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: 007-644/2017-1
Datum: 07. 09. 2017

Zadeva: Javna obravnava osnutka predloga Zakona o informacijski varnosti – redni postopek

Ministrstvo za javno upravo (MJU) je pripravilo osnutek predloga Zakona o informacijski varnosti (v nadaljevanju: ZIV). Z ZIV se sistemsko ureja področje informacijske varnosti v Republiki Sloveniji (v nadaljevanju: RS) ter se hkrati v nacionalni pravni red prenaša Direktiva 2016/1148/ES Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (Direktiva NIS) (UL L št. 194 z dne 19. 7. 2016, str. 1- 30).

K normativni ureditvi sistema za zagotavljanje informacijske varnosti državo spodbujajo in hkrati zavezujejo sprejeti strateški dokumenti na nacionalni in mednarodni ravni. O tem govorijo Resolucija o strategiji nacionalne varnosti RS[1], Strategija kibernetske varnosti[2], Strategija kibernetske varnosti Evropske unije »Odprt, varen in zavarovan kibernetski prostor«[3] ter že omenjena Direktiva 2016/1148/ES Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji[4].

[1] Resolucija o strategiji nacionalne varnosti Republike Slovenije. V: Uradni list RS [online], 2010, št. 27/2010, točka 5.3.5 Odzivanje na kibernetske grožnje in zlorabo informacijskih tehnologij in sistemov. Dostopno na: http://www.pisrs.si/Pis.web/pregledPredpisa?id=RESO61.

[2] Strategija kibernetske varnosti. Dostopno na: http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/DID/Informacijska_druzba/pdf/DSI2020_Strategija_Kibernetske_Varnosti.pdf

[3] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Digital Agenda for Europe - A Europe 2020 Initiative [online], 2013. Dostopno na: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

[4] Direktiva 2016/1148/ES Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji. Dostopno na: http://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32016L1148&from=SL

Predlog ZIV ureja ukrepe za doseganje visoke ravni varnosti omrežij in informacijskih sistemov v RS, ki so bistvenega pomena za nemoteno delovanje države v vseh varnostnih razmerah, ureja zagotavljanje bistvenih storitev za ohranitev ključnih družbenih in gospodarskih dejavnosti ter ureja zagotavljanje informacijske varnosti in kibernetske obrambe v RS. Določa minimalne varnostne zahteve in zahteve za priglasitev incidentov za zavezance tega zakona. Prav tako ureja pristojnosti, naloge, organizacijo in delovanje pristojnega nacionalnega organa, enotne kontaktne točke in posameznih skupin za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij (v nadaljevanju: CSIRT) na področju zagotavljanja informacijske varnosti in kibernetske obrambe ter ureja posamezna področja varovanja in posredovanja informacij, podatkov ter zaščite le-teh v opredeljenih omrežjih in informacijskih sistemih.

Predlog ZIV skladno z direktivo NIS med zavezanci zakona opredeljuje izvajalce bistvenih storitev in ponudnike digitalnih storitev. Izvajalci bistvenih storitev so subjekti, ki delujejo v sedmih sektorjih, vključitev katerih je po direktivi NIS obvezna:

- energija,
- digitalna infrastruktura,
- oskrba s pitno vodo in njena distribucija,
- zdravstvo,
- promet,
- bančništvo in
- infrastruktura finančnega trga.

Za potrebe ZIV je dodan še sektor zagotavljanja delovanja ključnih delov nacionalnega varnostnega sistema ter državnih organov in lokalnih skupnosti.

Za potrebe ZIV so digitalne storitve, ki jih ponujajo njihovi ponudniki storitve spletne tržnice, spletnega iskalnika in računalništva v oblaku.

