Řízení informačních rizik

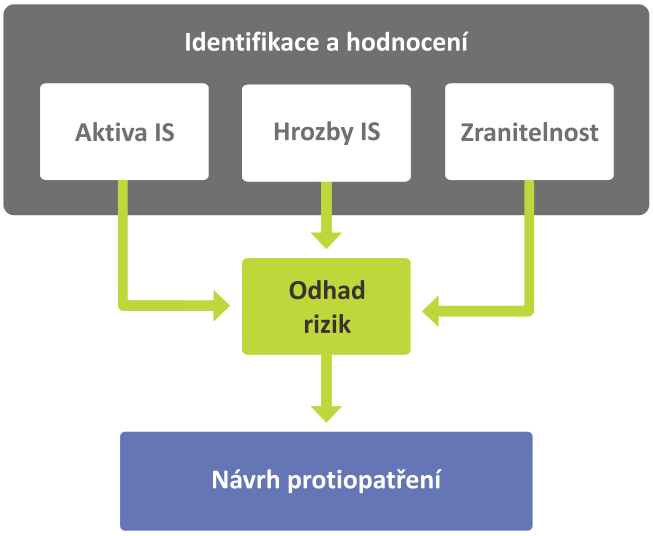
Služby v oblasti řízení informačních rizik slouží k posouzení aktuálního stavu bezpečnosti IS, tvoří důležitý informační zdroj pro zajištění bezpečnosti systémů a slouží jako podklady pro rozhodování o investicích do bezpečnosti.

V této oblasti Vám můžeme nabídnout:

- Analýzu současného stavu – rychlá identifikace slabých míst a nedostatků v zabezpečení, návrh doporučení pro jejich odstranění.
- Vytvoření modelu hrozeb IS/aplikace – identifikace možných ohrožení systému či aplikace.
- Analýzu rizik IS – komplexní identifikace aktiv, hrozeb a slabých míst, kvantifikace rizik, kterým je systém vystaven, návrh doporučení formou plánu bezpečnosti ICT.
- Specializované audity/analýzy zaměřené na určitou oblast.

Společnost AEC provádí analýzy a audity IS dle nejlepších zkušeností načerpaných během svého dlouhodobého působení na trhu v oblasti bezpečnosti ICT a podle uznávaných standardů:

- ISO 31000 Management rizik;
- Normy řady ISO/IEC 27000 zaměřené na řízení bezpečnosti;
- Metodiky OWASP, Microsoft apod. pro modelování hrozeb.



Zjednodušený model Analýzy rizik IS.

Proč AEC?

Společnost AEC využívá svých dlouholetých zkušeností při budování systémů řízení informační bezpečnosti a provádění úloh s tím spojených.

Naše řešení charakterizuje:

- silný tým analytiků a technických konzultantů;
- úzká vazba na technickou bezpečnost;
- využití kvalitativního přístupu analýz;
- podpora procesu analýzy použitím vlastního SW nástroje;
- vysoká flexibilita a otevřenost k požadavkům zákazníka.

Kdy provést analýzu rizik?

Analýza rizik informačního systému se provádí např. v následujících situacích:

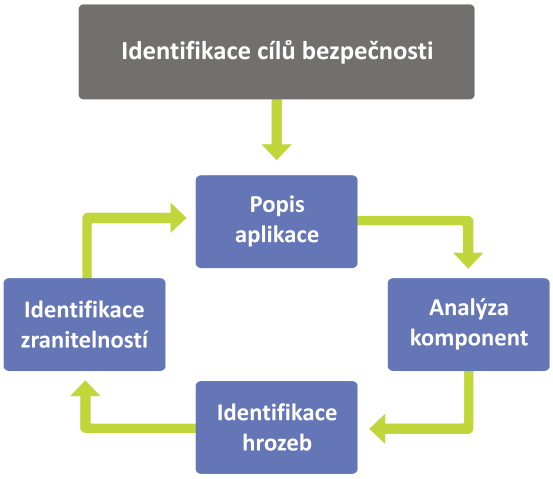
- zjištění aktuálního stavu bezpečnosti IS;
- kvantifikace rizik, kterým je Váš informační systém vystaven;
- v případě zavádění systému řízení informační bezpečnosti (ISMS);
- pro uspokojení požadavků auditorských firem, mateřské společnosti apod.;
- před zavedením nákladných bezpečnostních opatření;
- nutí-li Vás k tomu legislativa;
- v případě vážných pochyb o bezpečnosti informací (nedůvěra v administrátora, třetí stranu, která spravuje Váš IS apod.).

Kdy vytvořit model hrozeb?

- provozujete-li systémy s citlivými daty a chcete-li zajistit jejich bezpečnost;
- pokud chcete znát možné příčiny bezpečnostních incidentů;
- když chcete vědět, proti jakým typům útoků a hrozeb máte svoje systémy chránit.

Mezi hlavní přínosy realizace služeb z oblasti řízení informačních rizik patří:

- 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 nezávislou stranou.
- 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, lidské chyby atd. včetně možných scénářů zneužití.
- Významné zvýšení bezpečnosti IS implementací navržených opatření.
- Získání argumentů pro rozhodnutí managementu o přidělení investic do bezpečnosti IS.



Proces modelování hrozeb (zdroj OWASP).

Naši zákazníci

- Česká pošta, s.p.
- KBC Group NV Czech Branch
- OTE, a.s.
- ZUNO Bank AG
- ING Management Services s.r.o.
- GMC Software Technology
- Ministerstvo průmyslu a obchodu
- Úřad pro ochranu osobních údajů

AEC, spol. s r.o.
Purkyňova 2845/101
612 00 Brno, Czech Republic
Phone: +420 530 507 200
Fax: +420 530 507 220

AEC, spol. s r.o.
European Business Center
Dukelských hrdinů 34
170 00 Praha 7, Czech Republic
Phone: +420 267 311 402
Fax: +420 266 177 155

AEC
DATA SECURITY

www.aec.cz