yubico

YubiHSM 2: protege las claves criptográficas

El YubiHSM 2 es un módulo de seguridad de hardware (HSM) dedicado que ofrece una protección superior contra el robo y el uso indebido de las claves privadas.

Las claves criptográficas almacenadas en software son vulnerables a las amenazas de seguridad

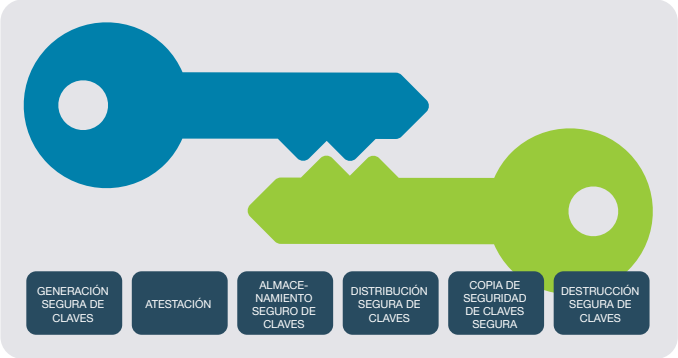
Las brechas de seguridad son un problema en aumento en todo el sector y que en 201 ya costó a las empresas una media de 3,8 millones de dólares por infracción[1]. El almacenamiento de software de claves criptográficas para servidores es cada vez más vulnerable a medida que los ataques se vuelven más sofisticados. El robo de claves criptográficas de un servidor puede causar una vulneración de seguridad grave. Por ejemplo, si se compromete una clave privada de una Autoridad de Certificación (CA), un atacante puede fingir que es su sitio web. Debido a los daños potenciales que provocan, que superan con creces a los de una infracción típica, como el cierre de todos los servidores, de los sistemas de los usuarios finales y del acceso de los usuarios durante días o semanas, lo que complica la recuperación, una seguridad sólida de las claves privadas criptográficas es más importante que nunca.

El YubiHSM 2 revoluciona la seguridad eficaz de claves criptográficas

Normalmente, las organizaciones han utilizado módulos de seguridad de hardware (HSM) que eran caros y difíciles de configurar. Sin embargo, con el YubiHSM 2, organizaciones de todos los tamaños pueden permitirse una seguridad de claves criptográficas eficaz, a lo largo de todo el ciclo de vida, en un factor de forma de hardware portátil y asequible. Con el YubiHSM 2, las empresas pueden evitar que los atacantes, el malware y el personal interno malicioso copien las claves criptográficas.

YubiHSM 2 ofrece una seguridad mejorada y una implementación práctica

El YubiHSM 2 ofrece una solución HSM asequible que permite una implementación sencilla además de un almacenamiento y un funcionamiento seguro de las claves. Las empresas pueden integrar rápidamente el YubiHSM 2 utilizando el SDK 2.0 de código abierto provisto por Yubico que ofrece los siguientes beneficios de seguridad:



Protección del ciclo de vida de la clave criptográfica

Protección mejorada para claves criptográficas

- Evitar la mala gestión de claves criptográficas: las claves criptográficas almacenadas en software se pueden copiar y son vulnerables a la distribución accidental. Si no se implementan procedimientos estrictos, es fácil para los administradores o cualquier personal interno malicioso copiar las claves en memorias USB con el fin de realizar copias de seguridad, enviarlas por ftp o compartirlas con otros a través de un servicio de almacenamiento en la nube. Una vez que esto sucede, las claves criptográficas pueden quedar olvidadas en una unidad USB o terminar almacenadas indefinidamente en un servicio o sistema externo. Las claves podrían incluso dejarse en la unidad de un servidor antiguo en espera de ser reciclado. El YubiHSM 2 basado en hardware ofrece una seguridad superior al evitar la copia y distribución accidental de claves criptográficas.
- Evitar el robo remoto de claves: las claves criptográficas almacenadas en software también son vulnerables al robo remoto. Los atacantes más sofisticados pueden obtener acceso de administrador o desplegar malware troyano que se instala en los servidores, busca claves criptográficas y luego las copia para su venta y distribución en sitios web oscuros como Alphabay. El almacenamiento de claves criptográficas en el YubiHSM 2 ofrece una seguridad superior basada en hardware y evita que el malware y los atacantes remotos puedan extraer las claves privadas.

[1] 2018 Cost of Data Breach Study (Estudio del coste de las infracciones de datos en 2018), Informe de investigación del Ponemon Institute

Rápida integración con seguridad fuerte de claves basada en hardware

- Obtener una completa caja de herramientas criptográficas: con el YubiHSM 2 SDK, los desarrolladores pueden integrar la compatibilidad del YubiHSM 2 en los productos y servicios que se estén desarollando. El YubiHSM 2 SDK da vida a las capacidades del YubiHSM 2, como la generación e importación de claves, la firma y verificación, y el cifrado y descifrado de datos para aplicaciones de código abierto y comerciales que abarcan muchos productos y servicios diferentes. Los casos de uso más comunes implican el procesamiento basado en hardware en chip para la generación y verificación de firmas.
- Compatibilidad con PKCS#11: gracias al YubiHSM 2 SDK, los desarrolladores pueden hacer que las características del YubiHSM 2 sean fácilmente accesibles a través del estándar del sector PKCS#11. Dado que la mayoría del software de autoridad de certificación comercial utiliza PKCS#11 para acceder a la clave de firma de la CA o para inscribir certificados de usuario, la compatibilidad con PKCS#11 permite a las organizaciones abordar los tipos de uso que tienen este requisito.

