

AUDIT INFORMAČNEJ BEZPEČNOSTI

Informačná bezpečnosť je podľa medzinárodnej normy ISO/IEC 27001 ochrana informácie pred širokým spektrom hrozieb, ktorej cieľom je :

- *zaistenie kontinuity obchodných procesov,*
- *minimalizácia strát a*
- *maximalizácia návratnosti investícií.*

V súčasnosti sa informácie v čoraz väčšej miere spracovávajú v elektronickej forme pomocou počítačov a iných informačných a komunikačných technológií. Potenciálna možnosť narušenia týchto informácií, či už priamo alebo prostredníctvom útoku na technické zariadenie alebo prostredie, v ktorom sa informácia spracováva, sa nazýva hrozba. Existuje množstvo činiteľov, ktoré môžu ohroziť alebo spôsobiť znefunkčnenie informačných a komunikačných technológií a znehodnotenie informácií, ktoré sú v nich spracovávané.

Sú to napríklad prírodné vplyvy, technické poruchy, ľudské chyby a omyly, škodlivý softvér, cieľavedomé útoky, počítačová kriminalita a medzinárodný terorizmus, ktoré by mohli spôsobiť vážne bezpečnostné problémy. Nezabezpečenie informácií môže mať za následok nenahraditeľné straty a narušenie dôveryhodnosti organizácie.

Cieľom informačnej bezpečnosti je minimalizovať možnosti uplatnenia sa hrozieb a v prípade vzniknutých následkov minimalizovať ich vplyv, čo je nevyhnutnou podmienkou tak pre verejnú správu ako aj súkromnú sféru.

Jednou z možností ako eliminovať možný dopad hrozieb na informačné technológie je aj vykonanie interného auditu informačnej bezpečnosti podľa normy ISO/IEC 27001, ktorý obsahuje:

- *fyzickú bezpečnosť a bezpečnosť prostredia,*
- *bezpečnosť zariadení,*
- *riadenie dodávky služieb poskytovaných tretími stranami,*
- *ochranu proti škodlivému softvéru,*
- *zálohovanie,*
- *manipuláciu s médiami,*
- *výmenu informácií a softvéru,*
- *monitoring,*
- *riadenie prístupu k sieti,*
- *riadenie prístupu do operačného systému,*
- *riadenie prístupu k aplikáciám a informáciám,*
- *mobilné počítačové systémy a práca na diaľku,*
- *kryptografické opatrenia,*
- *údržbu výpočtovej techniky,*
- *riadenie incidentov informačnej bezpečnosti.*

Audit je možné rozšíriť aj o kontrolu súladu s najnovším zákonom 122/2013 o ochrane osobných údajov, ktorý zahŕňa preverku aktuálnosti bezpečnostného projektu, bezpečnostných smerníc a ich zavedení do praxe.

