White Paper

Host Access Management and Security Server (MSS)
MSS Automated Sign-On for Mainframe Add-On

Ein Vergleich von Automated Sign-On-Optionen für den Mainframe

MICRO FOCUS

Mainframe-Sicherheit muss aufholen

Der mächtige Mainframe ist kein Computing-Dinosaurier. Dieser Hochleistungsrechner führt nach wie vor einen großen Teil der unternehmenskritischen Anwendungen der Geschäftswelt aus. Mit anderen Worten: Er wird so schnell nicht verschwinden. Das Problem ist, dass viele Mainframe-Anwendungen, die zum Teil vor Jahrzehnten geschrieben wurden, fest mit schwachen, aus acht Zeichen bestehenden Passwörtern arbeiten, die nicht zwischen Groß- und Kleinschreibung unterscheiden. Das war damals in Ordnung, reicht heute aber nicht mehr aus.

Gegen die immer ausgeklügelteren Sicherheitsbedrohungen von heute braucht es eine erheblich stärkere und einfacher zu verwaltende Lösung. Es gibt Lösungen, mit denen veraltete Passwortbeschränkungen überwunden werden können, aber welche ist die richtige für Sie? Dieses White Paper untersucht alle bedeutenden Optionen und bietet hilfreiche Auswahlrichtlinien.

Das Problem mit Mainframe-Passwörtern

Ihre letzte Bargeldabhebung am Automaten oder Ihr letzter Versicherungsfall wurde wahrscheinlich von einem Mainframe genehmigt. Doch auch wenn Mainframes sehr leistungsfähig sind, haben sie einige Eigenarten, die sie in einem modernen Unternehmen zum fünften Rad am Wagen machen. Eine dieser Eigenarten ist das Mainframe-Anwendungspasswort. Es ist aus folgenden Gründen problematisch:

- **Fehlende Abstimmung auf moderne Sicherheitsanforderungen**
  Früher berücksichtigten Netzwerke und Hacker unseren Alltag nicht. Das ist heute anders, weshalb für den Zugriff auf die meisten Geräte und Anwendungen ein Passwort erforderlich ist. Aber Passwörter allein reichen nicht aus. Ihre Wirksamkeit ist abhängig von Passwortstandards und der Passwortverwaltung.

  Best Practices verbieten beispielsweise Klebezettel an Monitoren und schreiben Passwörter mit zehn bis zwölf Zeichen und mindestens einem Großbuchstaben und einem Sonderzeichen vor. Was die Verwaltung angeht, ist ein einziges Passwort für den Zugriff auf alle Netzwerkressourcen einschließlich Mainframe-Anwendungen am einfachsten. Aber niemand möchte unternehmensweite Passwörter auf acht Zeichen vereinfachen.

- **Probleme bei der Passwortverwaltung**
  Den meisten Menschen fällt es nicht leicht, sich alle Passwörter zu merken. Jedes Mal, wenn sie das Passwort vergessen, muss es von einem Systemadministrator zurückgesetzt werden – eine alltägliche, arbeitsintensive Aufgabe, die von wichtigeren IT-Projekten ablenkt.

  Laut der Gartner Group handelt es sich bei 20 bis 50 Prozent aller Helpdesk-Anrufe um das Zurücksetzen von Passwörtern. Und Forrester Research gibt an, dass sich die durchschnittlichen Arbeitskosten für das Zurücksetzen eines Passworts auf ca. 70 US-Dollar belaufen*. Die Statistiken mögen unterschiedlich ausfallen, trotzdem bleibt die Tatsache, dass die Passwortverwaltung eine Verschwendung von Geld und Zeit ist.

* **www.mandylionlabs.com/PRCCalc/PRCCalc.htm**

- **Ein zusätzlicher, veralteter Schritt für Benutzer**
  Wenn sich Benutzer bei ihrem Computer anmelden, erhalten sie üblicherweise Zugriff auf alle autorisierten Unternehmensressourcen – mit Ausnahme des Mainframes. Um auf ihre Mainframe-Anwendung zuzugreifen, müssen sie sich erneut anmelden. Und das immer wieder, für jede Mainframe-Anwendung, auf die sie zugreifen. In der heutigen Zeit des schnellen Zugriffs auf Netzwerkressourcen stellt dieser zusätzliche Schritt ein Relikt aus der Vergangenheit dar.

