yubico

YubiHSM 2 - säkrar krypteringsnycklar

YubiHSM 2 är en dedikerad säkerhetsmodul (Hardware Security Module) som erbjuder skydd för privata nycklar mot stöld och missbruk.

Krypteringsnycklar som lagras i mjukvara är sårbara inför hot

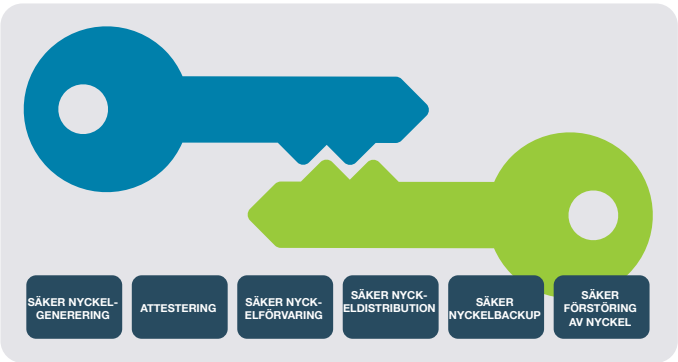
Säkerhetsöverträdelser har blivit ett allt större problem som under 2018 kostade företag i genomsnitt 3,8 miljoner USD per överträdelse[1]. Mjukvarulagring av krypteringsnycklar för servrar blir mer sårbara eftersom attackerna blir alltmer sofistikerade. Stulna krypteringsnycklar från en server kan leda till katastrofala säkerhetsföljder. Exempelvis om en privat nyckel stjäls från en certifikatutfärdare kan attackeraren låtsas att vara din webbplats. Med potentiella skador som långt överstiger en vanlig överträdelse, krävs avstängning av alla servrar, slutanvändarsystem och användaråtkomst under många dagar eller veckor. Det komplicerar återhämtningen för den eller de som råkar ut för attacken, och gör att stark säkerhet för privata krypteringsnycklar är viktigare än någonsin.

YubiHSM 2 ger effektivt skydd för privata nycklar

Företag har länge använt Hardware Security Modules (HSM) som både är dyra och svåra att installera. Men med YubiHSM 2 kan företag i alla storlekar effektivt öka säkerheten för privata krypteringsnycklar i en bärbar och prisvärd utformning. YubiHSM 2 ger företag möjlighet att förhindra otillåten kopiering av krypteringsnycklar, samt förhindrar skadlig programvara och farliga insiders.

YubiHSM 2 erbjuder säker miljö och enkel installation

YubiHSM 2 erbjuder en kostnadseffektiv HSM-lösning som är enkel att använda och ger säker lagring av krypteringsnycklar. Företag kan snabbt integrera med YubiHSM 2 med hjälp av SDK 2.0 som ger följande säkerhetsfördelar:



Säkrar livscykeln för krypteringsnyckeln

Ökat skydd av krypteringsnycklar

- **Förhindrar slarvig hantering av krypteringsnycklar:** krypteringsnycklar som lagras i programvara kan kopieras och är sårbar för oavsiktlig distribution. Utan strikta procedurer är det enkelt för administratörer eller farliga insiders att kopiera nycklarna till USB-flashminne för säkerhetskopieringsändamål, ladda upp till ftp eller dela med andra via en molnlagringstjänst. YubiHSM 2 förhindrar detta. När detta har hänt kan krypteringsnycklarna glömmas kvar på en USB-enhet eller hamna i en extern tjänst eller ett system. Nycklarna kan till och med lämnas kvar på hårddisken på en gammal server som ska återvinnas. Hårdvarubaserade YubiHSM 2 erbjuder överlägsen säkerhet genom att förhindra kopiering och distribuering av krypteringsnycklar.
- **Förhindra fjärrstöld av nycklar:** Krypteringsnycklar som lagras i programvara är också sårbara för fjärrstölder. Sofistikerade angripare kan få administratörsåtkomst eller installera trojaner på servrar, söker efter krypteringsnycklar och kopierar dem sedan för försäljning och distribution på Dark Web, exempelvis Alphabay. Sparar du krypteringsnycklar i YubiHSM 2 får du överlägsen hårdvarubaserad säkerhet och eliminerar skadlig programvara och fjärrattacker från att kunna hämta de privata nycklarna.

