Unternehmensübersicht

SSH Communications Security

SSH Communications Security: Identitäts- und Zugriffsmanagement für Secure Shell-Umgebungen

Das Secure Shell-Protokoll ist der De-facto-Standard für die sichere Übertragung von Dateien und die Remote-Verwaltung von Systemen. Die überwiegende Mehrheit der großen Unternehmen und Regierungsbehörden weltweit vertraut auf Secure Shell, um die Vertraulichkeit und Integrität unternehmenskritischer IT-Funktionen sicherzustellen. Jedoch ist Secure Shell (SSH) ein Protokoll und keine Sicherheitslösung an sich. Schlecht umgesetzte SSH-Implementierungen können Unternehmen dem Risiko von Datenschutzverletzungen, Denial-of-Service-Angriffen und Compliance-Lücken aussetzen.

Als Entwickler des Secure Shell-Protokolls ist SSH Communications Security als Branchenexperte anerkannt. Wir verfolgen das Ziel, Secure Shell-Lösungen bereitzustellen, die Risiken minimieren, die Compliance gewährleisten und Kosten senken. Die Produkte und Services von SSH Communications Security helfen zurzeit über 3000 Unternehmen und Regierungsbehörden (darunter 7 der 10 führenden „Fortune 500“-Unternehmen) dabei, dieses Kernelement ihrer IT-Infrastruktur zu verwalten und zu kontrollieren.

Die Datensicherungsplattform

Es scheint paradox zu klingen, doch die falsche Anwendung eines Sicherheitsprotokolls kann zu einer verringerten Sicherheit führen. Das Secure Shell-Protokoll wird weithin für viele kritische IT-Funktionen eingesetzt: Systemverwaltung, automatisierte Datenübertragung und Backups. Zu oft jedoch wird SSH ohne die Standards des Identitäts- und Zugriffsmanagements (IAM) implementiert, die allgemein für Endnutzer gelten. Dieser Umstand ist besonders alarmierend, weil SSH-Benutzer (in der Regel Systemadministratoren) für gewöhnlich über höchste Zugriffsrechte verfügen – die selbst noch über denen von C-Level-Führungskräften liegen. Viele große Unternehmen haben die Kontrolle und den Überblick darüber verloren, wer Zugriff auf ihre kritischsten Systeme hat und welche Vorgänge auf diesen Systemen stattfinden.

Die Sicherheitslösung von SSH Communications Security basiert auf einer modularen Architektur, die die vollständige IAM-Kontrolle auf Secure Shell-Umgebungen ermöglicht. Die Kernmodule dieser Lösung stellen folgende Funktionen bereit:

- **SSH-Implementierung**. Nutzen Sie zuverlässige und unterstützte SSH-Software, um kritische IT-Funktionen zu sichern, ohne bestehende Anwendungen und Prozesse zu unterbrechen.
- **SSH-Management.** Verwalten und aktualisieren Sie die SSH – Softwareumgebung zentral. Kontrollieren Sie die Verteilung, die Richtlinien und die Nutzung von SSH-Schlüsseln.
- **SSH-Transparenz.** Autorisierte, störungsfreie Einblicke in die Vorgänge der Anwendungen und Datenübertragungen, die durch SSH abgesichert sind. Nutzen Sie SIEM, DLP, Audit und Forensik.

Ihre Vorteile

Einfach gesagt: Unternehmen, die die Datensicherungsplattform implementieren, minimieren ihr Risiko für Datenverluste aufgrund von Datenschutzverletzungen, erreichen Compliance der von der Branche und der Regierung vorgegebenen Sicherheitsstandards und senken gleichzeitig ihre Kosten. Eine verwaltete SSH-Umgebung ist sicherer und kosteneffizienter zu betreiben.

Wirtschaftlichkeit Ihrer Sicherheitsinvestition

Kosten

- Implementierung, Konfiguration und Verwaltung automatisieren.
- Manuelle Prozesse eliminieren.
- Eine Konsole, umfassender Verwaltung.
- Nahtlose Integration in die bestehende Infrastruktur (SIEM, DLP, IPS).

Risiko

- Richtlinienkontrolle.
- Gegenmaßnahmen – Schwachstellen erkennen und beheben.
- Benutzerrechte überwachen.

Compliance

- Standards, wie z.B. PCI-DSS, SOX, NIST, HIPAA, erfüllen oder übertreffen.
- Offene Audit-Aufgaben abschließen.
- Schlüsselfertige Compliance-Berichte. Audit-Prozess vereinfachen und beschleunigen.

