ssh communications security

CASE STUDY

HKU SPACE IMPROVES PRIVILEGED ACCESS MANAGEMENT

– CryptoAuditor Provides Immediate Visibility into Encrypted Privileged Access

Hong Kong's HKU SPACE is a leading tertiary educational organization. As an extension of the University of Hong Kong, HKU SPACE provides professional and continuing education services. HKU SPACE selected SSH Communication Security's CryptoAuditor for monitoring, controlling, and auditing the activities of privileged user access.

QUICK FACTS ABOUT HKU SPACE

- Customer Name: HKU School of Professional and Continuing Education (HKU SPACE)
- Industry: Educational Institution
- Employees: About 3,000 staff members and teachers
- URL: hkuspace.hku.hk

CHALLENGES

Like many educational organizations, HKU SPACE's IT infrastructure employs multiple operating systems including Linux, Windows, and various Unix systems. Though the deployed systems have been carefully prepared to be as secure as possible, it is important to manage the access control of privileged users to minimize security risks.

The administrators for each system (Unix and Linux root users, Windows administrators) have wide privileges for system-level access. These Power User accounts are remotely accessible with encrypted protocols such as SSH, RDP, SFTP and SSL. While encryption is an absolute necessity, it also includes a risk of an advanced attacker hiding its actions within the encrypted connection, and thus bypassing existing security solutions.

HKU SPACE had enabled root login over Secure Shell (SSH) and realized the potential risk and its impact. In the daily work, most of HKU SPACE staff is required to use shared privileged (root) accounts on the Linux hosts. The HKU SPACE also makes use of outsourced IT services.

Use of shared accounts and outsourced services has resulted in reduced visibility on privileged user activities, both for internal administrators and outsourced IT providers. Lack of visibility also means that, from a forensic analysis standpoint, there is no audit traces to examine in case of a data security breach.

SOLUTION

HKU SPACE understood that the lack of privileged access control puts the organization at risk. Their management required a solution to monitor, control, and audit the encrypted (SSH, RDP, SFTP and SSL) access to their systems. They wanted to prevent potential breaches and enable effective forensics should a breach happen.

HKU SPACE required a privileged access monitoring solution with:

- Full session recording with video replay and searchable audit trails.
- Transparent monitoring of encrypted privileged sessions (SSH, SFTP, RDP, SSL).
- Control over and visibility into third-party access in real time.
- An easy solution for shared use of privileged accounts.
- No changes to existing environment – no agents to install on endpoints and servers.
- Integration to their existing SSL VPN solution.
- Scalability and high-availability.

ADDITIONAL BENEFITS

CryptoAuditor allows HKU SPACE to monitor, control, and audit encrypted access by insiders and third-party contractors. Visibility and control enables effective management of their network. In addition to HKU SPACE's primary requirements, CryptoAuditor also delivers extra benefits such as:

- Rapid, straightforward deployment.
- Auditing the encrypted traffic on a need-to-know basis.
- Compliance with standards such as PCI DSS, SOX, HKMA, MAS.
- Empowering SIEM, DLP, IPS to stop malicious activity on the fly.
- Scalable, distributed cloud ready architecture.
- Enabling enforcement of smart card or other 2-factor authentication methods for privileged encrypted access.

Going forward, HKU SPACE is looking to further expand their privileged access control over different security zones with CryptoAuditor.

Network Environment