA

Per garantire una corretta integrazione dell'autenticazione MFA, tenete questi fattori a mente durante la ricerca di un fornitore:

- Cercate soluzioni in grado di offrire più opzioni e applicazioni di autenticazione.
- Non sentitevi costretti a utilizzare un solo tipo di autenticazione fisica (in altre parole, non lasciate che l'hardware che scegliete determini la vostra filosofia di autenticazione).
- Cercate dei fornitori che sviluppino un framework aperto, costantemente aggiornato per integrare nuove tecnologie.
- Cercate dei fornitori che semplifichino il sistema per voi.

Non ha senso richiedere una solida autenticazione per accedere alle applicazioni aziendali e una debole autenticazione per accedere alle applicazioni mainframe di importanza critica. Poiché le minacce alla sicurezza continuano a crescere ed evolvere, le aziende devono essere pronte per affrontare la sfida. Micro Focus offre un metodo sicuro, gestibile e conveniente per soddisfare questa esigenza.

Micro Focus
Italia
+39 02 366 349 00

Micro Focus
Sede centrale
Regno Unito
+44 (0) 1635 565200

www.microfocus.com

www.microfocus.com