Analýza rizík

Služby hodnotenia informačnej bezpečnosti sa používajú na posúdenie súčasného stavu bezpečnosti a identifikáciu rizík, ktorým je váš systém vystavený. Sú dôležitým zdrojom informácií pre rozhodovanie o investíciách do bezpečnosti.

V tejto oblasti ponúkame:

Analýzu súčasného stavu
Vyhodnotenie súladu s vybraným štandardom informačnej bezpečnosti (napr. ISO 27001) a identifikáciu slabých miest a bezpečnostných nedostatkov vrátane ich prioritizácie v danom prostredí, návrhy a odporúčania na odstránenie identifikovaných nedostatkov.

Analýza rizík IS
Príprava metodiky pre analýzu rizík informačnej bezpečnosti alebo využitie existujúcich metodík. Následne sa podľa zvolenej metodiky vykoná komplexná identifikácia a hodnotenie aktív súvisiacich s informačnou bezpečnosťou, identifikácia a hodnotenie hrozieb informačnej bezpečnosti, identifikácia a hodnotenie zraniteľností informačnej bezpečnosti. Hodnotenie úrovne rizík informačnej bezpečnosti podľa metodiky a podpora pri rozhodovaní o riadení rizík. Príprava návrhov opatrení, ktoré môžu znížiť riziká na prijateľnú úroveň.

Návrh plánu riadenia rizík
Návrh bezpečnostných opatrení/ odporúčaní vrátane ich načasovania vzhľadom na možnosti spoločnosti.

Analýzy sa vykonávajú v súlade s normami ISO/IEC 27005, ZoKB, alebo inými metodikami zvolenými zákazníkom.

Kedy vykonať analýzu rizík?

Analýza rizík informačného systému sa zvyčajne vykonáva v nasledujúcich prípadoch:

- Ak existuje požiadavka na posúdenie aktuálnej úrovne bezpečnosti IS.
- Ak potrebujete kvantifikovať riziká, ktorým je váš informačný systém vystavený.
- Po rozhodnutí zaviesť jasne definované pravidlá riadenia informačnej bezpečnosti.
- Počas implementácie analýzy rizík informačného systému (ISMS).
- Ak to požadujú audítori, akcionári alebo iné osoby.
- Ak zákazník požaduje dôkaz o kvalite vášho zabezpečenia.
- Ak je potrebné poskytnúť podklady o strategických rozhodnutiach týkajúcich sa implementácie nákladných bezpečnostných opatrení.
- V súlade s legislatívnymi požiadavkami, ako je napríklad zákon o kybernetickej bezpečnosti.
- V prípade vážnych pochybností o bezpečnosti vašich informácií, napríklad ak nedôverujete tretej strane, ktorá spravuje váš IS, alebo ak je vaša spoločnosť terčom útoku.

Charakteristiky riešenia

- Zázemie silného tímu analytikov a technických poradcov.
- Úzke naviazanie na technickú bezpečnosť - do analýzy rizík dokážeme zahrnúť technické skúšky.
- Používanie kvalitatívneho a kvantitatívneho prístupu k hodnoteniu rizík.
- Možnosť využitia širokej škály softvérových nástrojov.
- Vysoká flexibilita a otvorenosť voči požiadavkám zákazníka - metodiku dokážeme prispôsobiť požiadavkám klienta alebo použiť jeho interné postupy.
- Vysoká flexibilita a otvorenosť k požiadavkám zákazníka - metodiku dokážeme prispôsobiť požiadavkám klienta alebo použiť jeho interné postupy.

Prínosy

- Určenie priorít pre ďalšie investície a projekty v oblasti bezpečnosti.
- Určenie optimálneho pomeru medzi investíciami a dosiahnutou úrovňou bezpečnosti.
- Získanie informácií o dosiahnutej úrovni bezpečnosti IS od nezávislej strany.
- Identifikácia rizík a zraniteľností, ktoré predstavujú bezprostrednú hrozbu pre hlavné funkcie a aktíva organizácie.
- Vypracovanie dokumentov pre tvorbu bezpečnostnej dokumentácie IKT v organizácii.
- Identifikácia hrozieb, ako je únik údajov, zneužitie oprávnení, ľudská chyba atď., vrátane možných scenárov zneužitia.
- Výrazné zvýšenie bezpečnosti IS zavedením navrhovaných opatrení.
- Získanie argumentov na presadenie potrebných bezpečnostných opatrení.

Zjednodušený model analýzy rizík IS