REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE ZA INFORMACIJSKO VARNOST

URSIV

Zakon o informacijski varnosti ZInfV-1: pogosta vprašanja in odgovori

Odgovori na pogosta vprašanja o novem Zakonu o informacijski varnosti (ZInfV-1)

Uvodoma pojasnjujemo, da za odločanje o razlagi in uporabi Direktive (EU) 2022/2555 (NIS 2) ni pristojen Urad Vlade Republike Slovenije za informacijsko varnost (URSIV), ampak na podlagi Pogodbe o delovanju Evropske unije (PDEU) Sodišče EU opravlja nadzor nad zakonitostjo aktov EU ter odloča o veljavnosti in razlagi aktov EU. Posredovana pojasnila tudi nimajo vpliva na morebitne upravne, sodne in druge postopke, sprožene na podlagi ZInfV-1 ali Direktive NIS 2, ker lahko posamezni pristojni organi pri odločanju zavzamejo drugačno stališče. Prav tako s podanimi pojasnili ne nastane svetovalno oziroma pooblastilno razmerje v smislu stranka: pooblaščenec.

Pojasnjujemo še, da vsebina ZInfV-1 v pretežni meri izhaja iz Direktive NIS 2, med tem ko so nekatere njegove določbe povsem nacionalnega izvora in se ne prevzemajo iz omenjene direktive. Kot izhaja iz člena 5 Direktive NIS 2 gre za direktivo minimalne harmonizacije, kar pomeni, da lahko države članice pri prenosu te direktive sprejmejo ali ohranijo določbe, ki zagotavljajo višjo raven kibernetske varnosti pod pogojem, da so take določbe v skladu z obveznostmi držav članic, določenimi v pravu EU.

Kazalo vprašanj

1. Kako ugotovim, ali sem zavezanec po ZInfV-1?

Pri preverjanju, ali je subjekt zavezanec po novem zakonu o informacijski varnosti (ZInfV-1), je treba v obzir vzeti najmanj 3., 6. in 7. člen ZInfV-1.

3. člen ZInfV-1 opredeljuje, da se za bistvene in pomembne subjekte v sektorjih bančništva in infrastrukture finančnega trga iz Priloge 1 ZInfV-1, IV. in IX. poglavje omenjenega zakona ne uporabljata.

ZInfV-1 se ne uporablja za subjekte, ki jih Republika Slovenija izvzame s področja uporabe Uredbe (EU) 2022/2554 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o digitalni operativni odpornosti za finančni sektor in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011 (UL L št. 333 z dne 27. 12. 2022, str. 1), zadnjič spremenjene z Delegirano uredbo Komisije (EU) 2024/1774 z dne 13. marca 2024 o dopolnitvi Uredbe (EU) 2022/2554 Evropskega parlamenta in Sveta v zvezi z regulativnimi tehničnimi standardi, ki določajo orodja, metode, postopke in politike za obvladovanje tveganj na področju informacijsko-komunikacijske tehnologije (IKT) ter poenostavljen okvir za obvladovanje tveganj na področju IKT (UL L št. 2024/1774 z dne 25. 6. 2024), (v nadaljnjem besedilu: Uredba 2022/2554/EU) v skladu s četrtim odstavkom 2. člena navedene uredbe.

ZInfV-1 se ne uporablja za tiste informacijsko-komunikacijske sisteme, v katerih se varujejo tajni podatki, za katere je nacionalni varnostni organ iz zakona, ki ureja tajne podatke, opravil varnostno vrednotenje in izdal varnostno dovoljenje za delovanje sistema v skladu z navedenim zakonom. Za te sisteme se uporabljajo predpisi s področja varovanja tajnih podatkov in pravila varovanja tajnih podatkov mednarodnih zvez ali organizacij, katerih članica je Republika Slovenije, ali mednarodni sporazumi s področja tajnih podatkov, ki jih je sklenila Republika Slovenija. Ne glede na omenjeno pa nacionalni varnostni organ iz zakona, ki ureja področje tajnih podatkov, priglaša incidente v informacijsko-komunikacijskih sistemih pristojnemu nacionalnemu organu po tem zakonu.

