OSNUTEK PREDLOGA 13. 6. 2025

Na podlagi šestega odstavka 20. člena Zakona o informacijski varnosti (Uradni list RS, št. 40/25), Vlada Republike Slovenije izdaja

UREDBO O USPOSABLJANJU ODGOVORNIH OSEB NA PODROČJU OBVLADOVANJA TVEGANJ INFORMACIJSKE IN KIBERNETSKE VARNOSTI

I. SPLOŠNE DOLOČBE

1. člen

(vsebina uredbe)

Ta uredba določa program in način usposabljanja odgovornih oseb bistvenih ali pomembnih subjektov iz prvega odstavka 20. člena Zakona o informacijski varnosti (Uradni list RS, št.-40/21; v nadaljnjem besedilu: ZInfV-1) na področju obvladovanja tveganj informacijske in kibernetske varnosti ter njihovega vpliva na dejavnosti oziroma storitve, ki jih izvaja subjekt, z namenom zagotavljanja visoke ravni varnosti omrežij in informacijskih sistemov ter zaščite pred kibernetskimi grožnjami.

2. člen

(področje uporabe)

Uredba velja za vse pravne osebe, samostojne podjetnike posameznike ali posameznike, ki samostojno opravljajo dejavnost, državne organe, organe lokalnih skupnosti, javne agencije, nosilce javnih pooblastil, druge osebe javnega prava in druge subjekte, ki so bistveni ali pomembni subjekti na podlagi ZInfV-1.

3. člen

(cilji usposabljanja)

Cilji usposabljanja so:

1. povečanje ozaveščenosti o tveganjih na področju informacijske in kibernetske varnosti;

2. pridobitev temeljnega znanja o ključnih grožnjah in ranljivostih, ki vplivajo na omrežja, informacijske sisteme in podatke;

3. izboljšanje znanja in veščin za prepoznavanje, ocenjevanje in obvladovanje varnostnih tveganj;

4. pridobitev temeljnega znanja o načrtovanju in izvajanju neprekinjenega poslovanja;

5. seznanitev z obveznostmi glede varnosti dobavnih verig;

6. seznanitev s postopki za izvajanje dolžnega nadzorstva nad izvajanjem varnostnih ukrepov in postopkov za obvladovanje tveganj informacijske in kibernetske varnosti za zagotavljanje skladnosti z zakonodajo in predpisi na področju informacijske varnosti.

II. PROGRAM IN IZVAJANJE USPOSABLJANJA

4. člen

(vsebina programa)

(1) Program usposabljanja obsega naslednje vsebine:

1. uvod v informacijsko in kibernetsko varnost, zakonodaja, regulative ter mednarodni standardi;

2. upravljanje sredstev in upravljanje tveganj;

3. ocena vplivov na poslovanje in neprekinjeno poslovanje;

4. odzivanje na incidente informacijske varnosti;

5. varnost dobavnih verig;

6. izvajanje dolžnega nadzorstva in pogoste ugotovitve neskladja s predpisi iz inšpekcijskih nadzorov.

(2) Usposabljanje se izvede po Programu usposabljanja iz Priloge 1, ki je kot priloga sestavni del te uredbe.

5. člen

(izvajalec usposabljanja)

(1) Usposabljanje izvaja pristojni nacionalni organ za informacijsko varnost (v nadaljnjem besedilu: izvajalec usposabljanja) prek njegovih uslužbencev, ki imajo ustrezne strokovne kompetence in jih s sklepom imenuje predstojnik pristojnega nacionalnega organa za informacijsko varnost.

(2) Za izvedbo posameznih vsebin usposabljanja lahko na podlagi strokovne presoje predstojnika pristojnega nacionalnega organa za informacijsko varnost sodelujejo tudi uslužbenci skupin CSIRT.

