Whitepaper

Integration von Hostsystemen in moderne Sicherheitsframeworks

Die Welt rund um Ihre Host-Systeme hat sich verändert. Die leistungsstarken Unternehmenslösungen, die Jahrzehnte an Daten enthalten, passen nicht in Ihre schöne neue Sicherheitsinfrastruktur. Tatsächlich kann man sagen, dass Ihr modernes Sicherheits-Framework alles schützt – außer Ihren wichtigen Hosts. Die behördlichen Vorschriften fordern jedoch gleichen Schutz für alle Daten.

In diesem White Paper erfahren Sie, wie Sie Host-Systeme in das moderne Sicherheitskonzept integrieren – und so die technologische Lücke schließen – können, ohne dass der Geschäftsbetrieb gefährdet wird.

opentext™

Inhaltsverzeichnis

Seite

Die einzigartige Situation des Hosts

Es war einmal vor langer, langer Zeit, da befanden sich die Hostsysteme in einem sicheren Umfeld. Die Hostdaten wurden auf einem sicheren Weg von und zu einem vertrauenswürdigen Terminal übertragen. Der Host wusste, wer der Benutzer war, wo die Daten herkamen und wohin die Daten gingen.

Die Zeiten ändern sich. Heute gibt es offene Netzwerke, serviceorientierte Architekturen und Angreifer, die schneller hacken als die IT patchen kann. Die Hostsicherheit konnte mit der Situation nicht Schritt halten. Werden herkömmliche Hostzugriffssicherheitsmaßnahmen ergriffen, bleiben die Daten aus mehreren Gründen Gefahren ausgesetzt:

Schwache, dezentralisierte Authentifizierung

Häufig steht nichts außer einem einfachen achtstelligen Passwort zwischen einem bösartigen Hacker und Ihren kritischen Hostdaten. Die hostbasierte Authentifizierung alleine kann nicht das gesamte Potenzial des Identity Management Systems nutzen, das im Rest des Unternehmens eingesetzt wird.

Schwache, dezentralisierte Autorisierung

Nach der Anmeldung am Unternehmensnetzwerk kann jeder Benutzer einfach auf Ihre Hostanwendungen zugreifen. Dies bedeutet, dass ein Angreifer einfach nur die achtstellige Hostberechtigung stehlen muss, um unberechtigt zu den persönlichen Daten vorzudringen.

Dezentralisierte Revision

Jeder Host führt basierend auf der Host-ID jedes einzelnen Benutzers eine Revision des Hostzugriffs durch. Wenn mehrere Hosts beteiligt sind, müssen sich die Sicherheitsadministratoren die Protokolle auf jedem einzelnen Host ansehen – und dabei die Benutzer-IDs jedes Hosts mit der Benutzer-ID des Unternehmens vergleichen – um eine vollständige Revisionsliste zu erstellen.

Problematische Verschlüsselung

Bis zur Einführung der SSL/TLS-Verschlüsselung in den 90ern wurden die Daten und Passwörter zwischen dem Client und dem Host in Klartext übermittelt. Es gab keinen Schutz vor neugierigen Augen. SSL/TLS löste das Verschlüsselungsproblem, aber nicht ohne einen Haken: Verschlüsselter Traffic kann nicht über die DMZ überwacht werden, d. h., die IT-Sicherheit muss den Traffic durchlassen, ohne dass sie etwas über die Inhalte weiß.

Mangel an zentralisierter Kontrolle

Da die Authentifizierung, Autorisierung und Revision nur individuell für die einzelnen Hosts stattfinden kann, kann das zentrale Sicherheitsteam die Sicherheitsrichtlinien des Unternehmens nicht effektiv überwachen und konsequent durchsetzen.

Wenn man die kritische Bedeutung der Hostdaten bedenkt, sind dies wichtige Sicherheitslöcher. Aber wie können Sie Ihre Daten schützen, ohne die Hostanwendungen zu verändern, die in jahrzehntelanger Arbeit entwickelt wurden? Wie können Sie dafür sorgen, dass auch Ihre Hosts von der neuen sicheren Welt profitieren?

Das Abwehren neuer Sicherheitsbedrohungen, die durch immer raffinierter vorgehende Betrüger eingeführt werden, ist zu einer Lebensaufgabe geworden.

