ManageEngine
Key Manager Plus

El estado del (mal) manejo de claves en TI empresarial

El problema de la proliferación

- **60%** de las organizaciones albergan a más de 10,000 claves y certificados digitales, que se utilizan para asegurar datos y autenticar sistemas
- El **74%** de las organizaciones no sabe cuántos tipos de llaves y certificados que poseen

Impacto en la continuidad del servicio

- El **73%** de las organizaciones han experimentado imprevistos. interrupciones del servicio en algún momento debido a Vencimiento del certificado SSL / TLS.
- **55%** de las organizaciones han experimentado cuatro o más interrupciones relacionadas con certificados solo en los últimos dos años.

Rol "clave" en auditorías de cumplimiento

- **75%** de las empresas declaran las prácticas de gestión de claves no mejoradas ni documentadas son una de las principales razones de fallas de auditoría de cumplimiento.
- **67%** de las organizaciones están aplicando capas adicionales de cifrado en sus operaciones de TI para cumplir con regulaciones de la industria y políticas de TI.

TOP 2 DE PRIORIDADES

- Seguimiento de las fechas de vencimiento de los certificados SSL / TLS **(43%)**
- Reducción del uso de certificados desconocidos **(40%)** on dos de las cuatro prioridades estratégicas principales para la seguridad digital entre las empresas.

Consecuencias de una gestión de claves no fortalecida

Las siguientes cifras representan un promedio de la cantidad de veces que los siguientes incidentes han ocurrido en los últimos dos años, debido a prácticas inadecuadas de gestión de claves.

- Auditorías de cumplimiento fallidas = **5.8**
- Explotación del compromiso de CA para MITM y ataques de phishing = **5.0**
- Mal uso de certificado de servidor y / o clave privada = **4.9**
- Mal uso de certificado de firma de código y / o clave = **4.7**
- Interrupciones imprevistas del servicio = **4.1**

Estado general

- Capacidad de las empresas para gestionar el crecimiento, cantidad de claves y certificados (en una escala de 0 a 10) **4.7** Claramente existe una brecha significativa.

Abordar la brecha: ¿Cómo comenzar su viaje de gestión de certificados?

Descubrir
Descubra todos los certificados SSL / TLS implementados en su red.

Consolidar
Consolide los certificados descubiertos en un repositorio seguro y centralizado.

Centralizar
Evitar la proliferación de certificados centralizando su creación y despliegue.

Automatizar
Agilice y automatice la gestión completa del ciclo de vida de los certificados públicos: directamente desde la generación, aprovisionamiento, implementación y renovación de CSR.

Escanear
Escanee y corrija las vulnerabilidades de configuración de SSL regularmente, después de que los certificados tengan sido desplegado.

Monitorear
Configure el tipo correcto de mecanismo de alerta, allanando el camino para un certificado proactivo de renovaciones mucho antes del vencimiento.

Programe una demo ahora

Fuente: Instituto Ponemon, 2020.