6. člen

(trajanje in način izvedbe)

(1) Usposabljanje, ki je za udeležence brezplačno, traja najmanj osem pedagoških ur in se izvaja v obliki predavanja ali delavnice. Del usposabljanja se lahko izvede tudi na daljavo.

(2) Pristojni nacionalni organ za informacijsko varnost vsako koledarsko leto razpiše termine usposabljanj, kjer navede tudi način izvedbe prijave na usposabljanje.

(3) Prijave na ponovno usposabljanje je možno oddati šest mesecev pred pretekom izdanega potrdila o usposobljenosti.

(4) Pogoj za uspešno opravljeno usposabljanje in pridobitev potrdila o usposobljenosti je prisotnost na celotnem predpisanem usposabljanju.

7. člen

(potrdilo o usposobljenosti)

(1) Potrdilo o usposobljenosti izda izvajalec usposabljanja praviloma v tridesetih delovnih dneh po končanem usposabljanju. Potrdilo je v elektronski obliki.

(2) Potrdilo iz prejšnjega odstavka velja štiri leta. Po preteku tega obdobja je treba ponovno opraviti usposabljanje po programu in na način iz te uredbe.

8. člen

(evidenca potrdil)

(1) Izvajalec usposabljanja vodi elektronsko evidenco izdanih potrdil o usposobljenosti, ki vsebuje podatke o udeležencih, datumu usposabljanja, številki potrdila in veljavnosti potrdila.

(2) V evidenci izdanih potrdil o usposobljenosti se vodijo naslednji podatki:

- ime in priimek udeleženca usposabljanja;

- enotno matično številko občana za državljane Republike Slovenije ali datum rojstva za tuje državljane;

- datum uspešno opravljenega usposabljanja in

- evidenčno številko izdanega potrdila.

(3) Upravljalec evidence izdanih potrdil o usposobljenosti mora zagotoviti nepovratno brisanje pretečenih potrdil in pripadajočih podatkov iz evidence v letu, ki sledi letu, v katerem je pretekla veljavnost potrdil.

(4) Za pripravo letnih poročil o delovanju pristojnega nacionalnega organa za informacijsko varnost se podatki, ki izhajajo iz evidence potrdil o usposobljenosti, lahko obdelujejo samo v anonimizirani obliki.

III. KONČNA DOLOČBA

9. člen

(začetek veljavnosti)

Ta uredba začne veljati petnajsti dan po objavi v Uradnem listu Republike Slovenije.

PRILOGA 1

PROGRAM USPOSABLJANJA

1. Uvod v informacijsko in kibernetsko varnost, zakonodaja, regulative in mednarodni standardi

• Osnovni pojmi in definicije: Razumevanje temeljnih pojmov in konceptov informacijske in kibernetske varnosti.

• Pregled trenutnih groženj in trendov: Pregled in analiza aktualnih groženj in trendov v informacijski in kibernetski varnosti.

• Nacionalna zakonodaja: Pregled relevantne zakonodaje, ZInfV-1 in predpisi, izdani na njegovi podlagi.

• Evropski predpisi: Pregled evropskih predpisov, ki veljajo za posamezne sektorje in zavezance: uredbe, izvedbene uredbe, drugi akti.

• Mednarodni standardi: Pregled mednarodnih standardov in dobrih praks, kot so NIST CSF, ISO/IEC 27001, COBIT, ISO/IEC 22301.

2. Upravljanje sredstev in upravljanje tveganj

• Identifikacija in popis sredstev: Prepoznavanje in klasifikacija informacijskih sredstev oziroma virov ter izvedba njihovega popisa.

• Identifikacija tveganj: Metode za prepoznavanje varnostnih tveganj.

• Ocena tveganj: Tehnike za ocenjevanje tveganj in določanje njihovega vpliva.

• Obvladovanje tveganj: Razvoj in implementacija strategij za obvladovanje tveganj.

3. Ocena vplivov na poslovanje in neprekinjeno poslovanje

• Ocena vplivov na poslovanje (BIA): Metode za ocenjevanje vplivov varnostnih incidentov na poslovanje.