Za avtonomni informacijski in telekomunikacijski sistem iz zakona, ki ureja področje obrambe, ki ni zajet v tretjem odstavku 3. člena, se smiselno uporabljajo ukrepi za obvladovanje tveganj in priglasitve incidentov iz IV. poglavja ZInfV-1.

Banka Slovenije ni zavezanec po ZInfV-1.

Če subjekt ni izločen kot zavezanec po ZInfV-1, potem se pregleda 6 člen, ki pravi, da so zavezanci subjekti, ki spadajo med vrste subjektov iz Prilog 1 ali Priloge 2 (torej opravljajo storitve, ki so navedene v prilogah; sektor, podsektor, vrsta subjekta) in če imajo vsaj 50 zaposlenih in letni promet ali letno bilančno vsoto vsaj 10 milijonov eurov.

Zavezanci so tudi subjekti iz Priloge 1 in 2 ne glede na število zaposlenih ali letni promet ali letno bilančno vsoto, če:

1. storitev opravljajo:
   - ponudniki javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev,
   - ponudniki storitev zaupanja,
   - registri vrhnjih domenskih imen in ponudniki storitev sistema domenskih imen;

2. je subjekt edini ponudnik storitve ali dejavnosti v Republiki Sloveniji, katere izvajanje ga uvršča med vrste subjektov iz Priloge 1 ali 2;
3. bi motnja pri opravljanju storitve subjekta lahko pomembno vplivala na javni red, javno varnost ali javno zdravje;
4. bi motnja pri opravljanju storitve subjekta lahko povzročila sistemsko tveganje, zlasti za sektorje iz Priloge 1 ali 2, v katerih bi lahko taka motnja imela čezmejni vpliv;
5. ima subjekt poseben pomen na državni ali lokalni ravni za posamezni sektor iz Priloge 1 ali 2 ali za izvajanje posamezne storitve, ki ga uvršča med vrste subjektov iz Priloge 1 ali 2 ali zaradi medsebojne odvisnosti z drugimi sektorji iz Prilog 1 ali 2 v Republiki Sloveniji;
6. gre za subjekt javne uprave na državni ravni.

Zavezanci so tudi, ne glede na velikost in letno bilančno vsoto ali letni promet:

1. subjekti, ki so določeni kot kritični na podlagi zakona, ki ureja področje kritične infrastrukture;
2. subjekti, ki opravljajo storitve registracije domenskih imen, ne glede na njihovo velikost;
3. subjekti, ki so v državnih načrtih zaščite in reševanja opredeljeni kot službe državnega pomena, če bi nedelovanje njihovih omrežnih in informacijskih sistemov ogrozilo izvajanje nalog zaščite in reševanja iz prej navedenih načrtov, in
4. mestne občine kot subjekti javne uprave na lokalni ravni.

V nadaljevanju pa je treba za opredelitev, ali je zavezanec bistven ali pomemben, pogledati 7. člen ZInfV-1. Ob tem obstaja izjema za subjekte, ki opravljajo storitve registracije domenskih imen. Le-ti se ne razvrstijo med bistvene ali pomembne subjekte.

Bistveni subjekti so:

1. vrste subjektov iz Priloge 1, ki imajo vsaj 250 zaposlenih ali letni promet vsaj 50 milijonov eurov ali letno bilančno vsoto vsaj 43 milijonov eurov,
2. ponudniki kvalificiranih storitev zaupanja in registri vrhnjih domenskih imen ter ponudniki storitev DNS, ne glede na njihovo velikost,
3. ponudniki javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev, ki imajo vsaj 50 zaposlenih in letni promet ali letno bilančno vsoto vsaj 10 milijonov eurov,
4. subjekti javne uprave na državni ravni,
5. vse druge vrste subjektov iz Priloge 1 ZInfV-1, ki jih na podlagi 2. do 5. točke drugega odstavka 6. člena zakona in na predlog pristojnega nacionalnega organa določi vlada z odločbo;
6. subjekti, ki so določeni kot kritični na podlagi zakona, ki ureja področje kritične infrastrukture;
7. subjekti iz sektorja 9. Upravljanje storitev IKT iz Priloge 1 in niso subjekti iz 1. do 6. točke drugega odstavka 7. člena, ki jih na predlog pristojnega nacionalnega organa določi vlada.