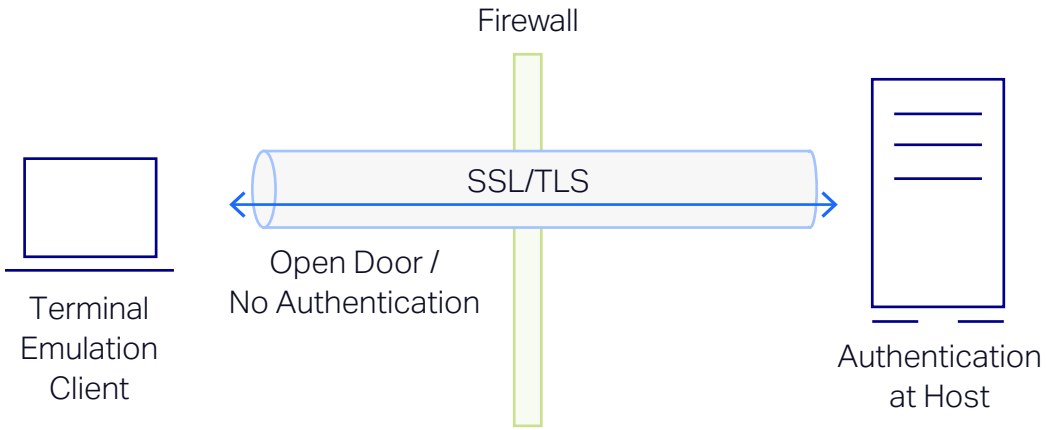

Abbildung 1. Die Hostsicherheit der ersten Generation bietet SSL/TLS-Verschlüsselung direkt am Host; die Authentifizierung findet jedoch erst statt, wenn die Verbindung am Host angekommen ist.

Moderne Sicherheitsframeworks

Das Abwehren neuer Sicherheitsbedrohungen, die durch immer raffinierter vorgehende Betrüger eingeführt werden, ist zu einer Lebensaufgabe geworden. Leider gibt es keine todsichere Möglichkeit, wie man dies schaffen kann. Die beste Verteidigung ist es, mit mehreren Sicherheitsschichten (einschließlich erweiterten Authentifizierungs- und Autorisierungstechnologien) zu arbeiten, um das Risiko zu minimieren.

So haben beispielsweise die IT-Organisationen der US-Regierung PKIs (Public Key Infrastructures; Infrastrukturen für öffentliche Schlüssel) und den Einsatz von Smartcards eingeführt, um besondere Standards für die Personenidentifikation wie PIV (FIPS 201) zu unterstützen. Nach und nach übernehmen auch immer mehr kommerzielle Unternehmen im Rahmen ihrer Bemühungen, neue Standards wie PCI DSS, SOX und HIPAA einzuhalten, diese Art von Kontrollen.

Moderne IAM-Systeme waren niemals darauf ausgerichtet, mit alten Hostsystemen zusammenzuarbeiten und umkehrt. Was aber wäre, wenn es eine Möglichkeit gäbe, die beiden Systeme zu integrieren – und die starke, zentral verwaltete Sicherheit auf Ihre Hostanwendungen zu erweitern – ohne den Geschäftsbetrieb zu gefährden? Und genau diese Möglichkeit gibt es. Sie nennt sich OpenText Host Access Management und Security Server (MSS).

Das Hinzufügen weiterer Sicherheitsschichten ist ein bewährtes Verfahren, das auch phasenweise durchgeführt werden kann. Die Realität sieht jedoch so aus, dass für eine starke Sicherheit auch ein starkes Management erforderlich ist. Aus diesem Grund entscheiden sich Organisationen für die Implementierung von Identity and Access Management-Systemen (IAM). IAM-Systeme wie Active Directory sind einer der Hauptbestandteile moderner Sicherheitsframeworks. Mit ihnen kann die IT-Abteilung von einer einzigen zentralen Stelle aus Zugriff auf Unternehmensdaten, Ressourcen und Anwendungen gewähren, widerrufen und prüfen.

