Analýza rizik

Služby v oblasti vyhodnocování informační bezpečnosti slouží k posouzení aktuálního stavu bezpečnosti a identifikaci rizik, kterým je váš systém vystaven. Tvoří důležitý informační zdroj pro rozhodování o investicích do bezpečnosti.

V této oblasti nabízíme:

Analýzu současného stavu
Vyhodnocení souladu s vybraným standardem infomační bezpečnosti (např. ISO 27001) a identifikace slabých míst a nedostatků v zabezpečení včetně jejich prioritizace v daném prostředí, návrhy a doporučení pro odstranění identifikovaných nedostatků.

Analýzu rizik IS
Příprava metodiky pro analýzu rizik informační bezpečnosti, nebo využití stávající. Následně dle zvolené metodiky komplexní identifikace a ohodnocení aktiv souvisejících s informační bezpečností, identifikace a ohodnocení hrozeb informační bezpečnosti, identifikace a vyhodnocení zranitelností aktiv informační bezpečnosti.

Vyhodnocení úrovně rizik informační bezpečnosti dle metodiky a podpora při rozhodování o řízení rizik. Příprava návrhů opatření, kterými mohou být rizika snížena na akceptovatelnou úroveň.

Návrh plánu zvládání rizik
Návrh bezpečnostních opatření/ doporučení včetně jejich časování s ohledem na možnosti společnosti.

Analýzy provádíme v souladu s normou ISO/IEC 27005, ZoKB, a nebo jiných zákazníkem zvolených metodik.

Kdy provést analýzu rizik?

Analýza rizik informačního systému obvykle probíhá v následujících případech:

- Když vznikne požadavek na zhodnocení současné úrovně bezpečnosti IS.
- Při potřebě kvantifikovat rizika, jimž je váš informační systém vystaven.
- Po rozhodnutí implementovat jasně definovaná pravidla pro řízení informační bezpečnosti.
- Při zavádění systému Analýza rizik informačního systému (ISMS).
- Když jsou kladeny požadavky ze strany auditorů, akcionářů nebo jiných subjektů.
- Pokud zákazník vyžaduje doklady o kvalitě vašeho zabezpečení.
- Při potřebě poskytnout podklady pro strategická rozhodnutí ohledně implementace nákladných bezpečnostních opatření.
- V souladu s legislativními požadavky, například Zákonem o kybernetické bezpečnosti.
- V případě vážných pochybností o bezpečnosti informací, například v situaci, kdy nedůvěřujete třetí straně spravující váš IS nebo kdy se vaše společnost stane terčem útoku.

Charakteristiky řešení

- Zázemí silného týmu analytiků a technických konzultantů.
- Úzká vazba na technickou bezpečnost - do analýzy rizik jsme schopni zahrnout také technické testy.
- Využití kvalitativního i kvantitativního přístupu k hodnocení rizik.
- Možnost využití široké palety softwarových nástrojů.
- Vysoká flexibilita a otevřenost vůči požadavkům zákazníka - jsme schopni přizpůsobit metodiku dle požadavků klienta či využít jeho interní postupy.
- Vysoká flexibilita a otevřenost k požadavkům zákazníka - jsme schopni přizpůsobit metodiku požadavků klienta či využit jeho interní postupy.

Přínosy

- Určení priorit pro další investice a projekty v oblasti bezpečnosti.
- Stanovení optimálního poměru mezi investicemi a dosaženou úrovní zabezpečení.
- Získání informací o dosažené úrovni bezpečnosti IS od nezávislé strany.
- Identifikace rizik a slabých míst, které bezprostředně ohrožují klíčové funkce a aktiva organizace.
- Vytvoření podkladů pro tvorbu bezpečnostní dokumentace ICT v organizaci.
- Identifikace hrozeb typu úniku dat, zneužití privilegií, lidských chyb, atd., včetně možných scénářů zneužití.
- Významné zvýšení bezpečnosti IS implementací navržených opatření.
- Získání argumentů k prosazování potřebných bezpečnostních opatření.

Zjednodušený model analýzy rizik IS