ssh communications security

DATA SHEET

UNIVERSAL SSH KEY MANAGER® 1.7

Identity und Access Management für Secure Shell Infrastrukturen

Der Universal-SSH Key Manager ist eine skalierbare, plattformübergreifende Lösung, welche die Sichtbarkeit von SSH Vertrauensbeziehungen sowie eine Nachvollziehbarkeit und Kontrolle von Secure Shell-Umgebungen ermöglicht. Er sorgt dafür das die Compliance Richtlinien für SSH Schlüssel eingehalten werden, reduziert des weiteren das Risiko von unbefugten Zugriffen und senkt die Kosten.

DAS PROBLEM

In den meisten großen Unternehmen dient Secure Shell (SSH) zur sicheren Authentifizierung und Geheimhaltung (Verschlüsselung) vieler geschäftskritischer Funktionen wie automatisierter Backups, täglicher Datentransfers und interaktiver Benutzerzugriffe für Systemadministratoren. Viele geschäftskritische IT-Funktionen werden durch SSH ermöglicht. Die meisten Unternehmen nutzen jedoch manuelle Prozesse zur Generierung, Konfigurierung und Bereitstellung von öffentlichen und privaten SSH-Schlüsseln, die diese Funktionen aktivieren.

Im Laufe der Zeit führt dies zu einer unkontrollierten Ausbreitung von Authentifizierungsschlüsseln. Sicherheitsmanager verlieren den Überblick und die Kontrolle darüber, wer Zugang zu welchen Servern hat und ob zuvor gewährte Zugriffsrechte zurückgenommen werden sollten. So wird es beinahe unmöglich, die Vertrauensbeziehungen von individuellen Benutzern, Systemkonten und Anwendungs-IDs und ihren entsprechenden Servern abzubilden.

Standardmäßige Identitäts- und Zugriffsmanagementlösungen, die Endnutzerzugriff regeln, beinhalten üblicherweise keinen auf SSH-Schlüsseln basierenden Zugriff zu Systemen und Konten. Aufgrund der fehlenden Governance und Kontrolle müssen Unternehmen mit erhöhten Risiken, Nichterfüllung von Compliance und den Kosten manueller Prozesse rechnen.

DIE HERAUSFORDERUNG

Herkömmliche Konzepte zur Verwaltung von SSH-Nutzerschlüsseln sind zeitaufwendig, teuer und bieten kaum Automatisierung oder Überprüfbarkeit. Da so viele geschäftskritische Funktionen – viele davon automatisiert– mit SSH arbeiten, ist es sehr schwierig, die Verwaltung von SSH-Schlüsseln unter Kontrolle zu bringen, ohne diese Funktionen zu unterbrechen. Das Problem zeigt sich insbesondere, wenn ein Zugang aufgrund von internen Änderungen, Kündigungen, Fusionen und Übernahmen gelöscht werden soll.

Unterstützte Secure Shell Versionen

ssh communications security

Centrify®

Attachmate

ORACLE SOLARIS

bitvise

UNIVERSAL SSH KEY MANAGER

DIE LÖSUNG

Der Universal SSH Key Manager (UKM) von SSH Communications Security ist eine Managementlösung für SSH-Benutzerschlüssel auf Unternehmensebene. UKM bietet einen unterbrechungsfreien Ansatz, der es Unternehmen ermöglicht die Kontrolle über die SSH Infrastruktur zu gewinnen und zu behalten, ohne durch Operationen die Produktionssysteme zu stören. Es besteht dabei auch keinerlei Notwendigkeit die bestehenden Arbeitsabläufe der Benutzer neu aufzusetzen oder Hunderte von automatisierten Prozessen zu ändern, welche letztendlich das Lebenselixier des laufenden Betriebes darstellen. Der unterbrechungsfreie Ansatz von UKM basiert auf den folgenden fünf Prinzipien:

- **Assess:** Definieren von SSH Richtlinien und anschließendem Abgleich der aktuellen SSH Umgebung mit Diesen.
- **Discover:** Aufdecken aller SSH-Schlüssel, abbilden aller Vertrauensbeziehungen und identifizieren aller Richtlinienverstöße.
- **Monitor:** Nachvollziehen der Schlüsselverwendung, um festzulegen welche Schlüssel sicher ohne Beeinträchtigung des Geschäftsbetriebs entfernt werden können.
- **Remediate:** Entfernen von Schlüsseln die gesperrt werden sollen und Sicherstellen, dass gültige Schlüssel den Compliance Richtlinien entsprechen.
- **Manage:** Beseitigung manueller Prozesse, zentralisieren der Kontrolle, Compliance Richtlinien durchsetzen und alle Aktivitäten prüfen.