Aber es gibt eine Schwierigkeit: IAM-Systeme können nicht für die datenreichen IBM-, HP-, UNIX- und Unisys-Hosts eingesetzt werden können, die es bereits seit Ewigkeiten im Unternehmen gibt. Und es gibt keine einfache Möglichkeit, die beiden Systeme zusammenzubringen. Die Hostlogik umzuschreiben, die das Herzstück Ihres Unternehmens ist, ist schwierig, riskant und teuer – selbst dann noch, wenn Sie irgendwie einen qualifizierten Mainframe-Programmierer finden, der noch nicht im Ruhestand ist. Ebenso inakzeptabel wäre es, Ihre starken IAM-Berechtigungen zu schwächen, um sie an die Host-Anmeldedaten anzupassen. Die Kosten, die dies verursachen würde, wären einfach viel zu hoch.

All dies sorgt dafür, dass Sie mit zwei separaten Sicherheitsinfrastrukturen arbeiten. Auf der einen Seite gibt es Ihre Hosts, die vermutlich über RACF oder Top Secret verwaltet werden. Auf der anderen Seite gibt es den ganzen Rest, der von IAM verwaltet wird. Und beide Infrastrukturen werden überschattet von immer strengeren behördliche Anforderungen, die Sie erfüllen müssen.

Brückenschlag mit der Host-IAM Alliance

Moderne IAM-Systeme waren niemals darauf ausgerichtet, mit alten Hostsystemen zusammenzuarbeiten und umkehrt. Was aber wäre, wenn es eine Möglichkeit gäbe, die beiden Systeme zu integrieren – und die starke, zentral verwaltete Sicherheit auf Ihre Hostanwendungen zu erweitern – ohne den Geschäftsbetrieb zu gefährden?

Und genau diese Möglichkeit gibt es. Sie nennt sich OpenText Host Access Management und Security Server (MSS). MSS und seine Zusatzkomponenten arbeiten mit Ihrem IAM-System zusammen, um den Hostzugriff über Ihre OpenText Reflection-, OpenText Extra!-, OpenText InfoConnect- und OpenText Rumba+ -Terminalemulatoren zentral zu verwalten und zu sichern. Es handelt sich um eine unterbrechungsfreie Lösung, für die keinerlei Änderungen an den Hostanwendungen oder dem IAM-System erforderlich sind.

Für jede der Sicherheitskategorien wird in Folge dargelegt, wie moderne Sicherheitsframeworks funktionieren und dann erklärt, wie sie mit MSS in Ihre Hostsysteme integriert werden können:

Zentralisierte Authentifizierung

So funktionieren moderne Sicherheitsframeworks: Ein IAM-System sorgt für starke Authentifizierung und strenge Sicherheitsrichtlinien im Unternehmen.

Was MSS tut: MSS bietet einen Administrationsserver, der das IAM-System nutzt, um die Berechtigungen eines Benutzers zu validieren, bevor er Hostzugriff gewährt. Mit anderen Worten: Benutzer können den Bildschirm für die Hostanmeldung erst erreichen, wenn sie mit strengen IAM-Berechtigungsnachweisen beweisen, dass sie wirklich die sind, die sie sind. Auf diese Weise kann für den Hostzugriff dieselbe starke Authentifizierung gefordert werden, die für den Zugriff auf andere Systeme erforderlich ist.

MSS erleichtert den Integrationsprozess, indem alle häufig verwendeten IAM-Systeme unterstützt werden, einschließlich Active Directory, NetIQ eDirectory by OpenText, IBM Tivoli Directory Server, OpenLDAP und Oracle Directory Server Enterprise Edition. Darüber hinaus unterstützt die Lösung verschiedene Authentifizierungstechnologien wie Kerberos-, NTLM-, CRL-, OCSP-, PKI- und X.509-Zertifikate, die von Smartcards wie CAC und PIV verwendet werden.

Zentralisierte Autorisierung

So funktionieren moderne Sicherheitsframeworks: Mit IAM-Systemen wird sichergestellt, dass die Benutzer nur Zugriff auf die Ressourcen und Informationen bekommen, die sie zur Erledigung ihrer Jobs benötigen.

