Executive Brief

VENAFI®

Health Care: 2017 SSH Study

Reveals widespread lack of security controls for SSH keys

How widespread is the exposure to SSH key compromise in the health care industry?

A November 2017 survey of over one hundred health care security professionals in the U.S., U.K. and Germany measured how well their organizations implement and manage security controls for SSH keys. The results show that most health care organizations are underprepared to protect against SSH-based attacks, with fewer than half following industry best practices for securing SSH keys.

Even though SSH keys are the credentials that provide the highest levels of privileged access, they are routinely untracked, unmanaged and unmonitored. In fact, most health care companies do not set policies and controls that limit how SSH keys can be used. This is particularly dangerous because SSH keys enable ongoing automatic connections from one system to another, often without the use of a second authentication factor. These connections create a persistent trust relationship—one that cyber criminals and malicious insiders are eager to access and misuse.

Only 8% of health care organizations have a complete and accurate inventory of SSH keys

Without a complete and accurate inventory, security teams in the health care industry cannot adequately protect the use of SSH for privileged administrative access. Simply put, they have no way of determining which keys are still active, who owns them or what they do. In the event of an intrusion, security teams can't isolate and remove compromised or out-of-date keys. Plus, they cannot ensure all access is revoked for employees who are terminated or reassigned.

47% do not adequately restrict the number of SSH administrators

Nearly half of health care companies, most or all administrators manage SSH keys for the systems they control. This results in unmonitored administrators who are empowered to generate and manage SSH keys across hundreds or thousands of systems. These administrators tend to use ad hoc processes and inconsistent security controls that leave health care companies without any inventory or regular review of their SSH trust relationships.

70% do not rotate SSH keys regularly

SSH keys do not expire and without regular SSH key rotation and revocation policies, health care organizations wind up with an unfettered web of trust relationships. Also, without life cycle policies that rotate SSH keys, existing weak, old, orphaned or unused keys live on perpetually, leaving health care organizations vulnerable to unauthorized privileged access by insiders, former employees and cyber criminals.

Most do not use two-factor authentication to protect SSH key usage

For SSH authentication, organizations use passwords, public keys or both. Although two-factor authentication is a best practice, 66% of health care companies do not apply this to SSH key users and 62% do not apply this to automated machine-to-machine communications. However, health care is the only industry surveyed (including financial services, government, retail, technology and health care) to apply two-factor authentication more frequently to automated machine-to-machine communications than SSH users.

Only 41% enforce policies that prohibit users from configuring their own SSH keys

While this is a strong start, half of health care organizations show weaker policy enforcement:

- 28% allow users to configure their own SSH keys
- 22% do not enforce policies that prohibit SSH users from configuring their own authorized keys

When SSH key configuration is left to each administrator's discretion, this results in inconsistent and potentially weak application of security controls. It is much more secure to have standardized security policies applied by a limited number of SSH key managers.

Over one-third do not enforce important limitations on how SSH keys are used

When poorly managed, SSH keys can be used to gain unauthorized privileged access. An improperly controlled SSH environment can be used to bypass security mechanisms—nullifying the use of SSH as a security protocol for important administrative tasks and machine-to-machine critical business functions. The study found that many health care companies are not following SSH security best practices:

- 40% do not limit port forwarding for SSH
- 37% do not limit the locations where authorized SSH keys can be used
- 33% do not remove SSH keys when users are reassigned or terminated

What are the best strategies for protecting SSH keys in health care organizations?

Adding a few simple best practices to your SSH management can radically reduce your exposure to SSH compromise. The following strategies will effectively secure privileged access across your organization:

- Limit the number and carefully monitor administrators who manage SSH for all systems
- Establish and enforce strict authentication, configuration and usage policies
- Reduce the risk of SSH key compromise with regular rotation and retirement practices
- Scan and monitor SSH-enabled systems for changes and anomalous usage, which can indicate a compromise

With the requirement to secure protected health information (PHI), it's critical for the health care industry to invest in SSH security and management. SSH best practices are not a one-time task, but ongoing security procedures that should be regularly audited, including a regular review of entitlements and trust relationships.

The Venafi Platform improves your SSH security with a centralized, complete and accurate view of your SSH key inventory. Enterprise-wide automation of the entire SSH key life cycle from issuance to decommissioning minimizes the risk of misuse. With Venafi, you can secure and control all SSH keys in your health care company for safe use of this security protocol and minimize your risk of unauthorized privileged access to critical systems and data.

ABOUT VENAFI

Venafi is the cybersecurity market leader in machine identity protection, securing the cryptographic keys and digital certificates on which every business and government depends to deliver safe machine-to-machine communication. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access.