SSH Communications Security führt verschlüsselte Kanalüberwachung für die Cloud ein

Wir präsentieren die privilegierte Zugangsverwaltung und Überwachung für Amazon EC2 Cloud-Umgebungen

HELSINKI, 11. März. 2015 – Mit der rasanten Ausbreitung von Cloud-Diensten wird eine effektive Cloud-Sicherheit immer wichtiger. Daher hat SSH Communications Security heute für den CryptoAuditor neue Funktionen zur privilegierten Zugangsverwaltung (PAM) und zur Überwachung sensibler Datenbestände, die in der Cloud gespeichert sind, angekündigt. Bereits in diesem Monat beginnen die ersten Testläufe bei Kunden, die allgemeine Verfügbarkeit ist für April geplant. Für weitere Informationen besuchen Sie unsere Website unter: http://www.ssh.com/products/crypto-auditor.

CryptoAuditor gibt großen Unternehmen, insbesondere Finanzinstituten, und Behörden die Möglichkeit, privilegierten Zugang zu ihrem Datenbestand in der Cloud zu kontrollieren, und bietet:

- **Unterstützung für Amazon-Cloud:** Das Angebot beinhaltet die Bereitstellung für die Amazon Elastic Compute Cloud (EC2) als Amazon Machine Image (AMI) und wird zusätzlich auch im Amazon Web Services (AWS) Marketplace verfügbar sein.
- **Maßgeschneiderte Sicherheit für dynamische Umgebungen:** Aufgrund des netzwerkbasierten Inline-Konzepts und dem skalierbaren Bereitstellungsmodell ist CryptoAuditor optimal dafür geeignet, privilegierte Zugriffe in flexiblen Cloud-Umgebungen zu verwalten. Durch die verteilte, virtuelle Gerätearchitektur und die transparenten Überwachungsmöglichkeiten kann sich CryptoAuditor an dynamisch verändernde Netzwerke anpassen, ohne vorhandene Geschäftsprozesse oder Benutzererfahrungen zu stören.
- **Cloud-basiertes PAM:** Organisationen, die Amazon-Cloud-Dienste verwenden, können jetzt privilegierten Zugang zu Cloud-Umgebungen authentifizieren und überwachen sowie privilegierte Identitäten in der Cloud-Infrastruktur verwalten.
- **Schutz vor Datenausschleusung:** CryptoAuditor verhindert Datenverlust über jeglichen verschlüsselten Kanalverkehr hinweg und bietet transparente Echtzeit-Kapazitäten für Unternehmen, die sensible Informationen in die Cloud übertragen.
- **Verschlüsselte Datenüberwachung:** CryptoAuditor kann die Inhalte der häufigsten Datenübertragungsverschlüsselungsprotokolle, die in Unternehmensumgebungen für interaktive und automatisierte Sitzungen verwendet werden, abfangen, überwachen, aufnehmen und wiedergeben.

Matthew McKenna, COO, SSH Communications Security, sagt:
„Sicherheitsbedenken verhindern häufig immer noch die Migration zu Cloud-Diensten, trotz der eindeutigen geschäftlichen Vorteile in puncto Flexibilität und Kostenersparnissen, die die Cloud bieten kann. Verschlüsselte Kanäle sind für die Sicherung vertraulicher Informationen entscheidend, gleichzeitig ist aber auch die Gefahr gegeben, böswillige Aktivitäten im Netzwerk zu übersehen. SSH hat ein größeres Marktpotenzial bei der Bereitstellung von CryptoAuditor in behördlichen und gewerblichen Cloud-Umgebungen und bietet die einmalige Gelegenheit, verschlüsselte Kanäle über die Anwendungsschicht und die Cloudstack auf Betriebssystemebene transparent zu überwachen, zu prüfen und zu kontrollieren. Diese neue Version des CryptoAuditor gibt Organisationen, die Amazon EC2 verwenden, Kontrolle und Transparenz, ohne dass die Sicherheit ihrer verschlüsselten Kanäle gefährdet ist.“

SSH Communications Security
Als Erfinder des SSH-Protokolls sind wir seit 20 Jahren marktführend im Bereich Entwicklung fortschrittlicher Sicherheitslösungen, mit denen verschlüsselte Netzwerke möglich, überwacht und verwaltet werden. Über 3.000 Kunden weltweit vertrauen der Verschlüsselung, der Zugangskontrolle und den verschlüsselten Kanalüberwachungslösungen des Unternehmens, um komplexe Compliance-Anforderungen zu erfüllen, ihre Sicherheitslage zu verbessern und Betriebskosten einzusparen. SSH Communications Security hat seinen Hauptsitz in Helsinki sowie Niederlassungen in Nord- und Mittel- und Südamerika, Europa und Asien. Die Aktien des Unternehmens (SSH1V) werden an der NASDAQ OMX Helsinki notiert. Weitere Informationen zu SSH Communications Security erhalten Sie unter www.ssh.com

Kontaktinformationen:

Christian Kreß, General Manager, SSH Communications Security, Niederlassung Deutschland
+ 49/6122-92769-20
christian.kress@ssh.com