Konkrétne problémy a skúsenosti pri nasadzovaní PKI (1)

Andrej Vávra

Úvod

Čo je to PKI?

Ide o skratku anglického pomenovania Public Key Infrastructure, slovensky infraštruktúra verejných kľúčov. PKI je založená na asymetrickej kryptografii (používa algoritmy ako RSA, Diffie-Hellman, eliptické krivky…) a veľmi elegantne zabezpečuje správu kľúčov (key management), čo bol hlavný nedostatok systémov založených na symetrickej kryptografii (používané algoritmy ako DES, Blowfish, AES…).

Čo rieši PKI?

Pomocou PKI môžeme prirodzene zaistiť bezpečnú komunikáciu v nezabezpečenom prostredí (napr. na internete). Pomocou PKI možno dosiahnuť kľúčové bezpečnostné atribúty, ako je autenticko sť, integrita, nepopierateľnosť a dôvernosť. Príkladom úspešného nasadenia PKI je protokol SSL (Secure Socket Layer), ktorý sa používa na dosiahnutie bezpečného prístupu na webové stránky. Ďalším známym produktom, ktorý používa infraštruktúru verejných kľúčov je PGP (Pretty Good Privacy).

Sú projekty nasadzovania PKI úspešné?

V 90. rokoch minulého storočia sa organizácie vrhli na PKI s tým, že im to vyrieši všetky problémy. Tento boom súvisel aj s rozmachom a následným pádom internetových spoločností. Z tohto pohľadu by sa mohlo zdať, že projekty PKI svoju šancu prepásli. Nie je to však pravda. Boli len preceňované a nezvládnuté. Úspešné projekty PKI riešili presne definované problémy a nesnažili sa vyriešiť všetko. Všeobecne pre PKI platí, že pomaly ďalej zájdeš.

Desať podmienok úspešného nasadenia PKI

V tejto časti budeme popisovať desať podmienok, ktoré musia platiť, aby nasadenie PKI bolo úspešné. Nevyhradzujeme si právo tvrdiť, že je to úplný a nemenný zoznam. Týchto desať podmienok na základe našich skúseností však pokladáme za najdôležitejšie.

1. **Nasadenie PKI musí riešiť a podporovať reálne potreby.** Toto platí pre každý projekt a v prípade nasadzovania PKI to platí dvojnásobne, pretože projekty PKI sú veľmi náročné časovo aj finančne. Máloktorá organizácia si môže dovoliť investovať peniaze do stratových projektov. Je potrebné kalkulovať s tým, že návratnosť investícií v krátkom časovom horizonte (jeden, dva roky) je pri nasadení PKI nereálna.
2. **Nasadenie PKI musí mať podporu výkonného vedenia organizácie.** Súvisí to s predchádzajúcim bodom. Pri nasadzovaní PKI vznikajú zákonite problémy i konflikty, preto je nutné, aby pre jeho realizáciu malo vedenie pochopenie a dosť vysokú mieru tolerancie.
3. **Nasadenie PKI musí mať širokú podporu vo vnútri organizácie.** Ani podpora výkonného vedenia organizácie ešte

automaticky nezaručí úspech pri nasadzovaní PKI, pretože pri nej ide najmä o koncových používateľov. PKI zavádza do ich pracovných postupov novinky, ktoré nemusia akceptovať. Preto je nevyhnutné formou prezentácií a školení neustále dokazovať a presviedčať, že nasadenie PKI im prinesie omnoho viacej výhod ako nevýhod. Najjednoduchšia možnosť je zrovnoprávniť elektronický podpis s rukou vytvoreným podpisom pri vybraných úkonoch. Napríklad pri schvaľovaní dovolenky nemusí pracovník vypisovať dovolenkové lístky, a potom zháňať svojho nadriadeného, aby mu ich podpísal. Jednoducho pošle elektronicky podpísanú žiadosť vo forme e-mailu.

4. **Musí byť určený projektový vedúci a silný projektový tím.** Projekt nasadenia PKI zasahuje všetky oblasti fungovania organizácie, a preto sa mu musí projektový vedúci venovať na 100 %. Projektový tím by mal mať vybudovanú silnú pozíciu v organizácii a nemala by to byť „trpená“ skupina zamestnancov.

5. **Projekt nasadenia PKI musí byť správne rozdelený na etapy a fázy s definovanými úlohami a zodpovednosťami.** Opäť všeobecná zásada. PKI je predovšetkým o budovaní dôvery, takže každému musí byť jasné, aké má povinnosti a zodpovednosti.

6. **Musí existovať nezávislá kontrola.** Úzko súvisí s predchádzajúcim bodom. V prípade PKI je vhodné definovať auditné plány a aj kontroly vykonávané externými subjektmi (analýza rizík, penetračné testy), aby bolo vždy možné dokladovať, že naša PKI je dôveryhodná.