Implementierung	Produktbeschreibung	Unterscheidungsmerkmale
Tectia SSH Client™ & Tectia SSH Server™	Enterprise-Lösung für die Sicherung der Systemverwaltung, Datenübertragung und Anwendungsanbindung in heterogenen Enterprise-Netzwerken	• Transparentes TCP-Tunneling auf Windows • Sichere FIPS 140-2–zertifizierte Verschlüsselung • Umfassender X.509 PKI-Support, für RSA SecurID, Kerberos, und Windows Domain-Authentifizierung
Tectia SSH for Mainframes™	Enterprise-Sicherheitslösung für die vollständige Integration von SSH und SFTP ins IBM z/ OS und die System z-Plattform für den sicheren Mainframe-Zugriff	• Transparente FTP-SFTP-Konvertierung • Beschleunigungssupport für sämtliche FIPS 140-2-zertifizierte Kryptographie-Hardware von IBM • Direktzugriff auf MVS-Datensätze • Nutzung bestehender RACF/ACF2/TSS-Keyrings und ICSF-Schlüssel sowie SAF und Zertifikatsprüfung
Tectia FTP-SFTP Converter™ & Tectia PCI Point to Point Encryption™	Unternehmen können schnell und kosteneffizient jeden FTP-Dateitransfer oder Anwendungsverkehr sichern, ohne die bestehende Infrastruktur, Skripts oder Anwendungen ändern zu müssen	• Transparente FTP-Konvertierung und TCP-Tunneling • Checkpoint-/Neustart-Funktion gewährleistet die zuverlässige Übertragung großer Dateien • Client-seitige SFTP API (Anwendungs-programmierschnittstelle) für Java und C • Auch für Mainframes geeignet

Management	Produktbeschreibung	Unterscheidungsmerkmale
Universal SSH Key Manager™	Enterprise-Lösung, um private und öffentliche Schlüsselbeziehungen zu Endnutzern, Service-Accounts und Anwendungs-IDs in Tectia SSH- und OpenSSH-Umgebungen zu erkennen, zu organisieren und zu verwalten	• Automatisch Informationen über private und öffentliche Benutzerschlüssel innerhalb der verwalteten Umgebung erfassen • Benutzer und Hosts in Gruppen organisieren und diese Gruppen nutzen, um Autorisierungsregeln zu erstellen, d.h. wer Zugriffsrechte auf welche SSH-Server erhält • Automatische Verwaltung von privaten und öffentlichen Schlüsseln (Verteilung, Ersatz, Entfernung)
SSH Host Key & Configuration Manager™	Abwicklung des Konfigurationsmanagements, Host-Key-Managements, der Richtliniendurchsetzung, des Monitoring, der Audits und Berichterstellung sowohl in Tectia SSH- als auch in OpenSSH-Umgebungen	• Masseninstallationen, Upgrades und Deinstallationen von SSH und OpenSSH durchführen • SSH-Softwarekonfigurationssätze erstellen, pflegen, zuweisen und anwenden • Ihre Server-Host-Authentifizierung mit automatisch verteilten öffentlichen Schlüsseln verwalten und automatisieren

Einblicke	Produktbeschreibung	Unterscheidungsmerkmale
CryptoAuditor™	Überwachung, Prüfung und Kontrolle von Benutzerzugriffsrechten in allen SSH,- RDP- und HTTP-Protokollen zentral, transparent und in Echtzeit	• Verteilte Inline-Verbindung mit minimal invasiver Implementierung: keine Änderungen der Benutzeroberflächen oder Anwendungen • Zentrale Speicherung von Audit Trails im verschlüsselten Format • Inhaltsbasierte Echtzeitbenachrichtigungen mit SIEM-Integration (SNMP/EMAIL) • IDS/DLP-Integration (ICAP) für Inhaltsanalyse und Befehls- und Datentransferverweigerung

SSH GERMANY

+49 621-78974610
Amselstraße 5
68307 Mannheim
Germany

EMEA (Die Zentrale)
+358 20 500 7000
Kornetintie
00380 Helsinki
Finland

AMERICAS
+1 781 247 2100
20 William Street, Suite G35
Wellesley, MA 02481
USA

APAC
+852 3602 3072
51/F Hopewell Centre
183 Queen's Road East
Wan Chai, Hong Kong