Bezüglich Sicherheitsrisiken, IT-Management-Problemen und Benutzerfreundlichkeit ist die Anmeldung beim Mainframe mit einem acht Zeichen langen Passwort eine Vorgehensweise, die modernisiert werden muss. Aber wie entscheiden Sie, welche der verfügbaren Optionen die richtige für Sie ist?

Welche Lösung ist die richtige für Sie?

Es gibt eine Handvoll möglicher Lösungen für die Verbesserung der Sicherheit, um die IT-Abteilungen bezüglich der Passwortverwaltung zu entlasten und die Benutzerfreundlichkeit zu verbessern. Diese Lösungen sowie Highlights, Überlegungen und Auswahlrichtlinien werden im Folgenden beschrieben.

Single Sign-on im Unternehmen (Enterprise Single Sign-On, ESSO)

ESSO ist eine Technologie, die dafür sorgt, dass Benutzer nicht bei jedem Zugriff auf eine Netzwerkressource ihre Anmeldedaten eingeben müssen (dies gilt auch für Mainframe-Anwendungen). Die Benutzer authentifizieren sich nur einmal mithilfe der standardmäßigen Authentifizierungsmethode des Unternehmens. Ab diesem Punkt meldet die ESSO-Lösung den Benutzer bei jedem Zugriff auf eine Netzwerkressource automatisch an.

So funktioniert's

Im ESSO-Anmeldedatenspeicher werden die Anmeldedaten (Benutzernamen und Passwörter) für alle Benutzer und Ressourcen im gesamten Unternehmen sicher verwahrt. Bei jedem Zugriff eines Benutzers auf eine Ressource, die eine Anmeldung vom Benutzer erfordert, fängt der ESSO-Desktopagent die Anmeldeaufforderungen ab, ruft die Anmeldedaten für diese Ressource vom Anmeldedatenspeicher ab und leitet Benutzernamen und Passwort an die Anwendung weiter. Dieser Vorgang ist für den Benutzer und die Anwendung transparent.

Die ESSO-Integration mit Mainframes funktioniert auf dieselbe Weise. Der ESSO-Desktopagent interagiert über die HLLAPI-Schnittstelle des Terminalemulators mit der Mainframe-Anwendung. Wenn der Mainframe einen Anmeldebildschirm anzeigt, füllt ihn der Agent mit den Anmeldedaten des Benutzers, die aus dem Anmeldedatenspeicher abgerufen werden.

Highlights

- **Erfordert keine Änderungen an der Mainframe-Anwendung**
  Die Mainframe-Anwendung weiß nicht, dass sich hinter dem Benutzer-Anmeldevorgang eine ESSO-Lösung verbirgt. Der Mainframe fordert den Benutzer zur Eingabe von Benutzer-ID und Passwort auf und erhält die Anmeldedaten dann vom Client. Die Anwendung überprüft anschließend diese Anmeldedaten beim Mainframe-Sicherheitszugriffs-Framework, um den Benutzer zu authentifizieren – so wie immer.
- **Nutzt bestehende Authentifizierungsmethoden des Unternehmens**
  Für die Mainframe-Anmeldung ist keine einheitliche Authentifizierungsmethode erforderlich. ESSO nutzt die standardmäßige Authentifizierungsmethode des Unternehmens, um den Benutzer zu identifizieren, und ruft die Mainframe-Anmeldedaten für diesen Benutzer dann vom Anmeldedatenspeicher ab. Auch wenn die ESSO-Lösung das acht Zeichen lange Passwort für die Mainframe-Anwendung zur Anmeldung des Benutzers verwendet, könnte sich der Benutzer ursprünglich mit dem Benutzernamen und Passwort der ESSO-Lösung, einem digitalen Zertifikat oder einem einmaligen Token authentifiziert haben.
- **Beinhaltet Mainframe-Anwendungen ohne weitere Kosten**
  Je nach der Art der Lizenzierung Ihrer ESSO-Lösung ist das Hinzufügen der Mainframe-Anmeldung möglicherweise ohne zusätzliche Kosten enthalten. Es fallen zwar Integrations- und Wartungskosten an, aber die meisten ESSO-Lösungen werden pro Benutzer lizenziert, unabhängig davon, welche Anwendungen mit der ESSO-Lösung verbunden sind.