Was MSS tut: Mit MSS können IAM-Autorisierungsschemas auf den Hostzugriff ausgeweitet werden, ohne dass etwas am Host oder am Benutzer-Workflow geändert werden muss. Beispielsweise können Sie Zugriff für eine bestimmte Gruppe oder Rolle gewähren, wodurch ein Benutzer Zugriff auf Ihren 3270 Mainframe, nicht aber Ihren Unisys-Host erhält. Mit dem MSS-Sicherheitsproxy kann die Autorisierung noch weiter ausgefeilt werden. Der Sicherheits-Proxy stellt ein patentiertes, zeitlich begrenztes und digital signiertes Token zur Verfügung, das PKI nutzt, um zu verhindern, dass unberechtigte Benutzer sich mit dem Host verbinden.

Darüber hinaus kann mit MSS definiert werden, was Benutzer (nicht) tun dürfen. So kann beispielsweise die Terminalemulation erhärtet werden, indem bestimmten Benutzern die Fähigkeit genommen wird, Makros zu bearbeiten oder die Verbindungseinstellungen für TLS 1.2 gesperrt werden.

Über den MSS-Administrationsserver können nach der Installation ganz einfach und während der Verarbeitung Anpassungen durchgeführt werden. Wenn die Benutzer das nächste Mal eine Sitzung öffnen, sind die Änderungen aktiv.

MSS erleichtert den Integrationsprozess durch die Unterstützung aller gebräuchlichen IAM-Systeme, einschließlich:

- Active Directory
- NetIQ eDirectory
- IBM Tivoli Directory Server
- OpenLDAP
- Oracle Directory Server Enterprise Edition

Darüber hinaus unterstützt die Lösung eine Vielzahl verschiedener Authentifizierungstechnologien, einschließlich:

- Kerberos
- NTLM
- CRL
- OCSP
- PKI
- X.509-Zertifikate, die zusammen mit Smartcards wie CAC und PIV verwendet werden.

MSS-Komponenten

In Ihrer MSS-Lizenz sind ein Administrationsserver und ein Metering-Server enthalten. Die folgenden Add-on-Produkte bieten zusätzliche, kritische Funktionalität:

MSS Security Proxy Add-On – Durchsetzung von Zugriffssteuerung am Perimeter durch patentierte Security-Technologie.

MSS Terminal ID Management Add-On – Dynamische Zuweisung von Terminal-IDs basierend auf Benutzername, DNS-Name, IP-Adresse oder Adresspool.

MSS Automated Sign-On for Mainframe Add-On – Befähigung der Benutzer, ihre Berechtigungen nur einmal einzugeben, um autorisierten Zugriff auf alle Enterprise-Systeme (einschließlich des Mainframes) zu erhalten.

MSS PKI Automated Sign-On Add-On – Automatisierte Anwendungsanmeldung bei wichtigen Unternehmenssystemen per PKI.

Mit MSS und seinen Add-on-Produkten kann die Hostsicherheit modernisiert werden, ohne dass Hostanwendungen oder das IAM-System geändert werden müssen.

Zentralisierte Revision

So funktionieren moderne Sicherheitsframeworks: IAM-Systeme dokumentieren, wer wann auf welches Netzwerk zugegriffen hat und stellen so den Netzwerkadministratoren die Daten zur Verfügung, die sie zum Erfüllen ihrer Revisionsanforderungen benötigen.

Was MSS tut: MSS nutzt das vorhandene IAM-System, um Benutzer zu authentifizieren, Hostzugriffe zu autorisieren und alle Aktivitäten an einer zentralen Stelle zu protokollieren. Mit diesem Prozess wird sichergestellt, dass Sie wissen, wer wann auf welchen Host zugegriffen hat. Auch wird sichergestellt, dass im Falle einer Revision ein dokumentierter Paper-Trail vorliegt.

Verschlüsselung

So funktionieren moderne Sicherheitsframeworks: Die Daten werden zu Beginn der Übertragung verschlüsselt – unabhängig davon, ob sie innerhalb oder außerhalb der Firewall stattfindet – und nach dem Empfang wieder entschlüsselt. Dieser Prozess schützt zwar die Daten, verhindert aber auch die erforderlichen Datenprüfungen in der DMZ.

