ManageEngine
Key Manager Plus

The state of PKI (mis)management in enterprise IT

The proliferation problem

- **60%** of organizations house more than 10,000 digital keys and certificates, which are used to secure data and authenticate systems.
- **74%** of organizations don't know how many types of keys and certificates they possess.

Impact on service continuity

- **73%** of organizations have experienced unforeseen service outages at some point of time due to SSL/TLS certificate expiration.
- **55%** of organizations have experienced four or more certificate-related outages in the past two years alone.

"Key" role in compliance audits

- **75%** of enterprises state unenforced / undocumented key management practices are one of the top reasons for compliance audit failures.
- **67%** of organizations are enforcing additional layers of encryption in their IT operations to comply with industry regulations and IT policies.

2 TOP PRIORITIES

- Keeping track of the expiration dates of SSL/TLS certificates **(43%)**
- Reducing the use of unknown certificates **(40%)**

are two of the top four strategic priorities for digital security among enterprises.

Consequences of unenforced PKI management

The figures below represent an average of the number of times the following incidents have occurred over the past two years, because of improper key management practices.

- Failed compliance audits = **5.8**
- Exploitation of CA compromise for MITM & phishing attacks = **5.0**
- Server certificate and/or private key misuse = **4.9**
- Code signing certificate and/or key misuse = **4.7**
- Unforeseen service outages = **4.1**

Overall State

- Ability of enterprises to manage the growing number of keys and certificates (on a scale of 0 to 10)= **4.7** Clearly, a significant gap exists.

Addressing the gap: How to begin your certificate management journey?

- **Discover**
  Discover all SSL/TLS certificates deployed across your network.
- **Consolidate**
  Consolidate the discovered certificates in a secure, centralized repository.
- **Centralize**
  Inhibit certificate proliferation by centralizing their creation and deployment.
- **Automate**
  Streamline and automate the complete life cycle management of public certificates—right from CSR generation, provisioning, deployment, and renewal.
- **Scan**
  Scan and remediate SSL configuration vulnerabilities regularly, after certificates have been deployed.
- **Monitor**
  Set up the right type of alerting mechanism, paving the way for proactive certificate renewals well ahead of expiration.

Schedule a web consultation now

Source: Ponemon Institute, 2020