Überlegungen

- **Verwendet statische Passwörter**
  Auch wenn die Benutzer ihr statisches Passwort nicht manuell eingeben, wird es trotzdem für die Anmeldung bei der Mainframe-Anwendung verwendet. Daher hängt die Mainframe-Sicherheit weiterhin davon ab, ob Benutzer ihre Passwörter sicher verwahren, und IT-Abteilungen müssen sich nach wie vor um die Verwaltung der Mainframe-Passwörter kümmern.
- **Wird als unternehmensweite Infrastrukturlösung implementiert**
  ESSO wird fast nie nur für den Mainframe-Zugriff implementiert, sondern eher für den Zugriff auf alle Unternehmensressourcen. Infolgedessen sind ESSO-Projekte typischerweise groß, kostspielig und erstrecken sich über mehrere Jahre, da sie mit vielen verschiedenen Infrastrukturtypen zusammenarbeiten. Der Mainframe-Zugriff kommt, wenn überhaupt, erst am Ende einer langwierigen ESSO-Bereitstellung.
- **Erfordert die Integration des Desktopagenten und des Terminalemulators**
  Durch ESSO nimmt die Komplexität Ihrer Infrastruktur für den Mainframe-Zugriff zu. Da der ESSO-Desktop-Agent über HLLAPI mit dem Terminalemulator integriert werden muss, muss mehr zugriffsbezogene Software auf dem Desktop verwaltet werden. Beispielsweise müssen Sie jedes Mal, wenn Sie Ihren Terminalemulator aufrüsten, sicherstellen, dass die Integration zwischen dem Emulator und dem ESSO-Desktopagenten weiterhin wie erwartet funktioniert. Je nach Emulator-Upgrade kann eine Anpassung oder gar Neuprogrammierung der Integration erforderlich sein.

Ist ESSO für Sie geeignet?

Ist in Ihrem Unternehmen bereits eine ESSO-Lösung im Einsatz? Unterstützt Ihre ESSO-Lösung Mainframe-Anwendungen? Lässt die Sicherheitsrichtlinie Ihres Unternehmens statische, acht Zeichen lange Passwörter für die Mainframe-Authentifizierung zu? Wenn ja, kann ESSO eine praktikable Lösung für die Automatisierung des Mainframe-Anmeldevorgangs sein.

ESSO: Das Fazit

Wenn in Ihrem Unternehmen bereits eine ESSO-Lösung im Einsatz ist, beginnen Sie damit. Aber wenn Sie von statischen Passwörtern allgemein weg möchten, suchen Sie nach einer Lösung, die zeitlich begrenzte, einmalige PassTickets verwendet.

Express Logon Feature (ELF)

ELF, auch als Certificate Express Logon bezeichnet, ist eine IBM-Lösung, mit der Benutzer sich mit einem x.509-Zertifikat automatisch bei einer Mainframe-Anwendung anmelden können.

So funktioniert's

Der Terminalemulations-Client stellt eine SSL/TLS-Verbindung mit dem Telnet-Server her, um die Mainframe-Sitzung zu starten. Der Emulations-Client führt anschließend ein Anmeldemakro aus, das Platzhalter in die Felder für Benutzer-ID und Passwort eingibt. Der Telnet-Server fordert die Mainframe-Benutzer-ID des Benutzers an – basierend auf dem Client-Zertifikat, das beim SSL/TLS-Handshake angegeben wurde – und ein zeitlich beschränktes, einmaliges PassTicket von RACF. Der Telnet-Server fügt dann die Mainframe-Benutzer-ID und das PassTicket in die Platzhalter aus dem Anmeldemakro ein und meldet den Benutzer automatisch bei der Mainframe-Anwendung an.