Pomembni subjekti so:

– vrste subjektov iz Priloge 2 ZInfV-1, vključno s tistimi, ki jih na podlagi 2. do 5. točke drugega odstavka 6. člena in na predlog pristojnega nacionalnega organa določi vlada z odločbo,
– subjekti iz 3. točke tretjega odstavka 6 člena, ki jih na predlog pristojnega nacionalnega organa določi vlada z odločbo. Pristojni nacionalni organ pripravi predlog na podlagi pobude Uprave Republike Slovenije za zaščito in reševanje, ki vsebuje poimenski seznam zadevnih subjektov, in
– drugi subjekti ali organi iz 6. člena zakona, ki niso bistveni subjekti na podlagi drugega odstavka 7. člena.

2. Ali bo URSIV obveščal podjetja, da sodijo med bistvene in pomembne subjekte na podlagi ZInfV-1 in da so zavezanci na podlagi ZInfV-1. Ali mora podjetje izvesti samoregistracijo in do kdaj?

ZInfV-1 ne določa pravne podlage, da URSIV obvešča subjekte o njihovih obveznostih. Na podlagi prvega odstavka 8. člena ZInfV-1 v roku iz prehodne določbe prvega odstavka 60. člena ZInfV-1 URSIV vzpostavil mehanizem za samoregistracijo zavezancev in sicer v štirih mesecih od uveljavitve zakona.

Postopek samoregistracije bodo morali izvesti vsi zavezanci, razen tisti, ki jih zakon izrecno izključuje. Zavezanci se bodo morali prek mehanizma za samoregistracijo registrirati v tridesetih dneh od dneva, ko so nastopile okoliščine, na podlagi katerih izpolnjujejo merila iz 6. člena ZInfV-1. Ne glede na to tridesetdnevni rok za samoregistracijo za tiste zavezance, ki jim je bila vročena odločba iz 5. točke drugega odstavka ali iz prve ali druge alineje tretjega odstavka prejšnjega člena, teče od dneva vročitve odločbe.

Po prehodni določbi drugega ostavka 60. člena ZInfV-1 pa tisti zavezanci, ki ob uveljavitvi tega zakona (že) izpolnjujejo merila iz 6. in 7. člena tega zakona, opravijo prvo registracijo po mehanizmu za samoregistracijo v šestih mesecih od uveljavitve tega zakona. Do vzpostavitve mehanizma za samoregistracijo se informacije pošljejo v digitalni obliki na elektronski naslov pristojnega nacionalnega organa.

3 Ali že obstaja mehanizem za samoregistracijo, ki naj bi ga najkasneje v roku dveh mesecev od uveljavitve ZInfV-1 vzpostavil pristojni nacionalni organ (PNO)?

Na podlagi 60. člena ZInfV-1 mora PNO vzpostaviti mehanizem za samoregistracijo zavezancev iz 6. člena tega zakona po prvem odstavku 8. člena tega zakona v štirih mesecih od uveljavitve tega zakona. Skladno z navedeno obveznostjo v PNO že potekajo aktivnosti za vzpostavitev mehanizma za samoregistracijo.

4. Ali že obstaja ustrezna, varna in odporna komunikacijska in informacijska infrastruktura, preko katere se lahko izmenjujejo informacije med bistvenimi in pomembnimi subjekti ter skupinami za odzivanje na incidente na področju računalniške varnosti (skupine CSIRT)?

Kot izhaja iz 13. člena ZInfV-1 skupine CSIRT izmenjujejo informacije z bistvenimi in pomembnimi subjekti ter drugimi ustreznimi deležniki z uporabo ustrezne, varne in odporne komunikacijske in informacijske infrastrukture, ki jo vzpostavi pristojni nacionalni organ, poleg tega sodelujejo s pristojnim nacionalnim organom pri uvajanju in uporabi orodij za varno izmenjavo informacij. Aktivnosti na PNO glede vzpostavitve informacijske infrastrukture potekajo.