• Načrti za neprekinjeno poslovanje (BCP): Priprava politike in načrta za zagotavljanje neprekinjenega poslovanja v primeru incidentov.

4. Odzivanje na incidente informacijske varnosti

• Praktičen prikaz incidenta informacijske varnosti: Prikaz pojava incidenta v omrežju in informacijskih sistemih, odziva in posledic.

• Odzivanje in sanacija: Postopki za učinkovito odzivanje na incidente in njihovo sanacijo.

5. Varnost dobavnih verig

• Identifikacija tveganj in ukrepi za zaščito dobavne verige: Prepoznavanje in ocenjevanje tveganj, povezanih z dobavnimi verigami, implementacija varnostih ukrepov za zaščito pred tveganji informacijske in kibernetske varnosti ter izvajanje nadzorstva nad ključnimi dobavitelji.

• Minimalne zahteve vsebine pogodb za pogodbene partnerje za področje informacijske varnosti: Varnostni ukrepi, ukrepi za neprekinjeno poslovanje, obveščanje o incidentih, ravnanje s podatki in možnost preverjanja izvajanja varnostne klavzule.

6. Izvajanje dolžnega nadzorstva in pogoste ugotovitve neskladja s predpisi iz inšpekcijskih nadzorov

• Seznanitev z izvajanjem dolžnega nadzorstva: Razvoj sposobnosti in postopkov za izvajanje dolžnega nadzorstva nad varnostnimi ukrepi in postopki.

• Seznanitev s pogostimi ugotovitvami neskladij s predpisi, ki so bili ugotovljeni v inšpekcijskih nadzorih in podanih priporočilih za izboljšanje varnosti ali učinkovitosti.

OBRAZLOŽITEV

I. UVOD

1. Pravna podlaga (besedilo, vsebina zakonske določbe, ki je podlaga za izdajo uredbe)

Predlagana uredba se izdaja na podlagi šestega odstavka 20. člena Zakona o informacijski varnosti (Uradni list RS, št. 40/25; v nadaljnjem besedilu: ZInfV-1).

Šesti odstavek 20. člena ZInfV-1 določa:
»(6) Pristojni nacionalni organ je pristojen za organiziranje usposabljanja odgovornih oseb iz prvega odstavka tega člena. Program in način izvajanja usposabljanja odgovornih oseb na področju informacijske in kibernetske varnosti določi vlada na predlog pristojnega nacionalnega organa.«.

2. Rok za izdajo uredbe, določen z zakonom

Prvi odstavek 64. člena ZInfV-1 sicer določa, da se Vlada izda predpisa iz tretjega odstavka 4. člena in šestega odstavka 20. člena tega zakona v šestih mesecih od uveljavitve tega zakona.

ZInfV-1 je bil v Državnem zboru Republike Slovenije sprejet po nujnem postopku, zato se predvideva sprejetje podzakonskih predpisov v najkrajšem možnem času.

3. Splošna obrazložitev predloga uredbe, če je potrebna

Direktiva 2022/2555/EU Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2) (UL L št. 333 z dne 27. 12. 2022, str. 80), zadnjič popravljeno s Popravkom (UL L št. 90348 z dne 12. 6. 2024, str. 139), (v nadaljnjem besedilu: Direktiva 2022/2555/EU) v drugem odstavku 20. člena določa, da države članice zagotovijo, da se morajo člani upravljalnega organa bistvenih in pomembnih subjektov usposabljati, in spodbujajo bistvene in pomembne subjekte, da podobno usposabljanje redno ponujajo svojim zaposlenim, da pridobijo dovolj znanja in spretnosti, ki jih usposobi za prepoznavanje in ocenjevanje tveganj in za oceno praks obvladovanja tveganj za kibernetsko varnosti ter njihovega vpliva na storitve, ki jih opravlja subjekt.

