yubico

Protección segura basada en hardware para claves criptográficas con YubiHSM 2

YubiHSM 2 garantiza seguridad criptográfica basada en hardware para aplicaciones, servidores y dispositivos informáticos a una fracción del costo y tamaño de los HSM tradicionales.

Llaves criptográficas almacenadas en el software son vulnerables a las amenazas

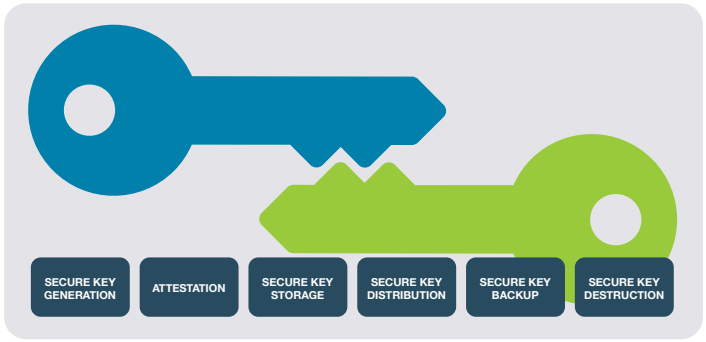
Las violaciones de seguridad son un problema creciente en toda la industria que en 2019 costó a las empresas un promedio de $ 8.9 millones por incidente[1]. El almacenamiento en software de claves criptográficas para servidores es cada vez más vulnerable a medida que los ataques se vuelven más sofisticados. Por ejemplo, si una clave privada se ve comprometida por una Autoridad de Certificación (CA), un atacante puede simularr ser su sitio web.

La YubiHSM 2 cambia el juego para una efectiva seguridad de clave

LaYubiHSM 2 garantiza el almacenamiento seguro de claves criptográficas en hardware y operaciones para aplicaciones, servidores y dispositivos informáticos al tiempo que elimina el costo y la complejidad de los módulos de seguridad de hardware (HSMs) tradicionales. Es resistente a la manipulación y ofrece bajo costo y un ROI de alta seguridad en un formato “nano” portátil que permite un uso flexible en diversos dispositivos y ubicaciones. Con el YubiHSM 2, las organizaciones pueden evitar que los atacantes, el malware y los intrusos maliciosos copien las claves criptográficas. Las empresas pueden integrarse rápidamente al YubiHSM 2 utilizando el SDK 2.0 de código abierto.

Protección segura basada en hardware para claves criptográficas

Las claves criptográficas almacenadas en software se pueden copiar, y son vulnerables a la distribución accidental y al robo en forma remota. Sin procedimientos estrictos, es fácil para los administradores o expertos maliciosos hacer una copia de las claves en unidades USB, enviarlas por FTP o compartirlas con otros a través de un servicio de almacenamiento en la nube. Además, los atacantes sofisticados pueden obtener acceso de administrador o implementar malware troyano que se instala en servidores, busca claves criptográficas y luego las copia para su venta en sitios de la “web oscura” como Alphabay.



Asegurando el ciclo de vida de las claves criptográficas

La YubiHSM 2 basada en hardware permite el almacenamiento y operación seguro de claves y al evitar la copia y distribución accidental de claves, previniendo el robo remoto de claves almacenadas.

- Almacenamiento y operaciones seguras de claves en hardware resistente a la manipulación, con registro de auditoría.
- Amplias capacidades criptográficas que incluyen hash, ajuste de clave, firma asimétrica, descifrado, certificación y más.

Diseño innovador par aun uso flexible

Los HSMs tradicionales montados en racks y basados en tarjetas no son prácticos para muchas organizaciones debido a problemas que ocasiona el tamaño y la complejidad de implementación del HSM. Además, el espacio en rack en los centros de datos compartidos a menudo incluye gabinetes de servidores físicos con puertas de malla metálica para asegurar el acceso y restringir el espacio disponible.

Con la YubiHSM 2, las organizaciones pueden proteger fácilmente servidores, aplicaciones, bases de datos, líneas de ensamblaje, dispositivos IoT, intercambios de criptomonedas etc. con una llave portátil en formato “nano” que permite una implementación rápida y flexible en diversos entornos.