5. Kakšni komunikacijski kanali obstajajo za kontakt s CSIRT v Sloveniji in kako se te kanale uporablja?

Glede na 13. člen ZInfV-1 aktivnosti na PNO glede vzpostavitve informacijske infrastrukture potekajo. Do vzpostavitve komunikacija poteka prek elektronske pošte.

6. Ali že obstaja nacionalna podatkovna zbirka ranljivosti informacijskih sistemov, ki bi jo moral vzpostaviti CSIRT Nacionalnega odzivnega centra za kibernetsko varnost (SI-CERT) in če da, kako se do te zbirke dostopa?

Za koordinirano razkrivanje ranljivosti skrbi SI-CERT (Koordinirano razkrivanje ranljivosti - SI CERT). Skladno s prvim odstavkom 13. člena ZINFV-1 bo Vlada RS določila skupino CSIRT, ki bo skladno z novim zakonom opravljala to nalogo.

Kot določa 59. člen ZInfV-1, ki določa skupino CSIRT za koordinirano razkrivanje ranljivosti, pa je potrebno upoštevati, da bo do določitve skupin CSIRT iz 13. člena ZInfV-1 njihove naloge izvajala:

- SIGOV-CERT, ki deluje kot notranja organizacijska enota pri pristojnem nacionalnem organu in je pristojen za obravnavo incidentov subjektov javne uprave na državni in lokalni ravni ter ponudnikov storitev zaupanja, ki jih izvajajo subjekti državne uprave, ter
- SI-CERT, ki deluje kot notranja organizacijska enota pri javnem infrastrukturnem zavodu Akademska in raziskovalna mreža Slovenije in je pristojen za obravnavo incidentov, ki jih priglasijo drugi zavezanci iz prvega odstavka 6. člena ZInfV-1, ki niso zajeti v prejšnji alineji, ter deluje kot koordinator iz prvega odstavka 17. člena ZInfV-1. Pristojen je tudi za obravnavo prostovoljno priglašenih incidentov subjektov, ki niso zavezanci po ZInfV-1 v skladu z drugim odstavkom 35. člena ZInfV-1.

7. Komu se v Sloveniji poroča o incidentih? Je to PNO ali CSIRT, mogoče kdo drug?

Kot izhaja iz 29. člena ZInfV-1, bistveni in pomembni subjekti pristojni skupini CSIRT nemudoma v skladu s prvim in drugim odstavkom 30. člena ZInfV-1 in nacionalnim načrtom odzivanja iz drugega odstavka 12. člena ZInfV-1 priglasijo vse incidente, ki imajo pomemben vpliv na zagotavljanje njihovih storitev. Pri tem se incident šteje za pomembnega (v nadaljnjem besedilu: pomemben incident), če:

- je zadevnemu subjektu povzročil ali bi mu lahko povzročil resne operativne motnje pri opravljanju storitev ali finančne izgube ali
- je vplival ali bi lahko vplival na druge fizične ali pravne osebe s povzročitvijo precejšnje premoženjske ali nepremoženjske škode.

8. V primeru suma, da je incident hudo kaznivo dejanje, je treba obvestiti organe kazenskega pregona. Je to pri nas policija?

Da, organ kazenskega pregona je Policija, ki ima za te potrebe že vzpostavljene poti prijave suma na kaznivo dejanje.

Kot določa 10. člen ZInfV-1 pa PNO sodeluje z organi in organizacijami, ki delujejo na področju informacijske varnosti, med drugim tudi z organi kazenskega pregona. PNO v okviru svojih rednih nalog zavezance redno ozavešča o pomembnosti prijave suma na kaznivo dejanje oziroma incidenta z vsemi znaki kaznivega dejanja, ki se preganja po uradni dolžnosti, organom kazenskega pregona, v skladu s Kazenskim zakonikom. 30. člen nadalje določa, da pristojna skupina CSIRT v okviru postopka priglasitve pomembnih incidentov poleg drugih usmeritev, zavezancem zagotavlja tudi usmeritve o poročanju organom kazenskega pregona, kadar obstajajo razlogi za sum, da ima incident znake kaznivega dejanja.

