yubico

YubiHSM 2 – Sichert kryptografische Schlüssel

Das YubiHSM 2 ist ein dediziertes Hardwaresicherheitsmodul (HSM) für hervorragenden Schutz privater Schlüssel vor Diebstahl und Missbrauch.

In Software gespeicherte kryptografische Schlüssel sind gegenüber Bedrohungen anfällig

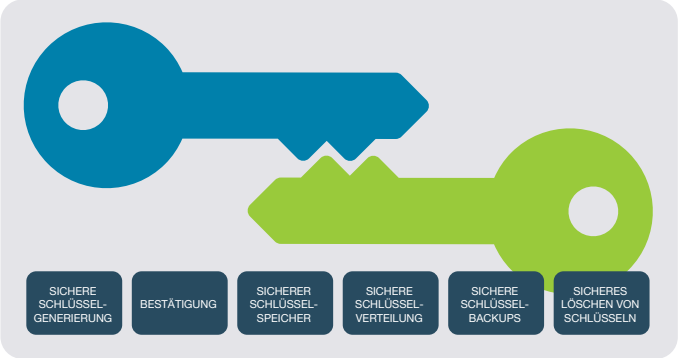
Sicherheitsverletzungen sind ein zunehmendes, branchenweites Problem, das Unternehmen 2018 im Schnitt 3,8 Millionen US-Dollar pro Datenleck gekostet hat[1]. Die Speicherung kryptografischer Schlüssel für Server in Software wird immer anfälliger für immer ausgefeiltere Angriffe. Der Diebstahl kryptografischer Schlüssel von einem Server kann ein katastrophales Datenleck zur Folge haben. Wenn beispielsweise ein privater Schlüssel von einer Zertifizierungsstelle kompromittiert wurde, kann ein Angreifer sich als Ihre Website ausgeben. Bei den potenziellen enormen Schäden dieser Art von Datenverletzung, bei der alle Server und Endbenutzersysteme heruntergefahren werden müssen und der Benutzerzugriff über Tage oder Wochen hinweg eingeschränkt ist, ist höchste Sicherheit für kryptografische private Schlüssel wichtiger als je zuvor.

Das YubiHSM 2 setzt einen neuen Maßstab für effektive Schlüsselsicherheit

Bisher haben Organisationen Hardwaresicherheitsmodule (HSMs) eingesetzt, die mit kostspieliger und komplexer Einrichtung verbunden waren. Mit dem YubiHSM 2 können allerdings Unternehmen aller Größenordnungen für effektive Sicherheit für kryptografische Schlüssel im gesamten Lebenszyklus sorgen, mit einem tragbaren und erschwinglichen Formfaktor. Mit dem YubiHSM 2 können Unternehmen verhindern, dass kryptografische Schlüssel von Angreifern, Malware oder böswilligen Insidern kopiert werden.

Verbesserte Sicherheit und praktische Bereitstellung mit YubiHSM 2

Das YubiHSM 2 bietet eine kostengünstige HSM-Lösung um kritische Schlüssel sicher zu speichern, sie unkompliziert zur Verfügung zu stellen und in einer sicheren Umgebung zu nutzen. Unternehmen können dank des Open-Source-SDK 2.0 eine schnelle Integration des YubiHSM2 mit den eignen Diensten erreichen und dadurch von den folgenden Sicherheitsvorteilen profitieren :



Schutz kryptografischer Schlüssel über den gesamten Lebenszyklus der Schlüssel

Verbesserter Schutz für kryptografische Schlüssel

- Mangelhaften Umgang mit kryptografischen Schlüsseln verhindern: In Software gespeicherte kryptografische Schlüssel können kopiert oder versehentlich verteilt werden. Administratoren oder böswillige Insider könnten solche Software-Schlüssel zu Backupzwecken in USB-Laufwerke kopieren, per FTP versenden oder über einen Cloud-Speicherservice mit anderen teilen. Anschließend können die kryptografischen Schlüssel auf dem USB-Laufwerk vergessen oder für unbegrenzte Zeit in einem externen Service oder System gespeichert werden. Die Schlüssel könnten sogar auf dem Laufwerk eines alten Servers verbleiben, der zum Recycling vorgesehen ist. Das hardwarebasierte YubiHSM 2 liefert hervorragende Sicherheit, indem es das versehentliche Kopieren und Verteilen von kryptografischen Schlüsseln verhindert.
- Remote-Diebstahl von Schlüsseln verhindern: In Software gespeicherte kryptografische Schlüssel sind auch anfällig gegenüber Diebstahl aus der Ferne. Erfahrene Angreifer, die sich administrativen Zugriff verschafft haben oder einen Trojaner bereitgestellt haben, der auf Servern installiert wird und dort nach kryptografischen Schlüsseln sucht. So können diese Schlüssel dann kopiert werden um sie auf Sites im Dark Web wie Alphabay zu verkaufen und zu verteilen. Die Speicherung kryptografischer Schlüssel im YubiHSM 2 bietet hervorragende hardwarebasierte Sicherheit und verhindert, dass Malware oder Angreifer aus der Ferne die privaten Schlüssel extrahieren können.

