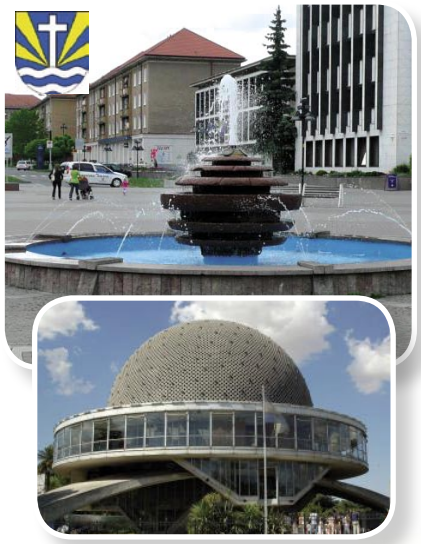
Prípadová štúdia zavedenia bezpečnostnej politiky v organizácii



Požiadavky zákazníka

Mestský úrad v rámci svojej činnosti pracuje s rôznymi druhmi informácií, ktoré majú rôzny stupeň dôvernosti. Preto je nutné s niektorými údajmi pracovať obozretne a zabezpečiť, aby sa nedostali do nepovolaných rúk. Pri realizácii týchto cieľov je potrebné sa riadiť výnosom Ministerstva financií MF/013261/2008-132 a jeho novelou z roku 2010 o štandardoch pre informačné systémy verejnej správy.

V tejto súvislosti bolo potrebné zabezpečiť:

- riadenie informačnej bezpečnosti,
- zabezpečenie realizácie a dodržiavania schválenej bezpečnostnej politiky,
- implementáciu systému riadenia a monitorovania rizík v súvislosti s informačnými systémami verejnej správy, a to najmä podľa relevantných technických noriem a pravidelné zbieranie relevantných údajov súvisiacich s rizikami,
- identifikáciu, analýzu a hodnotenie rizík spojených s využívaním aktív a informačných systémov verejnej správy.

Spoločnosť :
Mestský úrad
Žiar nad Hronom

Odvetvie :
Verejná správa

Požiadavky :
Zavedenie bezpečnostnej politiky do života organizácie

Riešenie :
Bezpečnostný projekt, bezpečnostná smernica

Nasadené riešenie

Podľa metodického pokynu k výnosu Ministerstva financií k §28 sa píše :

Bezpečnostná politika je dôležitým základom pre riadenie a správu informačnej bezpečnosti a zabezpečenie jej kontinuity. Základ bezpečnostnej politiky je ekvivalentný s bezpečnostným ámerom podľa §16 ods. 4 zákona č. 428 / 2002 Z. z. o ochrane osobných údajov, s rozšíreniami o niektoré presnejšie špecifikácie.

Nasadené riešenie

Nakoľko bezpečnostný zámer je neoddeliteľnou súčasťou bezpečnostného projektu podľa §16 odstavec 3) zákona č.428/2002 Z.z. o ochrane osobných údajov, prvým krokom k zavedeniu bezpečnostnej politiky bolo **vypracovanie bezpečnostného projektu.** Tým **bola pokrytá nielen oblasť ochrany osobných údajov, ale bol položený aj základ na ďalšie budovanie bezpečnostnej politiky**. Cieľom bezpečnostného projektu IS je definovanie prostriedkov, postupov a opatrení, ktoré chránia informácie počas vstupu, prenosov, spracovania, uloženia a výstupu proti strate dostupnosti, integrity a dôvernosti. Bezpečnostný projekt IS sumarizuje výsledky analýz a popisuje spôsob riešenia zabezpečovacích postupov, mechanizmov a prvkov vo všetkých bezpečnostných rovinách a praktickú implementáciu bezpečnostných praktík podľa príslušných STN a ISO noriem (predovšetkým 17799 a 13335). Znamená to, že:

1. Bezpečnostný projekt IS vymedzuje rozsah a spôsob technických, organizačných a personálnych opatrení potrebných na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na IS z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti.
2. Bezpečnostný projekt IS sa spracúva v súlade so základnými pravidlami bezpečnosti IS, vydanými bezpečnostnými štandardmi, právnymi predpismi a medzinárodnými zmluvami, ktorými je Slovenská republika viazaná.
3. Bezpečnostný projekt IS pozostáva z nasledovných častí - etáp riešenia:
   I. bezpečnostný zámer IS,
   II. analýza bezpečnosti IS,
   III. bezpečnostné smernice.

Z metodického pokynu k výnosu ministerstva financií :

Bezpečnostná politika sa odporúča vytvoriť vo forme jasne štruktúrovaného a prehľadného dokumentu, prípadne dokumentov. Táto politika by mala byť jasne previazaná s inými bezpečnostnými dokumentmi a smernicami tak, aby spolu tvorili kompaktný celok. Ďalšie špecifické požiadavky (ako napr. špecifické požiadavky na elektronickú podateľňu) môžu byť napr. jej súčasťou v osobitných častiach.

Ďalším krokom k úspešnému budovaniu bezpečnostnej politiky na úrade bolo **vypracovanie bezpečnostnej smernice** tak, aby plne korešpondovala okrem zákona o ochrane osobných údajov aj s výnosom Ministerstva financií 312/2010 v paragrafoch §28 až §42 o informačnej bezpečnosti. Do smernice boli zapracované aj odporúčania zistené na základe rizikovej analýzy, ktorá je súčasťou bezpečnostného projektu. Smernica popisuje zodpovednosť za informačnú bezpečnosť a zodpovednosť za jednotlivé aktíva. Popisuje havarijné plánovanie a nahlasovanie bezpečnostných incidentov, ktoré je potrebné jednak podľa zákona 428/2002 o ochrane osobných údajov, a takisto je požadované výnosom o štandardoch pre IS verejnej správy. Taktiež obsahuje zásady a postupy manipulácie s jednotlivými aktívami ako aj mobilný prístup do internej siete, či prístup externých firiem k aplikáciám a aktívam úradu.

Prínosy riešenia

Vypracovanie bezpečnostného projektu podľa §16 zákona 428/2002 o ochrane osobných údajov plne pokrylo aj požiadavky výnosu Ministerstva financií 312/2010 s tým, že o tieto požiadavky bola rozšírená bezpečnostná smernica a tým sme zabezpečili :

1. definíciu informačnej bezpečnosti, jej cieľov a rozsahu a potvrdenie dôležitosti bezpečnosti,
2. princípy riadenia informačnej bezpečnosti,
3. kontrolný mechanizmus riadenia informačnej bezpečnosti,
4. monitorovanie a manažment bezpečnostných incidentov,
5. periodické hodnotenie zraniteľnosti,
6. účasť tretej strany.

„ Bezpečnostný projekt so smernicou predstavuje pre nás pevný základ pre ďalšie budovanie a zlepšovanie bezpečnostnej politiky ako aj pre dodržiavanie výnosu Ministerstva financií o štandardoch pre informačné systémy verejnej správy. “

Peter Paulík
Správca IT