



G - Risk

Analýza rizík informačného systému

Neustále žijeme v ohrození.
Našťastie mnohé nebezpečenstvá sú málo
pravdepodobné - zemetrasenie, tsunami, vojna ...
Iné sú však pravdepodobnejšie - povodeň,
krupobitie, krádež.

**Do akej skupiny patria riziká, ktoré
ohrozujú váš firemný informačný systém?
Aká je ich pravdepodobnosť?
Čo o nich vlastne viete?**



GORDIAS
IT • SECURITY

G - Risk / Analýza rizík informačného systému



Analýza rizík IS je jednou z kľúčových aktivít zvyšovania informačnej bezpečnosti. Jej cieľom je dať pravdivé odpovede na otázky:

- Čo ohrozuje IS a údaje v ňom?
- Ako je IS proti týmto hrozbám chránený?
- Kde sú slabé miesta v bezpečnosti IS?

Spoločnosť GORDIAS má s analýzou rizík rozsiahle skúsenosti.

Naši konzultanti vykonali analýzu rizík pre orgány štátnej správy, priemyselné podniky, obchodné spoločnosti i finančné inštitúcie. Ich skúsenosti umožňujú zohľadniť charakter vašej organizácie a prispôbiť mu analýzu.

Analýza rizík sa skladá z niekoľkých fáz:

- určenie rozsahu, ohraničení, metodológie,
- zber a syntéza dát, uskutočnenie analýzy rizík,
- interpretácia výsledkov analýzy rizík.

Určenie rozsahu, ohraničení, metodológie

Prvým krokom je vymedzenie oblastí a súvisiacich aktív, ktorých sa analýza rizík týka. K základným aktívam patria dáta (v elektronickej podobe), služby, dokumenty (dáta v inej ako elektronickej podobe), softvér, hardvér, sieťová a telekomunikačná infraštruktúra, budovy, priestory, ľudia.

Metodológie na vypracovanie analýzy rizík môžu byť formálne alebo neformálne, detailné alebo zjednodušené, kvantitatívne (výpočtovo orientované) alebo kvalitatívne (postavené na popisoch či hodnoteniach). Neexistuje jednoznačná metodológia vhodná pre všetky prostredia a všetkých užívateľov.

Metodológia, podľa ktorej postupujú experti spoločnosti GORDIAS, má neformálny, kvalitatívny charakter, s optimalizovanou detailnosťou podľa konkrétneho projektu. Vždy je syntézou medzinárodne akceptovaných štandardov a odporúčaní.

Takto vytvorená metodológia má univerzálne použitie:

- Kvalitatívna metodológia je vhodná na ľubovoľné elementy, z ktorých vyplýva riziko.
- Jej terminológia je dobre zrozumiteľná.
- Je optimálna pre prostredia, kde je ťažké presne určiť hodnoty rizikových elementov.

Zber a syntéza dát, uskutočnenie analýzy rizík

Prvým krokom tejto fázy je zber dát. Jeho cieľom je:

- identifikácia a ohodnotenie aktív,
- identifikácia a analýza možných a aplikovateľných hrozieb,
- identifikácia a analýza bezpečnostných slabín,
- určenie dôsledkov naplnenia hrozieb.

Identifikácia a ohodnotenie aktív

Základné aktíva (dáta, dokumenty, softvér, hardvér, sieťová a telekomunikačná infraštruktúra, budovy, priestory, ľudia) majú svoje špecifiká v každej inštitúcii. K nim je potrebné priradiť priority ochrany na základe ich ceny, senzitivity, nutnosti pre správny chod infraštruktúry a pod.

Identifikácia a analýza možných a aplikovateľných hrozieb

V tomto kroku sú najskôr identifikované a popísané všetky relevantné hrozby pre analyzované prostredie aj s pravdepodobnosťou ich naplnenia. Potom sú určené aplikovateľné hrozby.

Identifikácia a analýza bezpečnostných slabín

Úroveň rizika je určená vzťahmi medzi hrozbami a bezpečnostnými slabínami. Riziko je redukované implementáciou bezpečnostného opatrenia. Jednotlivé bezpečnostné slabiny a hrozby je potrebné združiť do vzájomných vzťahov, čím sa analýza prispôbuje konkrétnemu prostrediu.

Určenie dôsledkov naplnenia hrozieb

V prípade, že by sa hrozba realizovala, aktívum by bolo postihnuté určitým dôsledkom. Dôsledky sú rôzne: zničenie, zabránenie prístupu k službe, prezradenie, modifikácia.

Interpretácia výsledkov analýzy rizík

Interpretácia jasne a explicitne prezentuje výsledky analýzy rizík vo forme záverečnej správy. Z tejto správy jednoznačne vyplýva ďalší postup plánovania, výberu a návrhu implementácie bezpečnostných opatrení.

Ak veríte v úspešnú budúcnosť vašej firmy, jedným z najdôležitejších krokov na vašej ceste do tejto budúcnosti je Analýza rizík informačného systému, ktorú vám ponúka spoločnosť GORDIAS.