Mit der optionalen Komponente “User Portal” ermöglicht UKM das Delegieren der wichtigsten Standardisierungsmaßnahmen an die Benutzer, die letztlich für die Anwendungen und Benutzer zuständig sind denen die Schlüssel gehören. Darüber hinaus bietet das “User Portal” eine einfache Möglichkeit SSH basierten Zugriff von einem zentralen Punkt aus im Einklang mit den Sicherheitsrichtlinien und vollständigem Audit-Trail anzufordern und bereitzustellen. UKM spart einem typischen Fortune 1000 Unternehmen im Durchschnitt 1 bis 3 Millionen Dollar pro Jahr an Betriebskosten bei gleichzeitiger Reduzierung des Risikos von schwerwiegenden Sicherheitsverstößen und Bereinigung von offenen Compliance Fragen. Unabhängig davon ob Ihre Umgebung OpenSSH, Tectia SSH oder andere SSH-Implementierungen verwendet bringt UKM dieses komplexe Problem unter Kontrolle.

ASSESS	DISCOVER	MONITOR	REMEDIATE	MANAGE
• Definieren von Richtlinien für SSH Schlüssel und Berechtigungen • Bericht über die Einhaltung der Richtlinien innerhalb Ihrer SSH Umgebung	• Verwendung eines Skript-basierten Scans, um schnell eine Bestandsaufnahme der SSH Schlüssel über Tausende von Hosts durchzuführen, oder einer Agentenlosen/Agenten Verbindung • Abbilden der Vertrauensbeziehungen und Abgleich dieser mit den definierten Richtlinien • Identifizieren von nicht genutzten oder nicht mehr benötigten Schlüsseln und Berechtigungen	• Nachvollziehen wann und von wo Schlüssel genutzt werden • Alarmierung, wenn Schlüssel hinzugefügt, entfernt oder geändert werden • Alarmierung bei nicht autorisierten Veränderungen der SSH Konfigurationen	• Entfernen nicht benutzter Schlüssel • Verschieben der Schlüssel in Root eigene Verzeichnisse • Aktualisieren und Beschränken von Berechtigungen • Erneuern von alten, nicht konformen Schlüsseln • Zentralisieren der Kontrolle	• Anbinden des Autorisierungsprozesses an existierende Ticket Systeme • Zentrales Verwalten und Durchsetzen von SSH Konfigurationen • Automatisieren der Bereitstellung sowie des Entfernens von Schlüsseln • Erkennen und Alarmieren von Richtlinienverstößen

FUNKTIONEN UND VORTEILE

Funktionen	Vorteile
Agentenlose und Skript-basierte Erkennung	Durchführen einer schnellen und unterbrechungsfreien Bestandsaufnahme der SSH-Schlüssel.
SSH Policies und Reports	Schneller Bericht über die Einhaltung der Richtlinien innerhalb Ihrer SSH Umgebung.
Automatisierungs- und Integrationsschnittstelle	REST API und CLI zur Anbindung an bestehende IAM Infrastrukturen und Arbeitsabläufen.
Echtzeit-Alarmierung	Versenden von Warnungen an SIEM Tools und beheben von Verstößen in Echtzeit.
Zentrale Verwaltung und Durchsetzung von SSH Client und Server Konfigurationen	Richtlinienkontrolle, stärkere Sicherheit, weniger Fehler.
User Portal	Erweitern des Key Managements auf die Endbenutzer innerhalb der Organisation. Benutzern erlauben Zugang anzufragen und zentralisiert gemäß der Richtlinien die Schlüssel bereitzustellen.
Compliance Unterstützung	Ermöglicht Compliance für aktuelle Anforderungen und geplante Updates von PCI. NIST/FISMA, SOX, HIPAA, Basel III Mandaten.

