Kapitola 8

Realizace bezpečnosti

Po prostudování kapitoly budete umět:

- stanovit základní přístup při zpracování bezpečnostní politiky;
- stanovit bezpečnostní opatření v návaznosti na výsledky analýzy rizik.

Klíčová slova:

Bezpečnostní politika, bezpečnostní opatření, bezpečnostní normy.

8.1 Stanovení bezpečnostní politiky

Bezpečnostní politika je základním dokumentem podniku, který vymezuje rozsah a určení nutných opatření při vybudování systému řízení bezpečnosti informací. Řeší základní organizační aspekty při formulování přístupu k budování bezpečnostních opatření. Při formulování bezpečnostních zásad je třeba při návrhu bezpečnostní politiky vycházet z toho, že realizovaný bezpečnostní systém musí zahrnovat nejrůznější úrovně i způsoby zabezpečení – od komplexních služeb a řešení na úrovni globálních sítí až k podnikovým sítím a jednotlivým koncovým zařízením s využitím nejmodernějších technologií ochrany před počítačovými viry, hackingem, útoky na dostupnost (denial of service) a nedbalostí koncových uživatelů. Samozřejmostí je zálohování důležitých dat mimo firmu. Jedná se tedy o komplexní ochranu v rámci stanoveného bezpečnostního perimetru podniku.

8.2 Bezpečnostní opatření – v návaznosti na analýzu rizik

Bezpečnostní opatření jsou realizována postupně pro zavádění jednotlivých bezpečnostních prvků podle stanovených priorit a ekonomických možností **podniku** s tím, že respektují výsledky analýzy rizik.

Návrh bezpečnostních opatření jednoznačně souvisí s mechanismy, které naplňují následující bezpečnostní funkce:

- systém identifikace a autentizace,
- řízení přístupu,
- funkce zajišťující integritu a důvěrnost,
- systém kontrol,
- mechanismy ochrany dat,
- mechanismy fyzické bezpečnosti.

Základní principy bezpečnostních opatření v rámci technologické infrastruktury jsou řízeny v souladu s doporučením dle ČSN ISO/IEC řady 27000.

Určujícím požadavkem na fungování bezpečnostních nástrojů je zajištění následujících bodů:

- vysoká dostupnost,
- aplikační load balancing,
- odolnost proti chybám a aktivním útokům,
- odolnost proti neoprávněnému přístupu,
- minimalizace škod způsobených logickou chybou => definice zálohovací strategie a obnovy,
- zajištění zabezpečené komunikace,
- zajištění informační infrastruktury splňující požadavky na integritu, dostupnost a bezpečnost zpracovávaných, distribuovaných a ukládaných informací,
- bezpečnostní monitoring,
- administrace systému.

Klíčovým principem návrhu řešení bezpečnostních opatření je procesní integrace, která je v souladu zejména s odpovídajícími postupy a doporučeními normy ČSN ISO/IEC 27001:2014.

Navrhovaná bezpečnostní protiopatření musí poskytovat ochranu v několika různých směrech:

- sníží hrozbu,
- sníží zranitelnost,
- sníží dopad nežádoucí události,
- detekují nechtěnou událost,
- umožní zotavení systému z nechtěné události.

V navržených opatřeních musí být dodrženy následující bezpečnostní principy:

- první úroveň bezpečnostních opatření se týká zajištění fyzické bezpečnosti serverů,
- přístup k databázím bude umožněn pouze pro přesně specifikované role s nezbytnými právy,
- provozované aplikace nebudou oprávněné upravovat data přímo a editace dat bude možná pouze pomocí uložených procedur, které zajistí správnou manipulaci s daty, přičemž bude využito auditní logování pro záznam přihlašování a činnosti jednotlivých uživatelů,
- požadavky na zabezpečení zpracovávaných informací i koncepce bezpečnosti informačních systémů podniku musí být v souladu s bezpečnostními předpisy podniku a s požadavky stanovenými v bezpečnostních zákonných opatřeních.

Základními dokumenty, které formují procesy a metody při zajišťování bezpečnosti v podnikových informačních systémech jsou uvedeny v bezpečnostních normách ČSN ISO/IEC řady 27000. Metodické řízení navrhovaného systému řízení bezpečnosti je obsaženo CoBit v. 5 a ITIL v. 3. Jedná se o soubory dokumentů, které vycházejí z „nejlepších přístupů“, které se při realizaci bezpečnosti využívají.

V návaznosti na tyto dokumenty lze koncipovat i realizovat správné postupy řízení, kontroly a auditu informačních technologií.

Vzhledem k tomu, že podle těchto dokumentů a zejména metodik musí realizace bezpečnosti podléhat procesnímu řízení. S tím souvisí nezbytné nastavení procesů, které zajišťují bezpečnost v informačních systémech. Je nutné tento přístup skloubit s bezpečnostními požadavky z pohledu využívaných bezpečnostních produktů (šifrovacích zařízení, zabezpečených úložišť apod.)

Procesní přístup je nutné nastavit i při řízení provozu.

V rámci realizace bezpečnosti je nutné realizovat systém správy nestandardních událostí. Ve smyslu metodiky ITIL se jedná o nastavení procesů:

- Správa incidentů
- Správa bezpečnostní problémů
- Správa změn

V kapitole je ukázán smysl návrhu, realizace a schválení bezpečnostní politiky. Následně jsou pak rozebírána jednotlivá bezpečnostní opatření pokrývající evidovaná rizika zjištěná v rámci analýzy rizik.

1. Charakterizujte účel realizace bezpečnostní politiky.
2. Jaké jsou hlavní účely při stanovení bezpečnostních opatření?
3. Jak se do návrhu bezpečnostních opatření promítají doporučení ČSN norem řady 2700?

Literatura k tématu:

[2] MATES, P., SMEJKAL, V. *E-government v České republice. Právní a technologické aspekty*. 2. podstatně přepracované a rozšířené vydání. Praha: Leges, 2012, 456 str., ISBN 978-80-87576-36-6.

[2] SMEJKAL, V., RAIS, K. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualizované a rozšířené vydání. Praha: GRADA, 2013, 488 str., ISBN 978-80-247-4644-9.