Was MSS tut: MSS nutzt den MSS-Sicherheitsproxy, der sich zwischen den Desktops und Hosts befindet. Der Sicherheitsproxy akzeptiert SSL/TLS verschlüsselte Pakete und entschlüsselt sie, bevor sie an den Host geliefert werden. Nach der Entschlüsselung können die Pakete von der Intrusion Detection, Content Detection und anderen Sicherheitsgeräten auf mögliche Angriffe oder Sicherheitslücken überwacht werden.

Der MSS-Sicherheitsproxy funktioniert nicht wie einfache SSL/TLS-Gateways oder Umleitungsfunktionen, die SSL/TLS-Verbindungen akzeptieren, ohne zuerst den Benutzer zu autorisieren. Derartige Lösungen laden unbefugte Benutzer regelrecht ein, bis hin zum Host vorzudringen. Mit MSS wird unbefugten Benutzern, die versuchen, eine SSL/TLS-Verbindung mit dem Host aufzubauen – ohne zunächst vom MSS-Administrationsserver authentifiziert und autorisiert zu werden – der Zugriff am MSS-Sicherheitsproxy verwehrt. Der Sicherheitsproxy nutzt ein von Micro Focus (jetzt Teil von OpenText) patentiertes, sicheres Token, um sicherzustellen, dass nur autorisierte Benutzer zu den Hostressourcen gelangen.

MSS unterstützt Verschlüsselungsstärken bis zu 256-Bit AES. Darüber hinaus unterstützt die Lösung Verschlüsselungsmodule, die für FIPS 140-2 validiert wurden – einem der höchsten Sicherheitsstandards der US-Regierung. Dieses hohe Sicherheitsniveau schützt Hosts vor böswilligen Inhalten. MSS stellt weiterhin ein Framework zur Verfügung, um bei Bedarf weitere Sicherheitsschichten hinzufügen zu können.

Zugriff auf mehrere Hosts über einen einzigen Port

So funktionieren moderne Sicherheitsframeworks: Über einen einzelnen Listener-Port kann auf mehrere Back-End-Server zugegriffen werden.

Was MSS tut: Mit MSS kann über eine einzige Öffnung der Firewall (beispielsweise Port 443) auf alle Hosts zugegriffen werden. Später können weitere Hosts hinzugefügt werden, ohne dass etwas an der Firewall geändert werden muss. Diese vereinfachte Konfiguration verringert nicht nur die Anzahl an Ports, die überwacht werden muss, sondern verkleinert auch die Angriffsfläche Ihres Netzwerks.

Zentralisierte Konfigurationskontrolle

So funktionieren moderne Sicherheitsframeworks: Die IT arbeitet mit einem IAM-System, um verschiedene Anwendungskonfigurationen innerhalb des Unternehmens zentral zu sichern, verwalten und bereitzustellen.

Was MSS tut: Mit MSS können Hostzugriffsaktionen zentral über die MSS-Konsole verwaltet werden. Zugriffe können basierend auf einer Gruppe oder Rolle gewährt oder verweigert werden und Sicherheitsupdates und Konfigurationsänderungen schnell angewendet werden, um das System an sich ändernde behördliche oder Geschäftsanforderungen auszurichten. Dabei ist es möglich, Anpassungen nach der Installation während der Verarbeitung durchzuführen. Kurzum: Hunderte oder Tausende Desktops können ganz einfach konfiguriert und gesperrt werden. All dies nach Ihrem Zeitplan und nicht nach dem von anderen.

Ein wichtiger Vorteil von MSS ist, dass vorhandene Sicherheitsinvestitionen genutzt werden, um Terminalemulationszugriffe auf Hostsysteme von einer zentralen Stelle aus zu autorisieren, zu authentifizieren und zu prüfen. Dies führt dazu, dass die praktischen und logistischen Probleme, die mit der separaten Umsetzung starker Sicherheitsmaßnahmen an jedem einzelnen Back-End-Host zusammenhängen, beträchtlich verringert sind.