[1] 2018 Cost of Data Breach Study, Forschungsbericht des Ponemon Institute

Schnelle Integration in hardwarebasierte hohe Schlüsselsicherheit

- Umfangreiche kryptografische Tools nutzen: Mit dem YubiHSM 2-SDK können Entwickler schnell Unterstützung für das YubiHSM 2 in die zu erstellenden Produkte und Services implementieren. Das YubiHSM 2-SDK erweitert die Funktionen des YubiHSM 2, wie das Generieren und Importieren von Schlüsseln, digitale Signaturen und Verifizierung solcher Signaturen sowie die Ver- und Entschlüsselung von Daten in Open-Source- und kommerziellen Anwendungen für viele verschiedene Produkte und Services. Die meisten Anwendungsfälle umfassen die hardwarebasierte Verarbeitung auf dem Chip für Signaturgenerierung und -verifizierung.
- Unterstützung für PKCS#11: Mit dem YubiHSM 2-SDK können Entwickler die Funktionen des YubiHSM 2 ganz einfach über den Branchenstandard PKCS#11 zugänglich machen. Da der Großteil der kommerziellen Zertifizierungsstellensoftware PKCS #11 für den Zugriff auf den Signaturschlüssel der Zertifizierungsstelle oder zum Registrieren von Benutzerzertifikaten verwendet, können Organisationen mit der PKCS#11 Schnittstelle die solche Anwendungsfälle einfach abdecken.

Praktische und vereinfachte Bereitstellung für Unternehmen aller Größenordnungen

- Unternehmensgerechter Schutz in einem tragbaren und erschwinglichen Formfaktor: Traditionelle 19-Zoll- und PCIe HSMs eignen sich aufgrund der Bereitstellungskomplexität oder Kosten des HSM für viele Unternehmen nicht. Darüber hinaus umfasst der Rackplatz in gemeinsamen Rechenzentren häufig physische Servergehäuse mit Metallgittertüren zum Sichern des Zugangs. Als das weltweit kleinste HSM passt das YubiHSM 2 einfach in den internen USB-Steckplatz in Servern ist so sicher aufbewahrt. Zudem kann es innerhalb von Stunden anstelle von Tagen bereitgestellt werden.

Abdeckung aktueller und zukünftiger Anwendungsfälle

Sicherer Umtausch von Kryptowährungen:
Der Kryptowährungsmarkt verzeichnet ein rasantes Wachstum und erreicht 2018 voraussichtlich einen Marktwert in Höhe von 1 Milliarde US-Dollar. Dieses enorme Wachstum ist auch mit zahlreichen Assets verbunden, die vor Sicherheitsrisiken geschützt werden müssen. Bei mehreren Kryptowährungsbörsen ist es zu Datenlecks gekommen. Diese Datenlecks nehmen stets zu und hätten allesamt möglicherweise mit einem Best Practice-Sicherheitsansatz unter Beteiligung eines Hardwaresicherheitsmoduls verhindert werden können. Mit dem YubiHSM 2-SDK können Entwickler von Lösungen für Kryptowährungsbörsen das YubiHSM 2 schnell integrieren, um kryptografische Schlüssel und sensible Finanzdaten zu schützen.

Sichere Internet of Things-(IoT-)Umgebungen: Das Internet der Dinge (Internet of Things, IoT) ist ebenfalls ein schnell wachsender Markt, in dem Systeme oft in gefährdeten Umgebungen betrieben werden. Dabei ist die Sicherung kryptografischer Schlüssel noch wichtiger, da Unternehmen sensible Informationen schützen müssen. Kryptografische Schlüssel werden in zahlreichen IoT-Anwendungen mit nur unzureichenden Sicherheitsmaßnahmen verwendet. Das ist teilweise darauf zurückzuführen, dass der Schutz kryptografischer Schlüssel und die Registrierung von Zertifikaten bei IoT-Gateways oder -Proxys bisher kompliziert waren und traditionelle HSMs zu groß und sperrig für bestimmte IoT-Umgebungen wie vernetzte Autos sind. Mit dem Open-Source-SDK können Entwickler von IoT-Anwendungen das tragbare YubiHSM 2 schnell integrieren, um kryptografische Schlüssel zu schützen und die feindliche Übernahme kritischer IoT-Umgebungen zu verhindern.

Sichere Cloud-Services: Hohe Sicherheit für Cloud-Umgebungen ist unerlässlich, da Organisationen sicherstellen müssen, dass ihre Daten in der Cloud geschützt werden. Das YubiHSM 2 kann in einem Rechenzentrum bereitgestellt und als Komponente einer Cloud-Infrastruktur eingesetzt werden. Unternehmen können sich entspannt zurücklehnen, wenn ihr Cloud-Serviceanbieter das YubiHSM 2 im Rahmen seines Angebots verwendet.

Sichere Microsoft Active Directory-Zertifikatdienste:
Das YubiHSM 2 kann kryptografische Schlüssel für die Microsoft-basierte PKI-Implementierung eines Unternehmens sicher bereitstellen. Das YubiHSM 2 für Microsoft Active Directory Zertifikatsservices schützt dabei nicht nur die privaten Schlüssel der Zertifizierungsstelle, sondern auch alle Signatur- und Verifizierungvorgänge die den privaten Schlüssel nutzen.

Zusammenfassung

Mit dem YubiHSM 2 können Unternehmen aller Größenordnungen die Sicherheit kryptografischer Schlüssel im gesamten Lebenszyklus verbessern, Risiken mindern und die Einhaltung gesetzlicher Vorschriften sicherstellen. Mit dem als Open-Source-SDK verfügbaren YubiHSM SDK 2.0 können Unternehmen Unterstützung für das YubiHSM 2 einfach und schnell in zahlreiche Plattformen und Systeme integrieren, und zwar für aktuelle und zukünftige Anwendungsfälle mit höchsten Sicherheitsanforderungen.

[2] https://www.smartcard-hsm.com/2017/02/14/IoT_Devices_with_SmartCard-HSM.html
[3] Hinweis: Alle Aspekte des YubiHSM 2 SDK 2.0 sind als Open-Source-Elemente verfügbar, mit Ausnahme des Key Storage Provider (KSP) für Microsoft Active Directory-Zertifikatdienste

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

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