White Paper

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

Multifaktor-Authentifizierung zur Autorisierung des Mainframe-Zugriffs

MICRO FOCUS

Unsichere Passwörter

Offen gestanden ist eine Authentifizierung von Benutzern durch Benutzernamen und Passwörter nicht mehr effektiv. Der Grund dafür? Benutzer gehen zu sorglos mit ihren Passwörtern um. Sie wählen leicht zu erratende Passwörter. Sie nutzen immer wieder dasselbe Passwort. Und sie notieren sich Passwörter auf Klebezetteln, die jeder finden kann.

Die Benutzer sind nicht das einzige Problem

Wenn Sie sich auf Benutzernamen und Passwörter verlassen, öffnen Sie Hackern praktisch Tür und Tor zu Ihrem Reich. Intelligente Kriminelle schreiben ausgeklügelte Algorithmen, um Wege in Ihr System zu finden. Wenn dann dasselbe Passwort für mehrere Anwendungen verwendet wird, können Hacker, die ein Passwort geknackt haben, damit ganz nach ihrem Gutdünken auch woanders herumspionieren. Beispielsweise könnte ein Hacker das Facebook-Passwort eines Benutzers stehlen und so Zugriff auf Ihre gesamte Unternehmens-Infrastruktur erhalten. Dies gibt großen Anlass zur Sorge.

Unterm Strich sind Passwörter Dinge, die der Benutzer kennt. Und sie können relativ leicht aufgezeichnet oder gestohlen werden. Für sich allein genommen sind Passwörter einfach nicht sicher genug.

Alte Mainframe-Passwörter sind furchtbar schlecht

Die beschriebenen Probleme von Passwörtern gelten auch für Mainframe-Passwörter. Der Unterschied besteht darin, dass Mainframe-Passwörter für ältere Anwendungen – die zum Betrieb Ihrer Geschäftsprozesse dienen und all Ihre sensibelsten Daten enthalten – nur durch Passwörter mit acht Zeichen ohne Beachtung von Groß- und Kleinschreibung geschützt sind. Diese wurden vor Jahrzehnten, in sichereren Zeiten, festgelegt. Damals hatten Mainframe-Anwendungen noch eine festcodierte Passwortsicherheit mit acht Zeichen, da diese ausreichend war. Doch das hat sich geändert.

Was ist Multifaktor-Authentifizierung (MFA)?

MFA kombiniert mehrere Identitätsquellen, um den Zugriff zu autorisieren. Die effektivsten MFA-Lösungen kombinieren mindestens zwei der folgenden drei Typen von Identitätsquellen:

- Etwas, das Sie *kennen*, z. B. eine PIN oder ein Passwort.
- Etwas, das Sie *besitzen*, z. B. eine Schlüsselkarte, ein Telefon oder Token.
- Etwas, das Ihre *Identität nachweist*, z. B. ein Fingerabdruck, ein Netzhautscan, Sprach- oder Gesichtserkennung.

Indem Sie mindestens zwei dieser drei Identitätsquellen für den Zugang erforderlich machen, verschärfen Sie Ihre Authentifizierungsanforderungen und senken das Risiko einer Sicherheitsverletzung deutlich.

Wachsender Bedarf für MFA

Unternehmen werden sich zunehmend über die Risiken bewusst, die mit einer Ein-Faktor-Authentifizierung bei Online-Transaktionen verbunden sind. „Laut dem Verizon-Datenmissbrauchsbericht 2013, der die Ein-Faktor-Authentifizierung als Hauptursache für Sicherheitslücken ausmacht, waren 76 Prozent der unbefugten Netzwerkzugriffe im Jahr 2012 auf schwache oder gestohlene Passwörter zurückzuführen." MFA kann dieses kostspielige Problem eliminieren und elektronische Zahlungen so schnell und sicher wie Bargeldzahlungen machen.

Was ist keine MFA?

Wenn Ihre Bank Sie um Ihre PIN und Ihre Sozialversicherungsnummer bittet, handelt es sich *nicht* um MFA. PINs und Sozialversicherungsnummern sind beides Dinge, die Sie *kennen*. MFA kombiniert jedoch zwei oder drei *verschiedene* Quellen von Dingen, die Sie kennen, haben oder Ihre Identität ausmachen.

