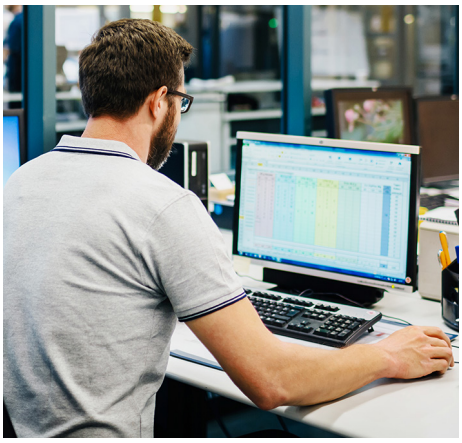
opentext™



Vereinfachen Sie mit Automated Sign-On den Mainframe-Zugriff.

Albert Einstein sagte einmal, die Definition von Wahnsinn sei es, immer wieder das Gleiche zu tun und andere Ergebnisse zu erwarten. Gleichermaßen wahnsinnig ist es, Jahr für Jahr die gleichen Sicherheitsmaßnahmen für den Mainframe-Zugriff zu verwenden und dann zu erwarten, dass alles auf magische Weise sicherer wird.

In der Vergangenheit gab es einige Weiterentwicklungen in Bezug auf einen sicheren Zugriff auf Enterprise-Anwendungen, um für die neuen Sicherheitsbedrohungen gewappnet zu sein; die Sicherheit beim Zugriff auf Mainframe-Anwendungen hingegen hat sich seit Jahrzehnten nicht verändert. Dieser Stillstand hat drei grundlegende Ursachen:

- Erstens: Die Legacy-Mainframe-Anwendungen leisten in den meisten Unternehmen noch immer einen Großteil der Arbeit. Verändert man die Anwendungen, ist dies riskant, schwierig und teuer. Bereits die Suche nach Mitarbeitern für die Aktualisierung der Security-Zugriffssteuerungen dieser Anwendungen ist eine nahezu unmögliche Aufgabe.
- Zweitens: In großen Unternehmen mangelt es oft an interner Motivation, sich an das Wespennetz der Mainframe-Infrastruktur heranzuwagen. Die Überlegungen der IT-Abteilung sehen dabei ungefähr aus wie folgt: Was, wenn wir etwas kaputt machen? Was machen wir, wenn es komplizierter wird als erwartet? Und was ist, wenn der Umsatz darunter leidet? Wir können keinen geschützten Raum für den Mainframe bereitstellen und alles reparieren, während wir uns gleichzeitig um das Alltagsgeschäft kümmern. Hinzu kommt, dass die Kosten für eine Duplizierung der Umgebung in Bezug auf Zeit und Geld zu hoch sind.
- Drittens: Es herrscht die Ansicht, dass der Mainframe hinter der Firewall sicher und geschützt ist und dass nur autorisierte Benutzer darauf zugreifen können. Es gibt jedoch keine Garantie, dass nicht irgendein Bösewicht die Mainframe-Anmeldedaten einer autorisierten Person stiehlt oder sich einhackt. Diese älteren Anwendungen arbeiten mit schwachen, aus acht Zeichen bestehenden Passwörtern, die nicht zwischen Groß- und Kleinschreibung unterscheiden. Es gibt keinen Netzwerk-Admin auf diesem Planeten, der der Ansicht ist, dass diese Passwörter stark genug sind, irgendetwas zu schützen. Dies gilt insbesondere für geistiges Eigentum oder Kundendaten.

Es stellt sich nun die Frage, wie man diesem etablierten Wahnsinn ein Ende bereiten kann, wenn einigen Ursachen dieses Verhaltens sehr reale und logische Ängste zugrunde liegen?

Die ungleichen Security-Systeme im Unternehmen

In den meisten Unternehmen gibt es zwei Security-Systeme. Das eine ist das IAM-System (Identity and Access Management), das den Zugriff auf die Enterprise-Ressourcen und -Anwendungen bereitstellt. Hierfür fordern die IAM-Systeme starke Passwörter – die normalerweise aus mindestens 12 Zeichen, darunter Klein- und Großbuchstaben, Zahlen und Sonderzeichen, bestehen müssen. Starke Passwörter sind ungleich schwerer zu hacken oder zu stehlen.

Für Mainframe-Systeme existiert eine eigene Art von „IAM“, die normalerweise als „RACF“ oder „Top-Secret“ bezeichnet wird. Über diese Systeme wird Authentifizierung und Autorisierung für Mainframe-Ressourcen bereitgestellt. Die Schwierigkeit liegt darin, dass die Anwendungen, die mit diesen Systemen arbeiten, in ihrem ursprünglichen Design nur den Einsatz schwacher, aus acht Zeichen bestehender Passwörter vorsehen.