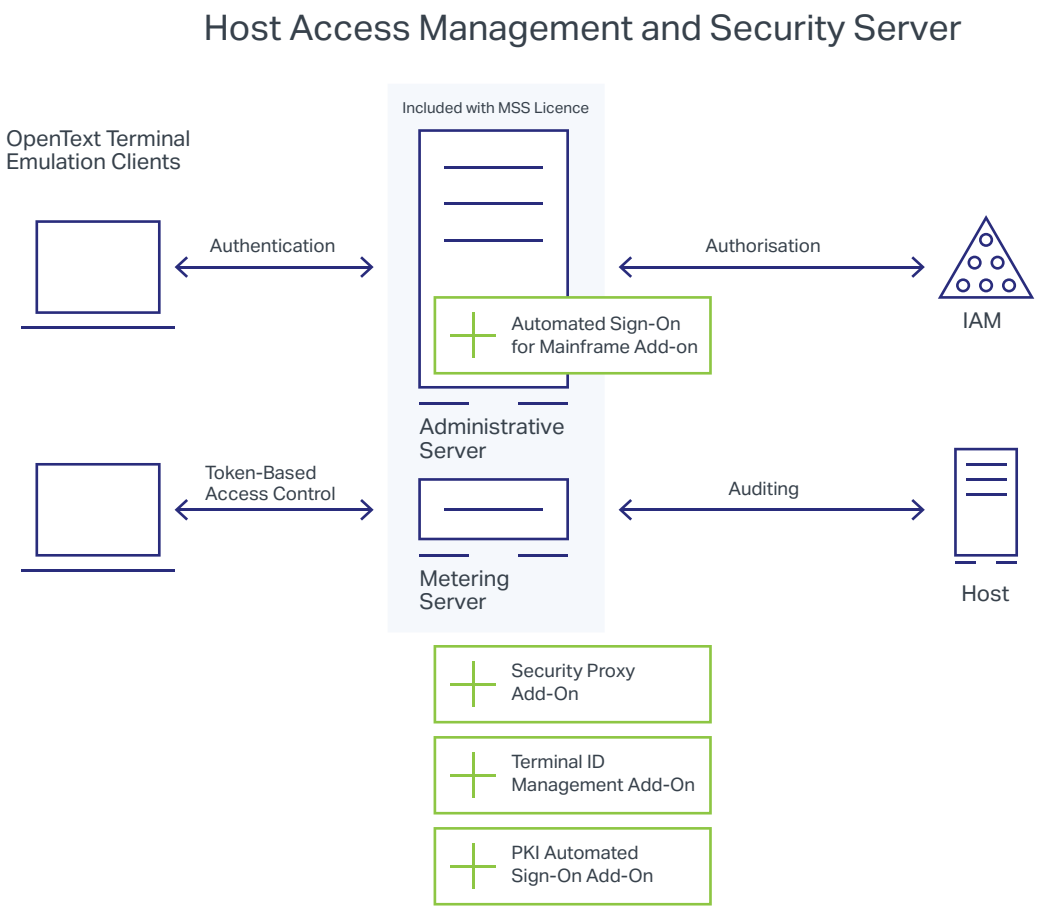

Abbildung 2. MSS agiert als Zugriffskontrollpunkt vor dem Host und stellt so sicher, dass die Benutzer vor dem Zugriff auf die Hostressourcen authentifiziert und autorisiert sind.

Gleicher Schutz für alle

Mit MSS kann endlich für alle wertvollen Host-Assets moderne, mehrschichtige Sicherheit bereitgestellt werden, ohne dass der Host oder das IAM-System geändert werden müssen. Durch die Integration dieser beiden kritischen Unternehmenssysteme über MSS können Sie:

- die Sicherheit für Ihre kritischen Hostanwendungen und Daten stärken;
- das Hostzugriffsmanagement optimieren;
- Ihre IAM-Investition durch eine Ausweitung von IAM auf die Hostsysteme maximieren;
- die Einhaltung der höchsten Sicherheitsanforderungen von heute erleichtern;
- Ihre Hostsicherheit sicher modernisieren, ohne dass die Benutzer-Workflows oder der Geschäftsbetrieb gestört werden.

Testen Sie MSS selber. Laden Sie den Evaluierungsleitfaden herunter unter **www.attachmate.com/products/mss/mss-eval-form.html** oder wenden Sie sich an Ihren Vertriebsmitarbeiter.

Erfahren Sie mehr unter
www.microfocus.com/opentext

Stets das Neueste erfahren

Blog von OpenText CEO Mark Barrenechea

262-DE0064-001 | O | 05/23 | © 2023 Open Text

opentext™