9. Tako v evropski direktivi NIS 2 kot tudi v ZinfV-1 je večkrat zapisano, da je treba izvajati tudi nadzor nad dobavitelji (ukrepi za varnost dobavne verige). Ali to pomeni samo nadzor nad dobavitelji in ponudniki storitev s področja kibernetske varnosti, ponudniki katerega koli IKT proizvoda ali storitve, ali se gre na splošno za vse dobavitelje, s katerimi podjetje sodeluje?

Kot izhaja iz 22. člena ZinfV-1, je eden izmed ukrepov za obvladovanje tveganj tudi, da morajo bistveni in pomembni subjekti zagotavljati varnost dobavne verige z določitvijo ustreznih minimalnih zahtev, povezanih z informacijsko in kibernetsko varnostjo, za ključne dobavitelje ali ponudnike storitev, pri čemer se zahteve nanašajo na odnose med posameznim subjektom in njegovimi neposrednimi dobavitelji ali ponudniki storitev. Bistveni in pomembni subjekti morajo pri presoji in izvedbi ustreznih varnostnih ukrepov za varnost dobavne verige upoštevati ranljivosti, ki so specifične za posameznega neposrednega dobavitelja in ponudnika storitev, ter splošno kakovost proizvodov in praks svojih dobaviteljev in ponudnikov storitev na področju kibernetske varnosti, vključno z njihovimi varnimi razvojnimi postopki. Ugotavljati morajo, kateri varnostni ukrepi so ustrezni in primerni za zagotovitev varnosti dobavne verige, poleg tega lahko preverjajo njihovo izvajanje pri dobaviteljih in ponudnikih storitev. Pri tem upoštevajo rezultate morebitnih usklajenih ocen tveganja za kritične dobavne verige, ki jih Skupina za sodelovanje pripravi v sodelovanju z Evropsko komisijo in Evropsko agencijo za kibernetsko varnost (ENISA) v skladu s prvim odstavkom 22. člena Direktive NIS 2.

10. Obstajala naj bi tudi usklajena ocena tveganja, ki naj bi jo pripravila Skupina za sodelovanje v sodelovanju z Evropsko komisijo in ENISA. Ali je že na voljo?

Po našem vedenju usklajene ocene tveganja, kot ga predvideva 22. člen NIS 2, skupina za sodelovanje še ni opravila.

11. Kako naj bi ta nadzor izgledal v praksi? Ali se lahko ponudnika, ki je zavezanec za NIS 2 šteje kot zaupanja vrednega in nadaljnji nadzor ni potreben?

Ker je NIS 2 evropska direktiva, ki ne velja neposredno v slovenskem pravnem redu, ampak bo prenesena z ZInfV-1, bodo subjekti zavezanci po ZInfV-1 in ne po NIS 2. Status zavezanca po ZInfV-1 pomeni, da je tak subjekt dolžan izpolnjevati zakonske zahteve, ne pa to, da že sam status zavezanca ZInfV-1 pomeni, da je zaupanja vreden. Vsak zavezanec po ZInfV-1, torej vsak bistveni ali pomembni subjekt bo lahko podvržen inšpekcijskemu nadzoru. Tudi če gre za subjekte, ki so del dobavne verige zavezanca (npr. proizvajalci, dobavitelji, ponudniki storitev), pa so ti subjekti že zaradi narave svojega proizvoda ali storitve tudi sami zavezanci po ZInfV-1, to ne pomeni nujno, da so zaupanja vredni in da zavezancem, ki s takšnimi proizvajalci, dobavitelji ali ponudniki storitev sklepajo pogodbe, ni potrebno ocenjevati tveganj dobavne verige ali opredeljevati varnostnih zahtev za ključne dobavitelje (in jih v okviru sklenjenih pogodb tudi nadzirati).