7. **Nasadenie PKI musí mať vyvážené technologické aj netechnologické časti.** Okrem technologickej časti, ktorej význam je zrejmý, je potrebné klásť dôraz aj na netechnologické časti. Ide hlavne o školenia koncových používateľov a tvorbu dokumentácie. Platí, že netechnologické časti projektov PKI sú podceňované a keď si ich význam uvedomíme, môže byť už príliš neskoro.

8. **Musí existovať „správna“ infraštruktúra.** Systém PKI po úspešnom nasadení sa stane kritickým systémom v rámci organizácie. Tomu musí zodpovedať aj technické zázemie, model fyzickej a procedurálnej bezpečnosti. Musíme minimalizovať existenciu „single point of failure“, aby sa napríklad nestalo, že fungovanie celej infraštruktúry sa zrúti, ak v nejakej pracovnej stanici nastane hardvérová chyba v sieťovej karte.

9. **Musí prebehnúť úspešná pilotná prevádzka.** Nedá sa nasadzovať PKI formou veľkého tresku. Pri každom nasadení vznikajú problémy a konflikty (s existujúcou infraštruktúrou, pracovnými postupmi), preto je potrebné postupné zavádzanie. Každý ďalší krok si treba overiť – ideálne v pilotnej prevádzke, ktorá by mala simulovať reálne prostredie a odhaliť väčšinu úskalí a problémov.

10. **Nasadenie PKI musí mať dobrú prevádzkovú podporu a plánovanie rozšírenia.** Po nasadení PKI sme neskončili. Koncoví používatelia potrebujú nepretržitú podporu, servis a my na základe spätnej väzby musíme plánovať rozšírenie i modifikáciu.

Kroky pri nasadzovaní PKI

V tejto časti budeme prezentovať šesť krokov pri nasadzovaní projektov PKI. Keďže ide o projekty, pri ktorých sa vytvára alebo modifikuje infraštruktúra, tak delenie na kroky (fázy, etapy) je veľmi dôležité (pozri predchádzajúcu kapitolu). Podotýkame, že v nasledujúcich krokoch uvažujeme iba o technologickom nasadzovaní PKI. Pravidlá a postupy pre implementáciu netechnologických častí (napríklad vytváranie dokumentácie) sa veľmi ťažko zovšeobecňujú, pretože vždy závisia od povahy konkrétneho projektu.

Krok 1: Inicializácia projektu a plánovanie
- Plánovanie projektu (stanovenie obchodných požiadaviek, celkové náklady, návratnosť investícií).
- Určenie projektového vedúceho a základného projektového tímu.
- Zapojenie sponzorov (členov výkonného vedenia) vo vnútri organizácie.
- Vytvorenie projektového plánu (požiadavky, špecifikácie, termíny, zodpovednosť).

Krok 2: Analýza požiadaviek a návrh
- Analýza požiadaviek PKI (čo má systém poskytovať, bezpečnostná politika, zakomponovanie do existujúcich systémov).
- Vzdelávanie a vnútropodnikové iniciatívy (školenia, stretnutia, prezentácie).
- Analýza požiadaviek na komponenty PKI (umiestnenie vo fyzických lokalitách, priestoroch), identifikácia potrebného hardvéru a softvéru.
- Identifikácia všetkých členov projektového tímu (až na úroveň systémových administrátorov).

Krok 3: Vývoj a testovanie
- Základné testovanie všetkých nasadzovaných komponentov (softvér, hardvér).
- Posúdenie nasadzovaného systému a prípadné modifikácie architektúry (veľmi vhodné je vykonať analýzu rizík nezávislou firmou).
- Určenie záberu pre pilotný projekt a následné rozširovanie (počty používateľov, zakomponované systémy, pracovné postupy).
- Školenia členov projektového tímu (pracovníci certifikačnej autority, pracovníci registračných autorít, pracovníci Help Desk).

Krok 4: Inštalácia, integrácia a testovanie
- Inštalácia počítačovej siete, sieťových komponentov, operačných systémov, aplikácií…
- Integrácia s existujúcimi systémami.
- Testovanie funkcionality.

Krok 5: Nasadenie
- Pilotná prevádzka (mala by trvať 4 – 6 týždňov a zahŕňať minimálne 50 koncových používateľov).
- Vzdelávanie koncových používateľov.
- Rozširovanie pilotnej prevádzky a postupný prechod do ostrej prevádzky.

Krok 6: Podpora
- Zabezpečenie podpory pre koncových používateľov (riešenie problémov, Help Desk).
- Plánovanie rozšírenia PKI na základe spätnej väzby.

Pokračovanie v budúcom čísle.

Mgr. Andrej Vávra

Tempest, s. r. o.
Landererova 1
811 09 Bratislava
Tel.: 02/50 26 71 11
e-mail: andrej_vavra@tempest.sk