REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO

DIREKTORAT ZA INFORMACIJSKO DRUŽBO

Tržaška cesta 21, 1000 Ljubljana

T: 01 478 47 78
F: 01 478 83 31
E: gp.mju@gov.si
www.mju.gov.si

Strokovna, zainteresirana in druga javnost

Številka: IPP 386-18/2018/1
Datum: 13. 2. 2019

Zadeva: Javna obravnava osnutka predloga Pravilnika o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev

Ministrstvo za javno upravo (MJU) je pripravilo osnutek predloga Pravilnika o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev (v nadaljnjem besedilu: pravilnik), ki se ga sprejme na podlagi tretjega odstavka 12. člena Zakona o informacijski varnosti (Uradni list RS, št. 30/18; v nadaljnjem besedilu: ZInfV).

ZInfV ureja področje informacijske varnosti in ukrepe za doseganje visoke ravni varnosti omrežij in informacijskih sistemov v Republiki Sloveniji, ki so bistvenega pomena za nemoteno delovanje države v vseh varnostnih razmerah ter zagotavljajo bistvene storitve za ohranitev ključnih družbenih in gospodarskih dejavnosti v RS. ZInfV predvideva, da so med zavezanci po tem zakonu tudi izvajalci bistvenih storitev (v nadaljnjem besedilu: IBS), ki za zagotavljanje informacijske varnosti in visoke varnosti omrežij in informacijskih sistemov vzpostavijo in vzdržujejo dokumentiran sistem upravljanja varovanja informacij ter sistem upravljanja neprekinjenega poslovanja.

S pravilnikom se tako podrobneje določa vsebino in strukturo varnostne dokumentacije, metodologiji za pripravo analize obvladovanja tveganj in za določitev ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov ter minimalni obseg ter vsebino varnostnih ukrepov IBS.

Pravilnik skladno z 12. členom ZInfV določa, da mora varnostna dokumentacija IBS za zagotavljanje informacijske varnosti ter visoke ravni varnosti omrežij in informacijskih sistemov obsegati najmanj:

- analizo obvladovanja tveganj z oceno sprejemljive ravni tveganj;
- politiko neprekinjenega poslovanja z načrtom njegovega upravljanja;
- seznam njegovih ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov, ki so bistvenega pomena za delovanje bistvenih storitev;
- načrt obnovitve in ponovne vzpostavitve delovanja informacijskih sistemov iz prejšnje alineje;
- načrt odzivanja na incidente s protokolom obveščanja nacionalnega CSIRT;

- načrt varnostnih ukrepov za zagotavljanje celovitosti, zaupnosti in razpoložljivosti omrežja in informacijskih sistemov, ki upoštevajo področne posebnosti.

Pravilnik sledi zakonu tako, da določa, da če ima IBS za zagotavljanje varnosti svojih omrežij in informacijskih sistemov že izdelano varnostno dokumentacijo na podlagi drugih predpisov, jo vsebinsko dopolni skladno s tem pravilnikom.

Pravilnik tudi določa, kako IBS pripravi analizo obvladovanja tveganj z oceno sprejemljive ravni tveganj ter kako pripravi seznam svojih ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov, ki so bistvenega pomena za delovanje bistvenih storitev. Pri tem pravilnik še določi, da IBS ta dva postopka izvaja v rednih časovnih presledkih ali kadar so predlagane ali nastanejo bistvene spremembe v okviru sistema upravljanja informacijske varnosti, ta dva postopka pa morata biti izvedena tako, da so njuni rezultati dosledni, primerljivi in veljavni.

Pravilnik podrobneje določa tudi minimalni obseg in vsebino varnostnih ukrepov, ki jih sprejme IBS (organizacijski, logično-tehnični in tehnični ukrepi).

Zainteresirano javnost vabimo, naj svoje morebitne pripombe in predloge na ta osnutek pravilnika poda v roku 30 dni od te objave.

S spoštovanjem,

dr. Uroš Svete
v. d. generalnega direktorja