Inšpekcija bo nadzor nad zavezanci po ZInfV-1 opravljala na podlagi Strateških usmeritev in prioritet inšpekcije, kjer so določeni pogoji za izvajanje rednih in izrednih inšpekcijskih nadzorov. Nadzor tipično obsega pregled varnostne dokumentacije zavezanca, pri čemer bo inšpektor preveril zlasti, ali bo dokumentacija zavezanca skladna z zahtevami ZInfV-1. Inšpektor bo v nadaljevanju preveril kako se predpisani varnostni ukrepi dejansko izvajajo, lahko pa bo izvedel tudi inšpekcijski varnostni pregled omrežja, s katerim bo za različnimi orodji izvedel identifikacijo in oceno morebitnih ranljivosti v omrežnih in informacijskih

sistemih ter preizkusil učinkovitost varnostnih ukrepov in mehanizmov ter izpostavljenosti kibernetskim grožnjam. Nadzor se bo izvajal tudi fizično pri zavezancu, kjer bo inšpektor preveril ustreznost prostorov, v katerih se bodo nahajali ključni, krmilni ali nadzorni IS zavezanca (npr. fizično in tehnično varovanje). Prioritetno se bo nadzor izvajal nad bistvenimi subjekti, kar pa ne pomeni, da bodo pomembni izvzeti iz inšpekcijskega nadzora.

12. Na podlagi direktive in novega zakona je treba uporabljati IKT proizvode in storitve, ki so certificirani, za kar naj bi obstajale evropske certifikacijske sheme. Kje dostopati do teh certifikacijskih shem in kako vedeti, ali je IKT produkt, ki ga podjetje uporablja, certificiran?

Evropske certifikacijske sheme za kibernetsko varnost so dostopne na spletne strani ENISA: https://certification.enisa.europa.eu/index_en.

ENISA bo v sodelovanju z nacionalnimi organi (v Sloveniji bo URSIV, določen z ZinfV-1) vzpostavila register certificiranih IKT proizvodov, storitev in procesov. Trenutno uradni register še ni (v celoti) vzpostavljen, saj večina shem še ni potrjenih. Ko bo posamezna shema potrjena, bodo organi za ocenjevanje skladnosti (CAB - Conformity Assessment Bodies) izvajali presoje, rezultati pa bodo tudi javno objavljeni.

Na tej točki lahko podjetje oz. zavezanec na spletni strani ENISA spremlja sheme in novice v povezavi z njimi, spremlja NCC-SI, kjer bodo prav tako novice v zvezi s potrjenimi certifikacijskimi shemami. Lahko povpraša dobavitelje, če je njihov produkt certificiran po enem od evropskih ali mednarodnih standardov (npr. ISO/IEC 27001, Common Criteria, itd.).

Kot že omenjeno, pa se bo v prihodnje lahko preverjalo certifikate neposredno v evropskem registru ali pri nacionalnem pristojnem organu.

Več informacij o postopku potrjevanja EUCC shem najdete tukaj: https://certification.enisa.europa.eu/about-eu-cyber-certification/developing-certification-schemes_en.

Veljavni certifikati EUCC certifikacijske sheme: https://certification.enisa.europa.eu/certificates_en.

Seznam nacionalnih organov, pristojnih za certificiranje na področju kibernetske varnosti: https://certification.enisa.europa.eu/take-action/national-cybersecurity-certification-authorities_en.

Seznam organov za ocenjevanje skladnosti, ki se sprotno posodablja: https://webgate.ec.europa.eu/single-market-compliance-space/notified-bodies/notified-body-list?filter=legislationId:164702,notificationStatusId:1.

13. Prav tako je zapisano, da se lahko zaupa IKT proizvodom in storitvam podjetij, ki so zavezanci za ZinfV-1 in v EU, evropski direktivi NIS 2. Kako lahko vemo, ali je neko podjetje zavezanec za eno ali drugo?