Highlights

- **Macht die Passwortverwaltung überflüssig**
  Da ELF die Benutzer mithilfe von PassTickets bei einem einzigen Mainframe-Konto anmeldet, entfällt die lästige statische Passwortverwaltung für dieses Konto. Mit anderen Worten: keine Helpdesk-Anrufe mehr wegen vergessener Passwörter.
- **Unterstützt eine zweistufige Architektur**
  Das zweistufige Design von ELF bedeutet, dass Sie ohne zusätzliche Middleware eine automatisierte Mainframe-Anmeldung zu Ihrer Umgebung hinzufügen können.
- **Ermöglicht Identitätszuordnung in RACF**
  Es muss kein separater Datenspeicher und kein separates LDAP-Verzeichnis erstellt werden, um die Zuordnungen zwischen den Unternehmensidentitäten der Benutzer und den Mainframe-Benutzer-IDs zu verwalten. Das digitale Zertifikat des Benutzers kann direkt in RACF zu den Kontoinformationen des Benutzers hinzugefügt werden.

ELF: Das Fazit

ELF bietet ein hohes Maß an Sicherheit dank PassTickets und wird in den führenden Terminalemulations-Clients unterstützt. Aber wenn Ihre Benutzer keine X.509-Zertifikate für die Authentifizierung verwenden, oder wenn sie mehr als eine Mainframe-Benutzer-ID haben, werden Sie eine flexiblere Lösung benötigen.

Überlegungen

- **X.509 für die Benutzerauthentifizierung erforderlich**
  Die Zwei-Faktoren-Authentifizierungsmethode unter Verwendung von digitalen Zertifikaten ist zwar sehr sicher, aber teuer in der Implementierung und Verwaltung. Heutzutage verwenden die meisten Unternehmen die Authentifizierung mittels Benutzernamen und Passwort, die nicht mit ELF kompatibel ist.
- **Unterstützt nur eine Mainframe-Benutzer-ID pro Benutzer**
  Da das Zertifikat eines Benutzers nur einer einzigen Mainframe-ID in RACF zugeordnet werden kann, funktionieren die automatischen Anmeldefunktionen von ELF nur für Benutzer mit einer Mainframe-Benutzer-ID. Mit anderen Worten: ELF kann die folgenden beiden Benutzertypen nicht unterstützen:
  1. Benutzer mit Zugriff auf mehrere Mainframe-Anwendungen. In diesem Szenario funktioniert ELF nur, wenn die Benutzer-ID für alle Mainframe-Anwendungen dieselbe ist, was nicht zwangsläufig in jeder Umgebung möglich ist.
  2. Benutzer mit mehreren IDs für eine bestimmte Mainframe-Anwendung. Dieses Szenario liegt vor, wenn einem Benutzer je nach der entsprechenden Aufgabe unterschiedliche Zugriffsrechte gewährt werden.
- **Zertifikate müssen bei jeder Aktualisierung neu zugeordnet werden**
  Die Zuordnung von RACF zwischen den Zertifikaten und der Mainframe-ID des Benutzers ist mit dem Zertifikat selbst und nicht mit der Identität des Benutzers verknüpft. Bei jeder Aktualisierung des Client-Zertifikats – typischerweise alle zwei bis drei Jahre aus Sicherheitsgründen – muss die Mainframe-ID des Benutzers dem neuen Zertifikat in RACF zugeordnet werden.

Ist ELF für Sie geeignet?

Wenn Ihre Benutzer nur eine Mainframe-Benutzer-ID haben und digitale Zertifikate Teil Ihrer Sicherheitsinfrastruktur sind, kann ELF das Richtige für Sie sein. Andernfalls sollten Sie nach einer flexibleren Lösung suchen.