Außerdem regt die Zunahme neuer gesetzlicher Vorschriften wie z. B. HIPAA die Annahme der MFA an. Am 26. März 2013 sind neue Vorschriften des US-amerikanischen Gesundheitsministeriums (Department of Health and Human Services) in Kraft getreten. Diese Vorschriften weiteten die HIPAA-Anforderungen an Sicherheit und Datenschutz auf Auftragnehmer, Lieferanten und Dienstleister aus, die Leistungen im Namen eines Gesundheitsdienstleisters oder Lösungen anbieten, bei denen medizinische oder patientenbezogene Daten verarbeitet werden. Aufgrund der hohen Geldbußen bei Verstößen führen viele Unternehmen MFA ein.

Warum wird die MFA angesichts dieser Vorteile nicht längst eingesetzt?

Änderungen gehen oft mit Widerständen bei der Annahme einher, und die Migration auf MFA stellt keine Ausnahme dar. Einwände gegen MFA gründen normalerweise auf einen oder mehrere der folgenden Faktoren:

- **Informationsdefizit** – Biometrische Authentifizierungsmethoden (z. B. Fingerabdruck-Scanner) sind bereits in Smartphones und PCs integriert. Viele Unternehmen wissen nur nicht, wie sie diese neue Technologie in ihre etablierte Sicherheitsinfrastruktur einbinden können.
- **Angst vor Unbekanntem** – Wird MFA z. B. das Benutzererlebnis verschlechtern? Da Benutzerfreundlichkeit oft Effizienz bedeutet, zögern Unternehmen, den Status Quo aus irgendwelchen Gründen zu ändern – sogar, wenn dies zu mehr Sicherheit führen würde.
- **Angst vor Misserfolg** – Um von allen Vorteilen einer MFA zu profitieren, müssen Sie sie durchgängig einrichten. Wenn Sie dies nicht beherzigen, werden Sie nur mittelmäßige Ergebnisse

erreichen. Der erforderliche Umfang einer Implementierung kann abschreckend sein.

Bei der Implementierung von MFA zur Autorisierung von Mainframe-Zugriff können die Hürden des Widerstands noch höher sein.

MFA für den Mainframe

Während die Sicherheit beim Zugriff auf Unternehmensanwendungen stetig verbessert wurde, um den zunehmend ausgefeilten Bedrohungen zu begegnen, ist die in Ihren Mainframe-Anwendungen kodierte Sicherheit seit Jahrzehnten unverändert. Wenn Sie einen Experten für IT-Sicherheit fragen, ob er achtstellige Passwörter ohne Beachtung von Groß- und Kleinschreibung für eine angemessene Authentifizierung für sensible Daten hält, wird er dies definitiv verneinen. Nichtsdestotrotz wird der Mainframe bei Diskussionen um die MFA oft ausgespart.

Die Herausforderung besteht darin, dass der Mainframe aufgrund seiner Robustheit und Zuverlässigkeit typischerweise isoliert vom Rest des Unternehmens angesehen wird. IT-Administratoren überlassen ihn lieber Mainframe-Experten. Diese Experten – Mainframe-Systemadministratoren – wissen, dass die Umstrukturierung von Mainframe-Anwendungen zur Annahme sicherer komplexer Passwörter riskant, schwierig und kostspielig ist. Es liegt nicht in ihrem Interesse, die 99,999-prozentige Zuverlässigkeit des Mainframes zu gefährden. So sehr ihnen die Sicherheit auch am Herzen liegt, befinden sie sich in einer Zwickmühle.

Zur Überwindung dieses Widerstandes ist ein Weg erforderlich, der die strenge, zentral verwaltete Sicherheit auf Mainframe-Anwendungen ausweitet – und zwar ohne den Geschäftsbetrieb zu gefährden.

Die Micro Focus Lösung

Tatsächlich gibt es einen sicheren, überschaubaren, kostengünstigen Weg, um eine strenge, zentral verwaltete Sicherheit auf Mainframe-Anwendungen auszuweiten. Sie nennt sich Micro Focus Host Access Management und Security Server (MSS). MSS funktioniert durch die Integration Ihres Mainframes in Ihr Identity and Access Management (IAM)-System, indem es den Mainframe-Zugriff über Ihre Micro Focus Terminalemulatoren verwaltet und schützt.