Določbe ZIV se ne uporabljajo za operaterje elektronskih komunikacij, za katere veljajo posebne obveznosti glede varnosti in celovitosti omrežij in storitev, kot so vzpostavljene z evropskim regulativnim okvirjem na področju elektronskih komunikacij (natančneje s 13a in 13b členoma Okvirne direktive[5]), in so prenešene v zakonu, ki ureja elektronske komunikacije (ZEKom-1), ter za ponudnike storitev zaupanja, za katere veljajo zahteve iz 19. člena Uredbe (EU) št. 910/2014 (t .i. Uredba eIDAS).

Metodologijo za določitev bistvenih storitev in njihovih izvajalcev mora država določiti sama, medtem ko se za ponudnike digitalnih storitev uporabijo enotna merila, sprejeta na ravni EU. Pri določitvi izvajalcev bistvenih storitev mora država poleg specifičnih sektorsko pogojenih meril upoštevati predvsem naslednja merila:

- subjekt zagotavlja storitev, ki je bistvena za ohranitev ključnih družbenih oziroma gospodarskih dejavnosti;
- zagotavljanje te storitve je odvisno od omrežij in informacijskih sistemov ter
- incident bi imel pomemben negativen vpliv na zagotavljanje te storitve.

[5] Direktiva 2002/21/ES Evropskega parlamenta in Sveta z dne 7. marca 2002 o skupnem regulativnem okviru za elektronska komunikacijska omrežja in storitve (Okvirna direktiva) (UL L št. 108 z dne 24. 4. 2002, str. 33), zadnjič spremenjena z Direktivo 2009/140/ES

Metodologija za določitev izvajalcev bistvenih storitev, ki upošteva tudi sektorske dejavnike, bo podrobneje predpisana v podzakonskem aktu ZIV.

Predlog ZIV definira varnostne zahteve in način priglasitve incidentov tako za izvajalce bistvenih storitev kot tudi za ponudnike digitalnih storitev. Poleg tega opredeli vsebino seznamov, ki se vodijo po tem zakonu in potrebno varnostno dokumentacijo ter varnostne ukrepe na strani zavezancev in na strani pristojnih organov.

Z organizacijskega vidika predlog ZIV opredeli naloge in pristojnosti pristojnega nacionalnega organa, nacionalnega in vladnega CSIRT, način njihovega medsebojnega sodelovanja ter njihovo sodelovanje z ostalimi deležniki na področju zagotavljanja informacijske varnosti. Pristojnosti na področju kibernetske varnosti trenutno že opravlja Urad Vlade Republike Slovenije za varovanje tajnih podatkov (UVTP), z ustanovitvijo in pričetkom delovanja pristojnega nacionalnega organa po ZIV (predvidoma s 1. 1. 2019) pa bo le-ta od UVTP-ja prevzel naloge, arhive in dokumentacijo, ki se nanašajo na kibernetsko varnost ter opravljal z ZIV delegirane naloge.

Nacionalni CSIRT začne izvajati naloge skladno z ZIV dne 1. 1. 2019, po predhodni določitvi izvajalca nalog CSIRT s strani Vlade RS. Do 1. 1. 2019 izvaja naloge nacionalnega CSIRT odzivni center SI-CERT pri Akademski in raziskovalni mreži Slovenije. Vladni CSIRT pa bo vzpostavljen na MJU.

Naloge inšpekcijskega nadzora in odločanja o prekrških se bodo po ZIV izvajale s strani inšpektorjev, inšpektorata pristojnega za informacijsko varnost. Zato bo MJU pripravil tudi predlog za uskladitev uredbe, ki ureja organe v sestavi ministrstev, z določbami ZIV, ki jo sprejme Vlada RS.

Vzporedno z ZIV MJU pripravlja tudi uredbo o informacijski varnosti, ki bo določila minimalne skupne zahteve informacijske varnosti, ki vključujejo enotne okvire upravljanja informacijske varnosti in temeljna nadzorstva za zagotavljanje informacijske varnosti v organih državne uprave.

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

S spoštovanjem,

mag. Bojan Križ
v.d. generalnega direktorja