ZInfV-1 v 6. členu določa merila, na podlagi katerih se posamezni subjekti uvrščajo v posamezne kategorije zavezancev po tem zakonu. Posamezni subjekti se lahko uvrstijo med zavezance na podlagi izpolnjevanja več različnih meril iz ZInfV-1, pri čemer je subjekt v

celoti zavezan tudi, če izpolnjuje samo eno merilo iz ZInfV-1. Prvi odstavek 6. člena ZInfV-1 določa, da so zavezanci po tem zakonu med drugim subjekti, ki spadajo med vrste subjektov iz Priloge 1 ali Priloge 2, ki sta sestavni del zakona, če imajo vsaj 50 zaposlenih in letni promet ali letno bilančno vsoto vsaj 10 milijonov eurov.

Z ZInfV-1 se prenaša Direktiva NIS2 v slovenski pravni red in določa obveznosti za podjetja, ki izvajajo kritične oziroma pomembne dejavnosti na področju kibernetske varnosti v Sloveniji. Zavezanost po zakonu je odvisna od narave dejavnosti podjetja in njegovega vpliva na nacionalno varnost in gospodarstvo. Med podjetji, ki bodo zavezana po ZinfV-1 so operaterji kritične infrastrukture (npr. energetika, transport, zdravstvo) in podjetja, ki opravljajo pomembne storitve za gospodarstvo (npr. IT storitve, telekomunikacije, finančne storitve).

Na podlagi 8, člena ZInfV-1 bo PNO vzpostavil seznam bistvenih in pomembnih subjektov ter subjektov, ki opravljajo storitve registracije domenskih imen. Ta seznam bo varovani podatek pristojnega nacionalnega organa, kar pomeni, da ne bo javno objavljen. Kot pojasnjeno, bodo morali zavezanci sami izvajati ocene tveganj tudi v svojih dobavnih verigah ali opredeljevati varnostne zahteve za svoje ključne dobavitelje in jih okviru sklenjenih pogodb tudi nadzirati.

14. Kako dokazovati skladnost (certificiranost) IKT produkta (sploh SW), katerega ponudnik ni iz EU?

Čeprav ponudnik ni iz EU, je možno, da izdelek ustreza mednarodno priznanim certifikacijskim shemam, ki jih priznavajo evropske regulacije. Podajamo nekaj primerov shem, ki zagotavljajo skladnost in na podlagi katerih je možno dokazati skladnost:

- ISO/IEC 27001 (Sistemi upravljanja informacijske varnosti): šteje kot potrdilo o skladnosti s splošnimi zahtevami glede varnosti podatkov in IKT sistemov,
- ISO/IEC 15408 (Common Criteria – EUCC): mednarodni standard za certificiranje varnosti IKT produkta, ki ga priznavajo številne države, tudi v EU. To je eden izmed najpogosteje uporabljanih certifikatov za programsko opremo in strojno opremo,
- SOC 2 (Service Organization Control 2): specifičen za IT podjetja in storitve, ki obdelujejo osebne podatke. Certifikacija po tem standardu se uporablja kot dokaz o varnosti in zaščiti zasebnosti podatkov, kar je tudi v skladu z GDPR,
- CSA STAR (Cloud Security Alliance Security, Trust & Assurance Registry): certifikat, ki potrjuje, da so izpolnjeni določeni standardi varnosti in zasebnosti za oblačne storitve.

15. ENISA naj bi naredila bazo ranljivih IKT produktov in storitev, kjer bi se dalo preverjati, če so ranljivi tudi produkti, ki jih uporablja naše podjetje. Ali ta baza že obstaja?

Da, ENISA je vzpostavila bazo ranljivih IKT produktov in storitev (EUVD – European Union Vulnerability Database). EUVD je javno dostopna baza podatkov, ki vsebuje informacije o znanih ranljivostih v IKT produktih in storitvah. Namenjena je tako organizacijam kot posameznikom, da preverijo, ali so izdelki, ki jih uporabljajo, ranljivi in da prejmejo smernice za odpravo teh ranljivosti.

EUVD: https://euvd.enisa.europa.eu/.

V iskalno polje vnesite ime IKT produkta ali storitve, ki ga uporablja vaše podjetje. Če so v bazi podatkov prisotne ranljivosti za iskani izdelek, boste našli podrobnosti, vključno z opisom ranljivosti, prizadetimi različicami in priporočili za odpravo.