[1] 2018 Cost of Data Breach Study, Ponemon Institute Research Report

Snabb integration med hårdvarustödd säkerhetslösning

- **Du får en omfattande kryptografisk verktygslåda:** Med YubiHSM 2 SDK kan utvecklare snabbt integrera support för YubiHSM 2 i de produkter och tjänster som byggs. YubiHSM 2 SDK kommer att liva upp funktionerna i YubiHSM 2 som att generera och importera nycklar, signera, verifiera, kryptera och dekryptera data för öppen källkod och kommersiella applikationer. Detta gäller för många olika produkter och tjänster. Vanligtvis används hårdvarubaserad bearbetning på chip för signaturgenerering och verifiering.
- **Support för PKCS#11:** Med hjälp av YubiHSM 2 SDK kan utvecklare enkelt göra YubiHSM 2-funktioner tillgängliga genom industristandard PKCS # 11. Eftersom de flesta certifikatutfärdare av kommersiell programvara använder PKCS # 11 för att komma åt certifikatutfärdarens signeringsnyckel eller för att registrera användarcertifikat, möjliggör stöd av PKCS # 11 att företag kan hantera användare som har detta krav.

Praktisk och enkel implementering för företag i alla storlekar

- **Säker företagslösning i bärbar och prisvärd utformning.:** Traditionella rackmonterade och kortbaserade HSM är inte praktiskt för många företag på grund av komplex HSM-installation eller höga kostnader. Dessutom innebär rackutrymme i delade datacenter ofta fysiska serverskal med metalldörrar för att försäkra säker åtkomst. Som världens minsta HSM passar YubiHSM 2 enkelt in i en USB-port på framsidan och ligger nästan i nivå för att tillgodose dessa fysiska säkerhetsdörrar och kan installeras under några timmar istället för dagar.

Riktar in sig på befintliga och ökande användarfall

Säkert utbyte av kryptovaluta: Marknaden för kryptovaluta växer snabbt och förväntas nå 1 biljon dollar. Med denna explosiva tillväxt kommer också en hög volym tillgångar som behöver skydd för att minska nya säkerhetsrisker. Det har förekommit brott mot flera transaktioner och antalet växer stadigt. Dessa skulle kunna ha förhindrats med säkerhetsmetod som involverar en hårdvarusäkerhetsmodul. Med YubiHSM 2 SDK kan utvecklare som bygger lösningar för kryptovalutatransaktioner snabbt integrera YubiHSM 2 för att skydda krypteringsnycklar och hålla känslig ekonomisk information säker.

Säkra Internet of Things (IoT) : IoT (Internet of Things) utvecklas snabbt där system ofta arbetar i fientliga miljöer. Det gör att krypteringsnycklar blir ännu viktigare eftersom organisationer behöver skydda känslig information. Krypteringsnycklar används i flera IoT-applikationer med otillräcklig säkerhet. Detta beror delvis på att det har varit komplicerat att skydda krypteringsnycklar och registrera certifikat på IoT-gateways eller proxyservrar och traditionella HSM:er är för stora och olämpliga för vissa IoT-miljöer, t.ex. anslutna bilar. Med SDK kan utvecklare som bygger IoT-applikationer snabbt skapa integration med den ultraportabla YubiHSM 2. Detta med målet att skydda krypteringsnycklar samt hindra att kritiska IoT-miljöer faller offer för fientliga övertaganden.

Säkra molntjänster: Stark säkerhet för molnmiljöer är avgörande eftersom företag måste se till att deras data förvaras säkert i molnet. YubiHSM 2 kan distribueras i ett datacenter och köras som en del av en molninfrastruktur. Du och ditt företag kan luta er tillbaka tack vare vetskapen om att molntjänsterna kör YubiHSM 2.

Säkra Microsoft Active Directory Certificate-tjänster: YubiHSM 2 kan erbjuda säkerhetskopierade nycklar för ett företags Microsoft-baserade PKI-implementering. Installera YubiHSM 2 i Microsoft Active Directory Certificate-tjänsterna skyddar inte bara certifikatutfärdarens privata nycklar utan skyddar också all signering och verifiering vid användning av den privata nyckeln.

Sammanfattning

YubiHSM 2 gör det möjligt för företag av alla storlekar att förbättra säkerheten för krypteringsnycklar under hela livscykeln, minska risken och säkerställa att reglerna följs. Med YubiHSM SDK 2.0 som öppen källkod kan ditt företag enkelt och snabbt integrera stöd för YubiHSM 2. Självklart fungerar det på ett brett utbud av plattformar och system för att se till att ditt företag är så säkert det bara går – och att ni är i trygga händer.

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 (utan extra avgift)
650-285-0088

[2] https://www.smartcard-hsm.com/2017/02/14/IoT_Devices_with_SmartCard-HSM.html [3] Note: Alla delar av YubiHSM 2 SDK 2.0 är tillgängliga som öppen källkod förutom Key Storage Provider (KSP) för användning med Microsoft Active Directory Certificate Services