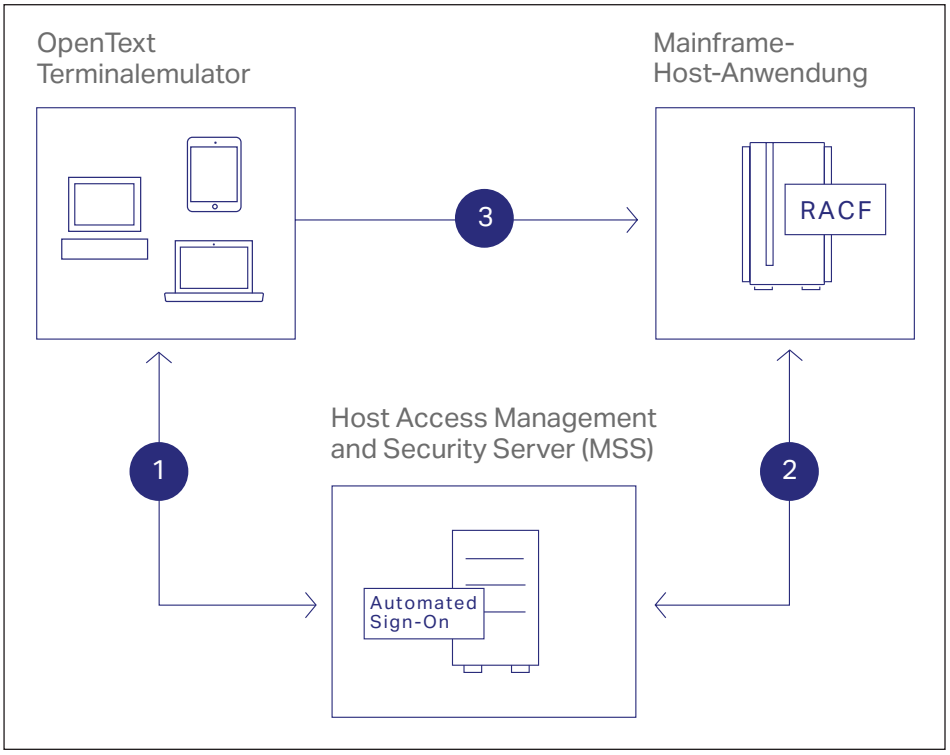
Es existieren also zwei separate Systeme für den Zugriff auf Enterprise-Ressourcen. Da stellt sich zwangsläufig die Frage: Warum ist es in Ordnung, eine starke Authentifizierung für den Zugriff auf Enterprise-Anwendungen zu fordern, während für den Zugriff auf die geschäftskritischen Mainframe-Anwendungen, über die Sie Ihr Geschäft abwickeln, nur eine schwache Authentifizierung erforderlich ist? Das ist wahnsinnig.

Beenden Sie diesen Wahnsinn

Was wäre nun, wenn es eine Möglichkeit gäbe, Ihr IAM-System zu nutzen, um den Zugriff auf das Host-System zu steuern und zu verwalten? Tatsächlich gibt es diese Möglichkeit. Sie nennt sich OpenText Host Access Management und Security Server (MSS).

Mit MSS kehrt der gesunde Menschenverstand zurück ins Unternehmen, indem Ihr Mainframe in das vorhandene IAM-System (Identity und Access Management) integriert wird. Über MSS wird ein Sicherheitssteuerungspunkt zwischen den Benutzern, die Mainframe-Zugriff benötigen, und Ihren Host-Systemen etabliert. Hierzu wird für die Autorisierung des Zugriffs auf den Mainframe die bereits vorhandene IAM-Struktur (insbesondere die starke Authentifizierung) genutzt.

Und um die Vernunft auf ein ganz neues Niveau zu erheben, bietet MSS ein spezielles Add-On-Produkt: Automated Sign-On. Automated Sign-On for Mainframe ermöglicht die automatische Anmeldung für alle Bereiche bis hin zur Mainframe-Anwendung. Die Benutzer brauchen also keine IDs oder Passwörter mehr eingeben. Stellen Sie sich das einmal vor. Keine Mainframe-Passwörter mehr.



1. Der Emulator startet eine Sitzung und fordert von Automated Sign-On die Anmeldedaten des Benutzers für die Host-Anwendung an.
2. Automated Sign-On fordert von RACF ein einmaliges PassTicket an und sendet es an den Emulator zurück.
3. Der Emulator nutzt die einmaligen PassTicket-Anmeldedaten, um den Benutzer automatisch bei der Host-Anwendung anzumelden.

Andere MSS-Add-On-Produkte sorgen für zusätzliche, dringend benötigte Sicherheit für den Host-Zugriff:

- **MSS Security Proxy Add-On:** Bereitstellung von durchgängiger Verschlüsselung und Durchsetzung von Zugriffssteuerung am Perimeter durch patentierte Security-Technologie.
- **MSS Advanced Authentication Add-On:** Aktivierung von Multifaktor-Authentifizierung für die Autorisierung des Zugriffs auf Ihre wertvollen Host-Systeme.
- **MSS PKI Automated Sign-On Add-On:** Automatisierte Anwendungsanmeldung bei wichtigen Unternehmenssystemen per PKI.
- **MSS Terminal ID Management Add-On:** Dynamische Zuweisung von Terminal-IDs basierend auf Benutzername, DNS-Name, IP-Adresse oder Adresspool.

MSS und diese Add-Ons nutzen die vorhandenen Ressourcen und Infrastrukturen, um den Host-Zugriff zu sichern und zu verwalten. Die Lösungen bieten einen nachhaltigen Geschäftswert und tragen zur Senkung der allgemeinen Betriebskosten bei. So tragen auch sie zu mehr gesundem Menschenverstand bei der Enterprise Security bei.

Erfahren Sie mehr unter
www.opentext.com

Stets das Neueste erfahren

261-DE0182-002 | O | 02/24 | © 2024 Open Text

opentext™