[AINIGMA]®

svetovanje za varno poslovanje

Ainigma d.o.o.
Kamnogoriška cesta 45
1117 Ljubljana
T +386 (0)599 69518
F +386 (0)1 282 11 46

E info@ainigma.si
I www.ainigma.si

ID DDV SI13039512
MŠ 22280009
TR NLB/02053-0255896275

Sistem upravljanja varovanja informacij

Prodor informacijskih in komunikacijskih tehnologij v praktično vse poslovne procese je povzročil, da so problemi varovanja poslovanja postali predvsem informacijski varnostni problemi, zagotavljanje varnega poslovanja organizacije pa predvsem vprašanje oziroma problem zagotavljanja informacijske varnosti. Sodobno poslovno okolje postavlja gospodarske družbe in druge organizacije ter organe (vnaprej: organizacije) pred nove varnostne izzive in tveganja. Obravnavanje in upravljanje varnostnih tveganj postaja sestavni in neločljivi del obravnavanja in upravljanja poslovnih tveganj.

Organizacija posluje varno, če z ustreznimi ukrepi in postopki zmanjša ali odpravi verjetnost (tveganje), da bi ji kakšna nevarnost ali grožnja preprečila oziroma onemogočila doseganje poslovnih ciljev oziroma kako drugače škodovala njenemu poslovanju.

Ukrepe in postopke, s katerimi bo organizacija zagotavljala tako raven varnosti svojega poslovanja, da bo, ob spoštovanju pravnega reda v okolju, v katerem deluje, dosegala želene poslovne cilje, na eni strani opredeljujejo predpisi in standardi, ki jih je dolžna spoštovati, na drugi strani pa norme, pravila in dobre prakse, ki jih želi izvajati zato, ker ji zagotavljajo nujne (pred)pogoje za tržno tekmo s konkurenti, optimalno učinkovitost in uspešnost ter zanesljivo in neprekinjeno poslovanje.

Čeprav ne gre zmanjševati pomena materialnih sredstev, objektov in drugih materializirinah virov, so osrednji dejavnik, ki narekuje varnostno organiziranost, praviloma neopredmetena sredstva oziroma intelektualni kapital organizacije. To so podatki in informacije, ki jih organizacije zbirajo, obdelujejo, uporabljajo, in hranijo v okviru svojega poslovanja, in so rezultat njihovih preteklih dejavnosti in spoznanj oziroma sestavni del aktualnih ali prihodnjih aktivnosti. Med te podatke in informacije sodijo tako osebni podatki strank, zaposlenih in drugih sodelavcev, kot tudi različne vrste drugih podatkov in informacij, katerih dostopnost organizacija zaradi predpisov ali lastne odločitve omeji na določen krog uporabnikov (npr. podatki, ki so internega značaja, podatki, ki so določeni za poslovno tajnost oziroma skrivnost, tajni podatki z delovnega področja državnih organov ipd.).

Predpisi, ki urejajo dolžnosti organizacij in drugih upravljavcev glede obdelave posameznih kategorij varovanih podatkov, postopke in ukrepe varovanja podatkov urejajo različno natančno in podrobno. Njihova skupna značilnost pa je, da so temeljne zahteve glede vseh kategorij podatkov za vse upravljavce enake: vsi morajo izvajati postopke in ukrepe, s katerimi zagotavljajo, da so varovani podatki v želenih časovnih in prostorskih okvirih dostopni le upravičenim oziroma pooblaščenim uporabnikom, ter da se skozi celotni življenjski ciklus podatkov ohranja njihova zaupnost, celovitost in dostopnost. Vsi predpisi tudi zahtevajo, da mora biti upravljavec podatkov za določeno preteklo obdobje sposoben naknadno ugotoviti, kdaj so bili posamezni varovani podatki zajeti, uporabljeni ali drugače obdelani in kdo je to storil.

Podjetje Ainigma vam lahko pomaga tako pri določitvi kot pri izvedbi potrebnih aktivnosti za izboljšanje varnosti vašega poslovanja s podatki in informacijami. Pristop k izvedbi teh dejavnosti praviloma temelji na metodologiji, določeni s standardom ISO/IEC 27002 : 2005, ob upoštevanju drugih standardov, dobrih praks in predpisov, relevantnih za posamično organizacijo. Rezultat skupnega dela je delujoč sistem upravljanja varovanja informacij in varovanja drugih virov, pomembnih za poslovanje organizacije, podprt z ustreznimi normativnimi, organizacijskimi ter tehnološko – tehničnimi postopki in ukrepi. Dokumentiranje aktivnosti poteka tako, da lahko organizacija, če to želi, skozi postopek certificiranja, določen s standardom ISO/IEC 27001 : 2005, preko zunanje presoje formalno preveri, ali dejansko izpolnjuje zahteve varovanja podatkov in informacij.