ZInfV-1 je sistemski zakon, ki ureja področje informacijske in kibernetske varnosti, določa nacionalni sistem informacijske varnosti v Republiki Sloveniji in je v naš pravni red v celoti prenesel Direktivo 2022/2555/EU, vključno z drugim odstavkom 20. člena te direktive.

ZInfV-1 pa v povezavi z usposabljanjem odgovornih oseb bistvenih in pomembnih subjektov vsebuje tudi nacionalno določbo šestega odstavka 20. člena tega zakona, ki določa pristojnost prisojnega nacionalnega organa za organiziranje usposabljanja odgovornih oseb iz prvega odstavka tega člena, pri čemer vlada na njegov predlog določi program in način izvajanja usposabljanja odgovornih oseb na področju informacijske in kibernetske varnosti

S predlagano uredbo Vlada Republike Slovenije torej določa: program in način usposabljanja odgovornih oseb bistvenih ali pomembnih subjektov iz prvega odstavka 20. člena Zakona o informacijski varnosti (Uradni list RS, št.-40/21; v nadaljnjem besedilu: ZInfV-1) na področju

obvladovanja tveganj informacijske in kibernetske varnosti ter njihovega vpliva na dejavnosti oziroma storitve, ki jih izvaja subjekt, z namenom zagotavljanja visoke ravni varnosti omrežij in informacijskih sistemov ter zaščite pred kibernetskimi grožnjami.

4. Predstavitev presoje posledic za posamezna področja, če te niso mogle biti celovito predstavljene v predlogu zakona

Presoja posledic in učinkov ZInfV-1 za posamezna področja je bila celovito predstavljena v predlogu ZInfV-1 in se nanaša tudi na predlagano Uredbo o usposabljanju odgovornih oseb na področju obvladovanja tveganj informacijske in kibernetske varnosti (v nadaljnjem besedilu: uredba).

II. VSEBINSKA OBRAZLOŽITEV PREDLAGANIH REŠITEV

SPLOŠNE DOLOČBE

Namen predloga uredbe je določitev načina in postopka usposabljanja odgovornih oseb bistvenih in pomembnih subjektov na področju obvladovanja tveganj informacijske in kibernetske varnosti ter njihovega vpliva na dejavnosti oziroma storitve, ki jih izvaja subjekt, z namenom zagotavljanja visoke ravni varnosti omrežij in informacijskih sistemov ter zaščite pred kibernetskimi grožnjami.

ZInfV- v prvem odstavku 20. člena določa, da so za izvajanje ukrepov iz 21. in 22. člena ZInfV-1 odgovorni predstojniki subjektov javne uprave, in odgovorne osebe pravnih oseb, to so fizične osebe, ki vodijo, nadzorujejo ali upravljajo poslovanje pravne osebe oziroma so po zakonu, aktu o ustanovitvi ali pooblastilu pristojne in dolžne zagotoviti zakonito delovanje (v nadaljnjem besedilu: odgovorne osebe) bistvenih ali pomembnih subjektov.

Tretji odstavek 20. člena ZInfV-1določa, da se odgovorne osebe najmanj vsaka štiri leta izobražujejo oziroma usposabljajo na področju obvladovanja tveganj informacijske in kibernetske varnosti ter njihovega vpliva na dejavnosti ali storitve, ki jih izvaja subjekt.

Šesti odstavek 20. člena ZInfV-1 določa, da je pristojni nacionalni organ pristojen za organiziranje usposabljanja odgovornih oseb iz prvega odstavka 20. člena ZInfV-1. Program in način izvajanja usposabljanja odgovornih oseb na področju informacijske in kibernetske varnosti določi vlada na predlog pristojnega nacionalnega organa.

Uredba velja za vse pravne osebe, samostojne podjetnike posameznike ali posameznike, ki samostojno opravljajo dejavnost, državne organe, organe lokalnih skupnosti, javne agencije, nosilce javnih pooblastil, druge osebe javnega prava in druge subjekte, ki so bistveni ali pomembni subjekti na podlagi ZInfV-1.

