Metodický pokyn MF SR: Základy správy rizík v súvislosti s IKT v 1.0

Každá správa (bezpečnostných) rizík v oblasti informačno-komunikačných technológií (IKT) začína vytvorením prvotnej analýzy rizík, čo je zároveň prvý krok v návrhu systému informačnej bezpečnosti. Takáto analýza rizík sa dá rámcovo popísať nasledovnými krokmi:

1. **Identifikuj a ohodnoť aktíva:** počítačové zariadenia a softvér sú aktíva rovnako, ako sú nimi informácie, uložené na počítačových zariadeniach; aj reputácia je aktívom.
2. **Identifikuj hrozby:** vytvor zoznam možných negatívnych vplyvov (hrozieb) na aktíva; pre kategorizáciu hrozieb existujú rôzne spôsoby resp. metodiky.
3. **Identifikuj zraniteľnosti:** analyzuj vyššie vytvorený systém z pohľadu zraniteľností, ktoré by mohli poškodiť identifikované aktíva.
4. **Vyhodnoť riziká:** každé riziko je principiálne založené na kombinácii hodnoty aktív, počtu a vážnosti hrozieb a počtu a vážnosti zraniteľností; pre kategorizáciu resp. výpočet rizík taktiež existujú rôzne spôsoby.

Po vytvorení analýzy rizík sa navrhne relevantná bezpečnostná politika a následne technické opatrenia, ktoré budú implementovať túto politiku. Cieľom bezpečnostnej politiky je najmä určenie, či a do akej miery sa má konkrétne riziko potlačiť a technické opatrenia slúžia na zabezpečenie, aby sa tak stalo.

Pre systémové riešenie nestačí jednorazová analýza, nutnou súčasťou správnej správy rizík je preto pravidelné auditovanie resp. overovanie či je zoznam aktív, hrozieb a zraniteľností stále platný a úplný, čo nie je nič iné ako revízne opakovanie vyššie popísaných krokov.