

Analýza rizík a analýza rizík CRAMM

je nevyhnutným procesom pre správny návrh a implementáciu bezpečnostných opatrení. Umožňuje identifikáciu bezpečnostných rizík, ktoré sú závislé od aktív (komponentov) hodnoteného systému, ich zraniteľnosti, vplyvu prostredia (sily hrozieb) a potenciálneho negatívneho vplyvu na činnosť systému (dopadov).

Naša metodika analýzy rizík pokrýva všetky oblasti bezpečnosti (bezpečnosť informačného systému, objektovú bezpečnosť, fyzickú a personálnu bezpečnosť, bezpečnosť podpornej infraštruktúry). Pri analýze rizík používame automatizované systémy aj neautomatizované postupy.

Dlhodobu a v rôznom prostredí aplikujeme efektívnu a časovo nenáročnú metodiku analýzy rizík neautomatizovaným postupom s rýchlými a preukázateľnými výstupmi, vhodnými pre manažment. Hlavným cieľom tejto metodiky je identifikácia hlavných hrozieb, zraniteľností a dopadov na strategické osi (strategické funkcie) organizácie.

Máme viacero skúseností s rôznymi automatizovanými systémami analýzy rizík.

S ich pomocou získate reálnu predstavu o bezpečnostných rizikách, navrhnutých bezpečnostných opatreniach a ich vplyve na bezpečnosť systému ešte pred investovaním do nákupu bezpečnostných technológií. Jedným z týchto systémov je nástroj CRAMM.

Analýza rizík podľa metodiky CRAMM neskúma bezpečnosť jednotlivých aktív IS, ale ich združuje do logických celkov – modelov aktív, ktoré sú potom predmetom analýzy rizík.

Analýza rizík nástrojom CRAMM sa v zmysle metodiky skladá z troch fáz, z ktorých každá je podporovaná dotazníkmi a pokynmi.

Fáza 1 – Identifikácia aktív, vytvorenie modelov, ohodnotenie aktív

Identifikácia aktív - dát, služieb nad údajmi, programového vybavenia, fyzických aktív a priestorov

Vytvorenie modelov aktív, ktoré definujú závislosť medzi rôznymi typmi aktív

Ohodnotenie dátových aktív (dopad pri prezradení, modifikácii, zničení, neprístupnosti)

Ohodnotenie fyzických a programových aktív (náklady na obnovu, rekonštrukciu).

Fáza 2 – Stanovenie rizík

Výpočet rizík, vyplývajúcich z hrozieb pôsobiacich na systém, alebo sieť, založených na ohodnotení aktív a hodnotení úrovne hrozieb a zraniteľnosti.

Fáza 3 – Riadenie rizík

Riadenie rizík zahŕňa identifikáciu, výber a zavedenie vhodných bezpečnostných opatrení pre zníženie rizika na prijateľnú úroveň.

Nástroj CRAMM vyberá opatrenia zo svojej knižnice opatrení tak, aby pokryli všetky možné hrozby identifikované v druhej fáze s ohľadom na vypočítanú mieru rizika. Takýmto spôsobom vznikne bezpečnostný profil IS.