STRATÉGIA KYBERNETICKEJ BEZPEČNOSTI

A: Štruktúra stratégie kybernetickej bezpečnosti

Stratégia kybernetickej bezpečnosti obsahuje najmenej určenie

1. bezpečnostných cieľov z hľadiska kybernetickej bezpečnosti,
2. spôsobu vyhodnocovania bezpečnostných cieľov, kritérií vyhodnocovania dosahovania bezpečnostných cieľov, spôsobov priebežného hodnotenia ich primeranosti a spôsobov kontroly postupov využívaných na dosahovanie bezpečnostných cieľov,
3. úlohy štatutárneho orgánu prevádzkovateľa základnej služby pri zabezpečovaní kybernetickej bezpečnosti a vyhlásenie o záväzku o podpore kybernetickej bezpečnosti,
4. všeobecných a špecifických zodpovedností a povinností v oblasti kybernetickej bezpečnosti a určenie príslušných bezpečnostných rolí potrebných na riadenie kybernetickej bezpečnosti vrátane určenia rozsahov činností, kompetencií a úloh; rozdelenie rolí na riadiacu zložku, výkonnú zložku a kontrolnú zložku, pričom riadiaca zložka je priamo riadená prevádzkovateľom základnej služby a kontrolná zložka je nezlučiteľná so všetkými ostatnými zložkami,
5. základného rámca na riadenie aktív podľa § 6, od ktorých závisí činnosť sietí a informačných systémov,
6. základného rámca riadenia rizík podľa § 6 v súvislosti s aktívami, od ktorých závisí činnosť sietí a informačných systémov a určenie bezpečnostných opatrení podľa oblastí v zmysle § 20 ods. 3 zákona v závislosti od identifikovaných rizík,
7. rozsahu a periodicity overovania stavu kybernetickej bezpečnosti prostredníctvom auditu kybernetickej bezpečnosti vrátane zhodnotenia súladu stratégie a bezpečnostných politík s požiadavkami zákona, iného všeobecne záväzného právneho predpisu, vnútorných predpisov a zmluvnými záväzkami,
8. postupu a zodpovedností pri revízii bezpečnostnej dokumentácie schvaľovanej prevádzkovateľom základnej služby vrátane periodicity pravidelných revízií a jej aktualizácií po každej zmene majúcej na ňu vplyv, ako aj z dôvodov mimoriadnych revízií.

B: Štruktúra bezpečnostnej politiky kybernetickej bezpečnosti

Bezpečnostné politiky	Súvisiace bezpečnostné štandardy
1. Organizácia bezpečnosti	– Riadenie bezpečnostnej architektúry – Systém riadenia kybernetickej bezpečnosti – Riadenie identít a prístupových práv – Riadenie privilegovaných prístupov – Bezpečnostný monitoring a správa bezpečnostných záznamov
2. Riadenie bezpečnostných rizík	– Testovanie a bezpečnostná certifikácia systémov – Metodika posudzovania vplyvu na ochranu osobných údajov – Metodika posudzovania rizík – Fyzická bezpečnosť a bezpečnosť prostredia – Riešenie bezpečnostných incidentov
3. Riadenie informačných aktív	– Klasifikácia informácií a kategorizácia sietí – Registratúrny poriadok a registratúrny plán
4. Pravidlá správania a dobrej praxe	– Práca na diaľku a používanie mobilných zariadení – Riadenie personálnej bezpečnosti – Pravidlá komunikácie
5. Riadenie dodávateľských vzťahov	– Riadenie dodávateľských služieb – Akvizícia informačných systémov
6. Riadenie vývoja a údržby v oblasti informačno-komunikačných technológií	– Vývoj a testovanie informačných systémov – Postupy údržby informačných systémov – Riadenie technických zraniteľností a manažment záplat
7. Riadenie a prevádzka informačno-komunikačných technológií	– Pravidlá prepájania systémov a prenosu elektronických informácií – Riadenie bezpečnosti sietí – Riadenie zmien infraštruktúry – Riadenie kapacity systémov a služieb – Riadenie kryptografických opatrení
8. Riadenie súladu	– Audit kybernetickej bezpečnosti – Spracúvanie osobných údajov a klasifikovaných informácií – Poskytovanie súčinnosti tretím stranám
9. Riadenie kontinuity procesov a činností	– Plány kontinuity prevádzkových činností – Plány havarijnej obnovy prevádzky – Metodika zálohovania a obnovy informácií