Automated Sign-On for Mainframe Add-On

Die Host Access Management and Security Server (MSS) Automated Sign-On for Mainframe Add-On-Software arbeitet mit Micro Focus Terminalemulation-Software, um Benutzer automatisch bei IBM 3270-Anwendungen anzumelden. Neben der Eliminierung statischer Passwörter arbeitet Automated Sign-On for Mainframe mit einer Reihe von Authentifizierungsmethoden, um eine stärkere Mainframe-Anwendungssicherheit ohne Neuprogrammierung bereitzustellen.

So funktioniert's

Wenn ein Benutzer eine Mainframe-Sitzung startet, fordert das Anmeldemakro des Emulators die Mainframe-Anmeldedaten des Benutzers von Automated Sign-On for Mainframe an. Automated Sign-On for Mainframe verwendet die Unternehmensidentität des Benutzers, um die Mainframe-Benutzer-ID zu erhalten. Dann erhält Automated Sign-On for Mainframe mithilfe von IBM z/OS Digital Certificate Access Server (DCAS) ein zeitlich beschränktes, einmaliges TAFC-PassTicket für die Zielanwendung. Es gibt die Mainframe-Benutzer-ID und das PassTicket an das Anmeldemakro des Terminalemulators zurück, das die Anmeldedaten an den Mainframe sendet, um den Benutzer bei der Anwendung anzumelden.

Highlights

- **Keine Passwortverwaltung mehr erforderlich**
  Automated Sign-On for Mainframe ermöglicht die Verwendung von PassTickets (statt statischer Passwörter) für die Anmeldung bei Mainframe-Anwendungen. Infolgedessen sind keine Mainframe-Passwörter mehr erforderlich, und die IT-Mitarbeiter müssen verlorene oder vergessene Passwörter nicht mehr zurücksetzen.
- **Unterstützt eine Vielzahl an Authentifizierungsmethoden**
  Automated Sign-On for Mainframe ist nahtlos mit vorhandenen Identity and Access Management-Systemen (IAM) kompatibel – von verzeichnisbasierten Benutzername/Passwort-Anmeldedaten bis hin zu digitalen Zertifikaten (obwohl digitale Zertifikate nicht erforderlich sind).
- **Unterstützt mehrere Mainframe-Benutzer-IDs**
  Automated Sign-On for Mainframe kann mehrere Mainframe-Benutzer-IDs einem einzigen Benutzer zuordnen, sodass Benutzer mit mehreren Mainframe-Konten die automatisierte Anmeldung für alle verwenden kann.

Überlegungen

- **Verwendet eine dreistufige Architektur**
  Automated Sign-On for Mainframe wird auf einem Middle-Tier-Server bereitgestellt, der sich zwischen dem Terminalemulations-Client auf der Workstation und der Anwendung auf dem Mainframe befindet – um das PassTicket vom z/OS DCAS-Dienst abzurufen.
- **Basiert auf der Zuordnung der Mainframe-Identität zur Unternehmensidentität**
  Sobald ein Benutzer authentifiziert wurde, stellt das IAM-System die Unternehmensidentität Automated Sign-On bereit. Damit Automated Sign-On funktionieren kann, muss IT dem Automated Sign-On-System eine Zuordnung der Unternehmensidentität des Benutzers zur Mainframe-Identität des Benutzers zur Verfügung stellen.
- **Nutzt DCAS-Dienst**
  Der IBM Digital Certificate Access Service (DCAS) muss auf dem Mainframe aktiviert werden. DCAS ist eine Komponente des z/OS-Kommunikationsservers (der z/OS TCP/IP-Netzwerk-Stack). Es ist in z/OS enthalten, aber nicht standardmäßig installiert.

Über PassTickets

PassTickets werden jedes Mal dynamisch von RACF erstellt, wenn Benutzer versuchen, sich bei Mainframe-Anwendungen anzumelden. Anders als statische Passwörter bieten PassTickets Schutz gegen Wiederholungen, da sie nur einmal verwendet werden können. PassTickets sind auch zeitlich begrenzt, was bedeutet, dass sie nach einem definierten Zeitraum ablaufen (standardmäßig 10 Minuten), selbst wenn sie nie genutzt wurden.