MSS ist zwischen dem Benutzer und Mainframe angesiedelt und nutzt Ihre vorhandene LDAP-Authentifizierungsstruktur zur Überprüfung der Anmeldedaten eines Benutzers, bevor diesem Zugriff auf den Mainframe gewährt wird. Mit anderen Worten können Benutzer den Bildschirm für die Host-Anmeldung erst erreichen, wenn sie durch strenge IAM-Berechtigungsnachweise, d. h. sichere komplexe Passwörter authentifiziert und autorisiert wurden.

MSS arbeitet mit einem Add-on-Produkt namens MSS Advanced Authentication zusammen, um für bestmögliche Sicherheit bei der Authentifizierung an Ihren Mainframe-Systemen zu sorgen. Gemeinsam unterstützen diese beiden Produkte derzeit 14 verschiedene Authentifizierungsmethoden, von Smartcards und SMS-basierten Bestätigungscodes bis zu Fingerabdrücken und Netzhautscans. Aus dieser Bandbreite von Optionen können Sie diejenigen auswählen, die für Ihr Unternehmen an einfachsten in der Annahme und langfristigen Anwendung sind.

MSS und MSS Advanced Authentication können auf einem Server oder auf dem Mainframe installiert werden – je nachdem, was die beste Lösung für Ihr Unternehmen ist. Die Produkte bieten eine flexible und hochsichere Lösung für den Mainframe-Zugriff, ohne den Geschäftsbetrieb zu beeinträchtigen.

Erwägungen bei der Einführung von MFA für den Mainframe

Bei der Einführung neuer Technologien kommt es oft zu Misserfolgen, wenn sich niemand Gedanken über die möglichen Auswirkungen gemacht hat. Bei der Einführung der MFA sollten Sie daher im Vorfeld für Folgendes sorgen:

- Festlegung und Implementierung einer globalen Authentifizierungsrichtlinie (anstelle eines punktuellen Ansatzes mit Ad-Hoc-Einführungen).
- Einfache Verwaltung der MFA (unter Vermeidung verschiedener Authentifizierungsmethoden für verschiedene Systeme).
- Einfache Verwendung von MSA (ziehen Sie in Betracht, gleichzeitig Single Sign-on zu implementieren, um den Authentifizierungsprozess zu vereinfachen).

Wenn die MFA optimal implementiert ist, macht sie den Benutzern das Leben leichter, denn es ist sicher einfacher, mit dem Finger über einen Scanner zu fahren und eine PIN einzugeben, als sich einen Benutzernamen und ein Passwort zu merken.

Tipps für die Auswahl eines MFA-Anbieters

Um eine reibungslose MFA-Integration zu gewährleisten, sollten Sie bei der Anbieterauswahl folgende Faktoren im Hinterkopf behalten:

- Suchen Sie nach Lösungen, die mehrfache Authentifizierungsoptionen und Anwendungen bieten.
- Lassen Sie sich nicht auf eine Form der physischen Authentifizierung festlegen (mit anderen Worten: Ihre Authentifizierungsstrategie sollte nicht von der gewählten Hardware abhängig sein).
- Suchen Sie nach Anbietern, die in einem offenen Framework entwickeln, das bei der Einführung neuer Technologien unverzüglich aktualisiert wird.
- Suchen Sie nach Anbietern, die Ihnen ein einfach zu handhabendes System bereitstellen.

Es ergibt keinen Sinn, eine strenge Authentifizierung für den Zugriff auf Enterprise-Anwendungen zu fordern, während für den Zugriff auf die geschäftskritischen Mainframe-Anwendungen, über die Sie Ihre Geschäft abwickeln, nur eine schwache Authentifizierung erforderlich ist. Da die Sicherheitsbedrohungen immer weiter wachsen, sollte sich Ihr Unternehmen für diese Herausforderung wappnen. Micro Focus bietet einen sicheren, einfach zu handhabenden und kostengünstigen Weg, dies zu tun.

Micro Focus
Deutschland
Fraunhoferstraße 7
D-85737 Ismaning
+49 89 42094 0

Micro Focus
Schweiz
Flughafenstrasse 90
CH-8058 Zürich-Flughafen
+41 43 456 2300

Micro Focus
Firmenhauptsitz
Vereinigtes Königreich
+44 (0) 1635 565200

www.microfocus.com

www.microfocus.com