Implementación práctica y simplificada para organizaciones de todos los tamaños

- Protección de nivel empresarial en un factor de forma portátil y asequible: los HSM tradicionales montados en bastidor y basados en tarjetas no son precisamente lo más práctico para muchas organizaciones, debido a los problemas que presenta la complejidad de su implementación o su coste. Además, el espacio de bastidor en los centros de datos compartidos suele incluir recintos físicos para servidores con puertas de malla metálica para asegurar el acceso. Al ser el HSM más pequeño del mundo, el YubiHSM 2 encaja fácilmente en una ranura USB frontal de los servidores y se coloca casi a ras para adaptarse a estos recintos de seguridad físicos. Además, se puede implementar en cuestión de horas, no en días.

Abordar tipos de uso existentes y emergentes

Intercambios seguros de criptomoneda: el gasto global en soluciones de blockchain está previsto que sea de 15.900 millones de dólares en 2023, según la consultora IDC. Con este crecimiento tan explosivo también hay un alto volumen de activos que necesitan protección para mitigar los riesgos de seguridad emergentes. Varios han sufrido ataques, y este número aumenta constantemente. Sin embargo, todos podrían haberse evitado con un enfoque de seguridad basado en prácticas recomendadas que incluyan un módulo de seguridad de hardware. Con el YubiHSM 2 SDK, los desarrolladores que generan soluciones para intercambios de criptomoneda pueden integrar rápidamente el YubiHSM 2 para proteger las claves criptográficas y mantener segura la información financiera confidencial.

Entornos seguros de Internet de las cosas (IoT): el Internet de las cosas (IoT) es un área que está emergiendo rápidamente y en la que los sistemas operan a menudo en entornos hostiles. Esto hace que la seguridad de las claves criptográficas sea aún más importante, ya que las organizaciones necesitan proteger la información confidencial. Las claves criptográficas se utilizan en muchas aplicaciones de IoT, pero con una seguridad insuficiente. Esto se debe en parte a que la protección de las claves criptográficas y el registro de los certificados en las pasarelas o proxies de IoT ha sido complicado, y los HSM tradicionales son demasiado grandes y poco manejables para ciertos entornos de IoT, como por ejemplo los coches conectados. Con el SDK de código abierto, los desarrolladores que crean aplicaciones de IoT pueden integrarlas rápidamente con el ultraportátil YubiHSM 2 para proteger las claves criptográficas y evitar que los entornos críticos de IoT sean víctimas de ataques hostiles.

Servicios seguros en la nube: una seguridad fuerte para los entornos de la nube es fundamental, ya que las organizaciones necesitan garantizar que sus datos se mantendrán seguros en la nube. El YubiHSM 2 puede implementarse en un centro de datos y ejecutarse como un componente de una infraestructura de nube. Las organizaciones pueden estar tranquilas sabiendo que el servicio de alojamiento en la nube de su elección utiliza el YubiHSM 2 como parte de su solución.

Servicios de certificados seguros de Microsoft Active Directory: el YubiHSM 2 puede proporcionar claves respaldadas por hardware para la implementación de PKI basada en Microsoft de una organización. La implementación de YubiHSM 2 en Microsoft Active Directory no solo protege las claves privadas de la Autoridad de Certificación, sino que también protege todos los servicios de firma y verificación que utilizan la clave privada.

Resumen

El YubiHSM 2 permite a organizaciones de todos los tamaños mejorar la seguridad de las claves criptográficas a lo largo de todo el ciclo de vida, reducir el riesgo y garantizar el cumplimiento de las normativas vigentes. Con el YubiHSM SDK 2.0 disponible como código abierto, las organizaciones pueden integrar de forma fácil y rápida la compatibilidad con YubiHSM 2 en una amplia gama de plataformas y sistemas para tipos de uso existentes y emergentes en los que una seguridad fuerte es más importante que nunca.

[2] https://www.smartcard-hsm.com/2017/02/14/IoT_Devices_with_SmartCard-HSM.html
[3] Note: Todos los aspectos del YubiHSM 2 SDK 2.0 están disponibles como código abierto, excepto el proveedor de almacenamiento de claves (KSP) para su uso con los Servicios de certificados de Microsoft Active Directory.

Yubico AB
Kungsgatan 44
2 ° piso
SE-111 35 Estocolmo
Suecia

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 EE. UU.
844-205-6787 (número gratuito)
650-285-0088