[1] 2019 Cost of Data Breach Study, Ponemon Institute Research Report

Se adapta fácilmente a un puerto USB y se ubica casi imperceptible para acomodar gabinetes de seguridad física.

- El formato “nano” permite una implementacion flexibley uso en diferentes dispositivos y lugares
- Implementación en puerto USB-A completamente oculto
- Compartible en red para uso de aplicaciones en otros servidores

Bajo costo, ROI de alta seguridad

Las claves criptográficas almacenadas en el software son susceptibles a hackers y a ataques de malware. Además, los HSM tradicionales pueden ser costosos de implementar.

Con la YubiHSM 2, las organizaciones obtienen seguridad criptográfica y operaciones de alto nivel empresarial sin el precio tradicional de HSM.

- Significativa reducción de Capex: hasta 90% más económico que los HSMs tradicionales
- Dispositivo de bajo consumo reduce el consumo de energía de la empresa

Integración rápida, fácil administración

Con el SDK de YubiHSM 2, los desarrolladores pueden integrar rápidamente el soporte para YubiHSM 2 en productos y aplicaciones con capacidades como generar e importar claves, firma y verificación, y cifrado / descifrado de datos. Los desarrolladores también pueden hacer que estas funciones sean accesibles a través del estándar de la industria PKCS # 1.

- Soporte de aplicaciones personalizadas utilizando bibliotecas de código abierto. Interfaces a través de YubiHSM KSP, PKCS # 11 y bibliotecas nativas.
- La administración remota reduce la complejidad de gestión y los costos.

Abordardando casos de uso existentes y emergentes

Asegurar intercambios de criptomonedas: El mercado de criptomonedas está creciendo rápidamente, con un alto volumen de activos que necesitan protección contra los riesgos de seguridad emergentes. Algunos intercambios han sido violados, se podrían haber evitado con un enfoque de seguridad de mejores prácticas que involucra un módulo de seguridad de hardware (HSM). Con el SDK de YubiHSM 2, los desarrolladores que crean soluciones para intercambios de criptomonedas 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 donde los sistemas a menudo operan en entornos hostiles. Las claves criptográficas se utilizan en numerosas aplicaciones de IoT, con una seguridad insuficiente. Esto se debe en parte a que proteger las claves criptográficas y registrar certificados en las puertas de enlace o servidores proxy de IoT ha sido complicado, y los HSM tradicionales son demasiado grandes y difíciles de manejar para ciertos entornos de IoT, como los automóviles conectados. Con el SDK de código abierto, los desarrolladores que crean aplicaciones de IoT pueden integrarse rápidamente con el YubiHSM 2 ultra portátil para proteger las claves criptográficas y evitar que los entornos críticos de IoT sean víctimas de tomas de control hostiles.

Asegurar Servicios en la nube: Es fundamental contar con una seguridad robusta para los entornos en la nube, ya que las organizaciones deben garantizar que sus datos se mantengan seguros en la nube. El YubiHSM 2 puede implementarse en un centro de datos y ejecutarse como un componente de una infraestructura en la nube. Las organizaciones pueden estar tranquilas sabiendo que el servicio de alojamiento en la nube de su elección está ejecutando el YubiHSM 2 como parte de su oferta.

Asegurar Servicios de Microsoft Active Directory Certificate: La YubiHSM 2 puede proporcionar claves respaldadas por hardware para la implementación de PKI en una organización basada en Microsoft. La implementación de YubiHSM 2 en los servicios de Microsoft Active Directory Certificate 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.

En resumen

La YubiHSM 2 permite que organizaciones de cualquier tamaño mejoren la seguridad de la clave criptográfica durante todo el ciclo de vida, reduzcan el riesgo y garanticen el cumplimiento de las normas. Con la YubiHSM SDK 2.0 disponible como código abierto, las organizaciones pueden integrar fácil y rápidamente el soporte para el YubiHSM 2 en una amplia gama de plataformas y sistemas para casos de uso existentes y emergentes donde una seguridad robusta es más crítica que nunca.

Representante en Paraguay:
ProActive Consulting
Juan B. Rivarola Matto 6237 c/ R.I.2 Ytororo
Teléfono 0981-478-921
Email: yubikey@proactive.consulting
www.proactive.consulting

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 USA
844-205-6787 (toll free)
650-285-0088