Glavni cilji usposabljanja sledijo ciljem iz ZInfV-1 in sicer so povečanje ozaveščenosti o tveganjih na področju informacijske in kibernetske varnosti; pridobitev temeljnega znanja o ključnih grožnjah in ranljivostih, ki vplivajo na omrežja, informacijske sisteme in podatke; izboljšanje znanja in veščin za prepoznavanje, ocenjevanje in obvladovanje varnostnih tveganj; pridobitev temeljnega znanja o načrtovanju in izvajanju neprekinjenega poslovanja; seznanitev z obveznostmi glede varnosti dobavnih verig in seznanitev s postopki za izvajanje dolžnega nadzorstva nad izvajanjem varnostnih ukrepov in postopkov za obvladovanje tveganj informacijske in kibernetske varnosti za zagotavljanje skladnosti z zakonodajo in predpisi na področju informacijske varnosti.

IZVAJANJE IN PROGRAM USPOSABLJANJA

Usposabljanje izvaja Urad Vlade Republike Slovenije za informacijsko varnost (v nadaljnjem besedilu: URSIV), ki je pristojni nacionalni organ za informacijsko varnost prek njegovih uslužbencev, ki morajo imeti ustrezne strokovne kompetence in jih imenuje direktor URSIV. Za izvedbo posameznih vsebin usposabljanja lahko sodelujejo tudi uslužbenci skupin CSIRT. Udeležba na usposabljanju je za udeležence brezplačna.

URSIV za vsako koledarsko leto razpiše termine usposabljanj, kjer navede tudi način izvedbe prijave na usposabljanje. Prijave na ponovno usposabljanje je možno oddati šest mesecev pred pretekom izdanega potrdila o usposobljenosti.

Usposabljanje traja najmanj osem pedagoških ur po 45 minut in se izvaja v obliki predavanja ali delavnice, del usposabljanja se lahko izvede tudi na daljavo. Pogoj za uspešno opravljeno usposabljanje in pridobitev potrdila o usposobljenosti je prisotnost na celotnem predpisanem usposabljanju.

Potrdilo o usposobljenosti izda izvajalec usposabljanja praviloma v tridesetih delovnih dneh po končanem usposabljanju v elektronski oblik in velja štiri leta. Po preteku tega obdobja je potrebno ponovno opraviti usposabljanje.

URSIV vodi elektronsko evidenco izdanih potrdil o usposobljenosti, ki vsebuje podatke o udeležencih, datumu usposabljanja, številki potrdila in veljavnosti potrdila.

Program usposabljanja je sestavljen iz šestih vsebinskih sklopov in sicer: 1. uvod v informacijsko in kibernetsko varnost, zakonodaja, regulative ter mednarodni standardi; 2. upravljanje sredstev in upravljanje tveganj; 3. ocena vplivov na poslovanje in neprekinjeno poslovanje; 4. odzivanje na incidente informacijske varnosti; 5. varnost dobavnih verig; 6. izvajanje dolžnega nadzorstva in pogoste ugotovitve neskladja s predpisi iz inšpekcijskih nadzorov. Bolj natančno je vsebina programa določena v Prilogi 1, ki je kot priloga sestavni del te uredbe.

KONČNA DOLOČBA

Uredba začne veljati petnajsti dan po objavi v Uradnem listu Republike Slovenije, kar je običajen rok za uveljavitev predpisov.

PRILOGA 1

V prilogi je natančneje določena vsebina vsakega od šestih vsebinskih sklopov, ki zasleduje cilje usposabljanja, določene v 3. členu uredbe. Vsebina posameznih sklopov je bila določena na podlagi mednarodnih standardov in dobrih praks na področju informacijske in kibernetske varnosti ter pridobljenih izkušenj pri izvajanju prejšnjega Zakona o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23; ZInfV).