TECHNISCHE SPEZIFIKATIONEN

Unterstützte Plattformen für SSH Key Manager Server und SSH User Portal	• Virtuelle Appliance für VMWare ESX 5.5 und andere Hypervisor • Red Hat Enterprise Linux / CentOS 6.5 und neuere 6.x Versionen
Unterstützte Datenbanken	• Oracle 11.2, PostgreSQL 9.2
Hochverfügbarkeit	• Hochverfügbarkeit und Skalierbarkeit durch Unterstützung von mehreren UKM Servern • Berührungsfrei gegenüber der Produktionsumgebung – keine Schwachstellen
Erkennen	• Erkennen von öffentlichen & privaten Schlüsseln nach Größe und Typ • Kennwortphrase • Fehlerhafte Schlüssel • Schlüsseleigentümer und andere Schlüsselattribute (einschließlich Standort, Genehmigungen, Schlüssel Kommentaren) • Vetrauensbeziehungen je Host & Host Gruppe • Host-Schlüssel
Monitoring	• Erkennt unbefugte Änderungen an SSH-Konfigurationen • Erkennt unbefugtes Hinzufügen, Löschen, Ändern von Benutzerschlüsseln • Erkennt und verfolgt SSH-Schlüsselbasierte Logins • Konfigurierbare Echtzeit-Alarmierungen per E-Mail
Schlüssel Durchsetzung	• Überführt Benutzerschlüssel in eine zentrale Administration (Verschieben von Schlüsseln in Root eigene Verzeichnisse auf dem Host) • Erstellung von Passwort Geschützten Schlüsseln und Durchsetzung der Einhaltung der Passwort Richtlinien • Zentralisierte Verwaltung von Autorisierungsrichtlinien • Verwaltung von Schlüsseleinschränkungen (wie “Command” und “Allow-from” Einschränkungen
Automatisierung	• Erzeugung, Bereitstellung, Erneuerung, Aktualisierung und Entfernung von Schlüsseln • Zentrales SSH Software Konfigurations-Management • Automatisierung der Prozesse durch Verwendung der integrierten Kommandozeile • Bereitstellung von Temporärem Zugang (Schlüssel werden nach Ablauf automatisch entfernt)
Admin-Authentifizierung	• Lokale Authentifizierung • Externe Konten aus dem Active Directory • Passwort und Zertifikate basierte Authentifizierung
Rollenbasierte Verwaltung	• RBAC für Key Manager Administratoren (für lokale sowie Active Directory Administratorkonten) • Benutzerdefinierte Rollen für die Aufgaben der unterschiedlichen Administratoren
Protkollierung, Warnmeldungen, Alarmierungen	• Umfassende Audit-Trails für Änderungen an SSH-Schlüsseln und SSH-Konfigurationen, die sowohl durch Key Manager Administratoren als auch durch unbefugte Änderungen auf den lokal gemanagten Hosts veranlasst werden • E-Mail und Syslog-Warnmeldungen für Änderungen an SSH-Schlüsseln und Konfigurationen • Warnmeldungen bei verdächtigen Schlüsselaktivitäten pro Host (Schlüssel nach dem Gebrauch entfernt)
Verwaltungsmethoden	• Web GUI (aktuelle & stabile Version von Firefox, Chrome, und Internet Explorer 10, 11) • CLI • REST API
Management-Verbindungsarten	• Unterstützung von Host-Management mit und ohne Agenten • Unterstützung von Skript-basierter Schlüssel Erkennung. Durchführen von Scans mit Hilfe von vorhandenen Orchestrierungstools (z.B. Chef, Puppet, Ansible) und importieren der Ergebnisse. Managementaktionen erfordern agentenbasierte/ agentenlose Verbindungen.
Unterstützte Schlüssel Algorithmen	• RSA, DSA, ECC/ECDSA, Ed25519
Unterstützte HSM Produkte	• SafeNet Luna 5.4 (Verwendung zur Schlüsselspeicherung für Agentenlose Verbindungen)

UNIVERSAL SSH KEY MANAGER
TECHNISCHE SPEZIFIKATIONEN

Unterstützte SSH-Versionen	• Attachmate RSIT 6.1, 7.1, 8.1 • Centrify SSH 2013 • OpenSSH 4.x - 6.x • SunSSH 1.1.5, 2.0 • Tectia SSH 6.4 • Tectia Server for IBM z/OS 6.3, 6.4 • Quest OpenSSH 4.x - 5.2 • Bitvise SSH Server 6.24

Unterstützte Plattformen für gemanagte Hosts	Plattform	Ohne Agent	Mit Agent
	HP-UX 11iv1, 11iv2, 11iv3 (PA-RISC)	•	•
	HP-UX 11iv2, 11iv3 (IA-64)	•	•
	IBM AIX 5.3, 6.1, 7.1 (POWER)	•	•
	IBM z/OS 1.13, 2.1	•	
	Microsoft Windows Vista, 7, 10, Server 2003, Server 2008, Server 2008 R2, Server 2012, Server 2012 R2		•
	Oracle Enterprise Linux 5	•	•
	Oracle Solaris 9, 10, 11 (SPARC)	•	•
	Oracle Solaris 10, 11 (x86-64)	•	•
	Red Hat Enterprise Linux 4, 5, 6, 7 (x86, x86-64)	•	•
	CentOS 4, 5, 6, 7 (x86, x86-64)	•	•
	SUSE Linux Enterprise Desktop 10, 11 (x86, x86-64)	•	•
	SUSE Linux Enterprise Server 10, 11 (x86, x86-64)	•	•
	Ubuntu Desktop 12.04, 14.04 (x86, x86-64)	•	
	Ubuntu Server 12.04, 14.04 (x86, x86-64)	•