



Automatizace správy klíčů s HSM Luna

Že je třeba občas měnit šifrovací klíče pro přenos a uchování citlivých dat, ví každý. Ale ruční změna hesel a klíčů včetně jejich distribuce je časově náročná a hrozí při ní riziko lidské chyby. Proč to nedělat centrálně a automaticky?

NÁROKY NA IT BEZPEČNOST ROSTOU

Pro většinu IT profesionálů na celém světě je bezpečnost jejich infrastruktury a dat, která v ní kolují, úkol číslo jedna. Nejde jen o legislativní požadavky typu GDPR, kdy hrozí firmám a organizacím až likvidační pokuty. **Citlivé informace tvoří často základ hodnoty firmy** a jejich krádež ji tak většinou zásadním způsobem postihne.

CENTRALIZUJTE A AUTOMATIZUJTE

praxe vychází, že šifrovací klíče je vhodné měnit jednou za šest měsíců. Každá taková změna je kritický bod ve fungování IT infrastruktury. Místo najmutí většího počtu drahých IT specialistů, lze využít pro správu a distribuci šifrovacích klíčů automatizovaného a centralizovaného řešení Luna HA cluster. **Stačí nastavit bezpečnostní strategii a nechat cluster pracovat.**

Šifrovací klíče jsou změněny jednou osobou na jednom centrálním místě a v rámci HA clusteru jsou **automaticky distribuovány** do jednotlivých částí sítě. Po uplynutí doby archivace dat je jednoduše v Luně změněn klíč k zálohovaným datům a **zálohovací disky je tak možné vyřadit** bez jejich mazání nebo fyzické likvidace. Zašifrovaná data na nich již nelze obnovit.

Luna též může **potvrdit dobu vzniku určitého záznamu**, například data o průjezdu kamionu mýtnou branou nebo čas fotografie z bezpečnostní kamery.

ON-SITE NEBO V CLOUDU

Centralizovanou a automatizovanou správu klíčů s pomocí Luny lze provozovat jak na vlastní infrastruktuře firmy nebo i v hostingů. Pro méně náročné aplikace se dá **kapacita jedné Luny sdílet** pomocí hostingů mezi řadou jednotlivých uživatelů.

Pokud firma ukládá svá data do cloudu, nemusí se bát jejich zneužití, a to ani v případě, že provozovatel cloudu typu Amazon, Google, Microsoft nebo Oracle musí vyhovět požadavku amerických úřadů a data jim předat, což nově platí i pro jejich evropská data centra. Citlivé informace jsou bezpečně zašifrované a **provozovatel cloudu k nim nemá klíče**.

VYUŽITÍ V PRAXI

Řešení HSM Luna může využít jakákoliv firma nebo organizace, která potřebuje přenášet a uchovávat velké množství **citlivých dat**, autorizovat velké množství **klíčů**, spravovat **certifikáty** nebo potřebuje zvýšit **prokazatelnost** vzniku určitého druhu dat.

Používá je proto například Ředitelství silnic a dálnic pro data z mýtných bran nebo provozovatel zahraničního satelitního mýtného systému pro autorizaci palubních jednotek OBU. HSM jsou ale skvělé i při ochraně osobních dat pacientů ve zdravotnictví nebo správě karet pražské Lítačky.

VÝHODY LUNY A HA CLUSTERU

- Špičková technologie na bázi Hardware Security Module
- Proces změny klíčů je rychlý a bezpečný
- Minimalizuje se riziko lidské chyby
- Data nemohou zneužít ani vlastní IT administrátoři
- Snadná implementace díky hotovým skriptům v clientovi Luny
- Výborné řešení pro IoT (internet věcí, chytré továrny a města)
- Delší životnost než většina ostatních síťových prvků (5 – 7 let)
- Po uplynutí období lze bezpečně vyřadit zálohovací disky
- Data jsou v cloudu v bezpečí i před cizími vládami
- Splňuje požadavky GDPR a ještě mnohem více

O NÁS

Společnost Business Systems, a. s. působí na českém trhu od roku 1997. Svým klientům z oblasti bankovníctví, zdravotnictví, energetiky, telekomunikací, cestovního ruchu, leteckého průmyslu i výrobním či obchodním společnostem zajišťuje tvorbu a provoz informačních systémů.