Automated Sign-On for Mainframe: Das Fazit
Wie ELF bietet Automated Sign-On for Mainframe dank PassTickets ein hohes Maß an Sicherheit. Der Unterschied liegt in seiner Flexibilität. Automated Sign-On for Mainframe unterstützt eine Vielzahl an Authentifizierungsmethoden und ermöglicht Ihnen die Zuordnung mehrerer Mainframe-Benutzer-IDs zu einem einzigen Benutzer.

Ist Automated Sign-On for Mainframe für Sie geeignet?
Werden Sie gebeten, die Sicherheit Ihrer unternehmenskritischen Mainframe-Anwendungen zu verstärken? Möchten Sie Mainframe-Passwortverwaltung abschaffen? Benötigen Sie die Flexibilität, nicht zertifikatbasierte Authentifizierungsmethoden und mehrere Mainframe-IDs für einen einzigen Benutzer unterstützen zu können? Automated Sign-On for Mainframe bietet eine sichere, effektive Möglichkeit zur Stärkung der Mainframe-Sicherheit ohne Neuprogrammierung der Mainframe-Anwendung.

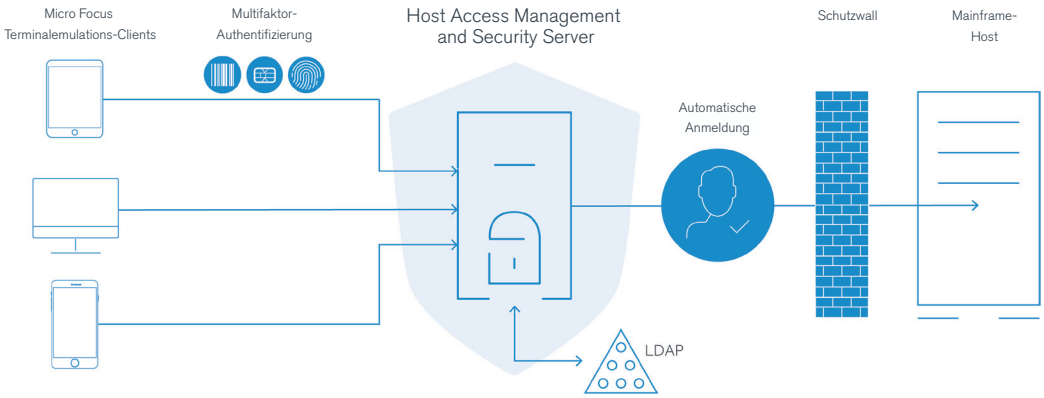

Abb. 1

Die Benutzer müssen den zusätzlichen Schritt der Eingabe eines Passworts zur Anmeldung bei ihren Host-Anwendungen nach der Authentifizierung beim Host Access Management and Security Server (MSS) nicht mehr ausführen. Das MSS Automated Sign-On for Mainframe Add-On übernimmt das für sie.

Mainframe ins Spiel bringen

Der Mainframe wird nicht wie der Dinosaurier aussterben, also sollten Sie ihn auch nicht so handhaben. Es gibt Möglichkeiten, ihn in Ihr modernes Sicherheits-Framework zu integrieren und die veraltete Anforderung eines acht Zeichen langen Passworts hinter sich zu lassen. Wenn Sie erst einmal die Funktionsweise dieser Lösungen verstanden haben, werden Sie die beste Option für Ihr Unternehmen auswählen können.

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

162-DE0077-002 | A | 01/17 | © 2016 Micro Focus. Alle Rechte vorbehalten. Micro Focus und das Micro Focus Logo sowie andere Namen sind Marken oder eingetragene Marken von Micro Focus oder Tochterunternehmen bzw. Schwestergesellschaften in Großbritannien, den USA und anderen Ländern. Alle weiteren Marken sind Eigentum ihrer jeweiligen Inhaber.