BEZPEČNOSTNÍ ANALÝZA

KDYŽ DOJEM NESTAČÍ, A CHCETE ZNÁT REÁLNÝ STAV...

Bezpečnostní analýza provádí dekompozici zkoumaného objektu na základní prvky, vyhledává a zkoumá vnitřní zranitelnosti, vnější hrozby a implementované ochranné mechanizmy, působící na jednotlivé prvky ve zvolených vrstvách bezpečnosti: počítačové a komunikační, fyzické, personální, administrativní a organizační.

Cílem bezpečnostních analýz je identifikovat maximum zranitelností a nedostatků obsažených ve zkoumaném objektu, odhadnout hrozby, rizika a možné negativní dopady na zkoumaný objekt, určit efektivitu a funkčnost stávajících ochranných mechanizmů a navrhnout nové tak, aby byla všechna rizika efektivně snížena nebo pokryta na akceptovatelnou úroveň.

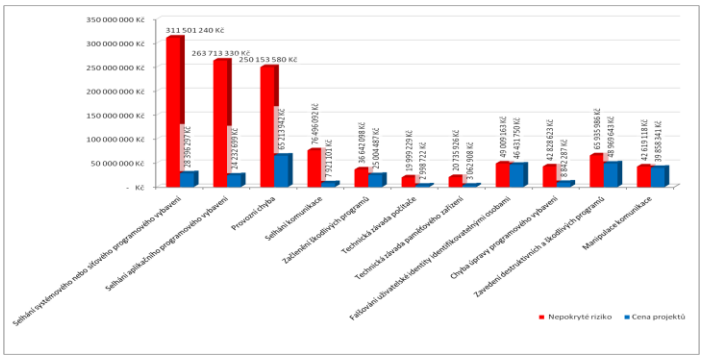
Objektem bezpečnostních analýz mohou být počítačové systémy, zařízení, datová aktiva, služby, aplikace, procesy nebo informační systém organizace jako celek.

Nabízíme různé typy analýz bezpečnosti informačních systémů a technologií s použitím mezinárodních metodik, realizované dle kriterií a požadavků zákazníka.

- ***Přehledová analýza rizik***
- ***Detailní analýza rizik***
- ***Technická bezpečnostní analýza***
- ***Srovnávací analýza stavu***
- ***Analýza dopadů na podnikání***
- ***Počítačová forenzní analýza incidentů***
- ***Analýza zranitelností***

Při plánování a řízení bezpečnosti jsou analýzy zaměřeny především na komplexní zmapování všech možných rizik ohrožujících zkoumané objekty (aktiva organizace) a ve všech parametrech bezpečnosti informací (důvěrnost, dostupnost, integrita). Následné kroky bezpečnostní analýzy zahrnují návrh efektivních a systémových protiopatření ve všech oblastech bezpečnosti informací.

Při provozu a údržbě bezpečnosti IS jsou analýzy zaměřeny na zkoumání určitých bezpečnostních mechanizmů nebo technologií ve zvolených oblastech bezpečnosti, nebo na následky selhání, případně porušení, ochranných opatření ve zvolených náhledech (požadavcích) na zajištění bezpečnosti IS.



Financování bezpečnostních projektů musí být založeno na transparentním hodnocení rizik a nedostatků v prostředí a chování organizace. Analýzy založené na kvantitativním přístupu zajistí dostatečné podklady pro finanční rozhodování o investicích do bezpečnosti a o nákladech na pokrytí identifikovaných rizik. Součástí analýzy je příprava plánů bezpečnostních projektů včetně odhadu zdrojů.

PLÁNOVÁNÍ, ŘÍZENÍ, PROVOZ A ÚDRŽBA BEZPEČNOSTI IS …

Přehledová analýza rizik

Cíl: rychlý přehled o nejzávažnějších hrozbách a zranitelnostech jednoho vybraného, zpravidla nejcitlivějšího datového aktiva reprezentujícího IS.

Využití: podklad pro rozhodnutí a přípravu na provedení detailní analýzy rizik. Velmi rychlé a cenově efektivní - max. 8hod.

Detailní analýza rizik

Cíl: komplexně zmapovat velikost rizik a jejich možných negativních dopadů; revize aktuálního stavu protiopatření a podrobný návrh efektivních protiopatření na pokrytí identifikovaných rizik.

Využití: úvodní etapa zavádění bezpečnosti IS v organizacích; základní fáze životního cyklu ISMS (systému řízení bezpečnosti IS).

Analýza dopadů na podnikání (BIA)

Cíl: určit velikost a závažnost následků nedostupnosti IS po různá časová období a identifikovat potřebná opatření pro jeho obnovu.

Využití: stanovení efektivních požadavků a výběr optimální strategie pro návrh a tvorbu havarijních plánů obnovy funkčnosti IS.

Analýza zranitelností

Cíl: identifikovat a ohodnotit zranitelnosti systémů a aplikací, ohodnotit bezpečnost interních i externích zařízení, penetrační testování.

Využití: součást procesů řízení zranitelností a bezpečnostních dohledů, provádění interních a externích penetračních testů.

Technická bezpečnostní analýza (RAC ISSEC)

Cíl: nalézt maximum zranitelností, obsažených v návrhu, instalaci nebo konfiguraci IS a navrhnout odpovídající protiopatření.

Využití: posouzení účinnosti návrhu nasazení bezpečnostních technologií; zpřesnění výsledků analýzy rizik nebo penetračního testování.

Srovnávací analýza stavu (GAP analysis)

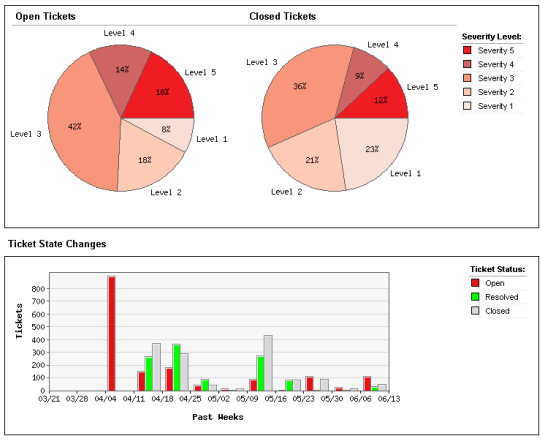
Cíl: identifikovat nedostatky aktuálního stavu bezpečnosti informací vůči vybraným mezinárodním normám (ISO/IEC 27002, ISO/IEC 27001, BASEL II…) a navrhnout potřebná a chybějící opatření.

Využití: podklady pro výběr a implementaci chybějících opatření dle zvolené normy pro bezpečnost IS a příprava na audit a certifikaci.

Počítačová forenzní analýza incidentů (CFI)

Cíl: identifikovat a zdokumentovat příčiny vzniku bezpečnostního incidentu, jeho průběh a rozsah následků a shromáždit tak důkazní materiál.

Využití: odborné vyšetření bezpečnostních incidentů, případně trestných činů, spáchaných v souvislosti nebo s využitím výpočetní techniky.



Risk Analysis Consultants, s. r.o.
Španělská 2
120 00 Praha 2
Česká republika
+420 221 628 400
rac@rac.cz
www.rac.cz

Risk Analysis Consultants je nezávislá poradenská společnost poskytující služby a řešení ve všech oblastech bezpečnosti informací v souladu s mezinárodními normami, související národní legislativou a respektováním individuálních podmínek klientů. Od roku 1995 pomáhá zajišťovat bezpečnost informací v informačních systémech organizací státní správy, bank, finančních institucí, telekomunikačních společností a průmyslových podniků v České republice i v zahraničí.

QR code RAC