Pri tem opozarjamo, da čeprav je EUVD izjemno uporabno in koristno orodje za preverjanje ranljivosti, ni nujno, da vsebuje vse obstoječe ranljivosti. Nekateri manj znani ali specifični izdelki morda niso zajeti. Zato je priporočljivo kombinirati iskanje v EUVD z drugimi viri, kot so: CVE (mednarodni seznam ranljivosti, ki ga vzdržuje MITRE), CNA (organizacije, ki so pooblaščene za dodeljevanje identifikatorjev CVE) ter nacionalni C-SIRT (specifične informacije za regijo).

16. Ali v Sloveniji že obstaja mehanizem za izmenjavo informacij o kibernetski varnosti in na kakšen način se obvesti pristojne organe, da subjekt v izmenjavi sodeluje?

10. odstavek 30. člena ZInfV-1 določa, da se bodo priglasitve pomembnih incidentov in medsebojno sodelovanje pristojnih organov izvajali po namenski digitalni platformi, ki jo vzpostavi pristojni nacionalni organ in po kateri poteka tudi izmenjava informacij med sodelujočimi organi na podlagi drugega odstavka 18. člena ZInfV-1. Sodelujoči organi imajo dostop do informacij o priglasitvah subjektov, ki so povezane z njihovim področjem dela.

Že sedaj, pa ima PNO vzpostavljen reden dialog s ključnimi deležniki, kjer je omogočena tudi izmenjava aktualnih informacij in dogajanj na področju informacijske in kibernetske varnosti. PNO prav tako na vsakih 6-mesecev objavi poročilo o stanju na področju informacijske in kibernetske varnosti, kjer je povzeto dogajanje v slovenskem prostoru.

Subjekti oziroma zavezanci že skladno s trenutno zakonodajo prejemajo, in bodo tudi v bodoče prejemali obvestila o zadevah s področja zagotavljanja kibernetske varnosti skupin CSIRT.

17. V členu 19 je zapisano, da je PNO pristojen za usposabljanje odgovornih oseb vseh subjektov. Ali program usposabljanja že obstaja in kako se ga udeleževati?

1. odstavek 20. člena določa, da so za izvajanje ukrepov iz 21. in 22. člena tega zakona 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. 6. odstavek 20. člena ZInfV-1 določa, da program in način izvajanja usposabljanja odgovornih oseb na področju informacijske in kibernetske varnosti določi vlada na predlog pristojnega nacionalnega organa. 64. člen ZInfV-1 določa, da bo vlada izdala podzakonski predpis, s katerim bo podrobneje določila izvajanje usposabljanj v šestih mesecih od uveljavitve ZInfV-1. V okviru PNO se trenutno predvideva, da bodo usposabljanja izvajali uslužbenci PNO za informacijsko varnost, ki imajo ustrezne strokovne kompetence. Trenutno je predvideno, da bodo usposabljanja potekala na podlagi posebnega programa, po zaključku usposabljanj pa bodo (predvidoma) udeleženci opravljali preizkus znanja in pridobili potrdilo o usposobljenosti s strani izvajalca usposabljanj.

18. Ali že obstaja platforma za priglasitev incidentov, ki bi jo morale vzpostaviti skupine CSIRT in če da, kako do nje dostopati?

Tako kot postopki samoregistracije, se bodo tudi postopki priglasitve pomembnih kibernetskih incidentov izvajali po namenski digitalni platformi, ki jo bo vzpostavil PNO, kot določa 10. odstavek 30. člena ZInfV-1. Aktivnosti na PNO glede te naloge že potekajo.

19. Na podlagi 46. člena novega zakona je razvidno, da morajo pomembni subjekti izvajati samooceno skladnosti najmanj enkrat na dve leti. Ni pa popolnoma jasno, ali mora pomemben subjekt po izvedbi samoocene komu predložiti to samooceno (npr. PNO-ju) ali pa je predložitev potrebna le v primeru inšpekcijskega postopka?

Kot določa 25. člen ZInfV-1, pomembni subjekti izvedejo samooceno skladnosti najmanj enkrat na dve leti ali v primeru pojava pomembnega incidenta.

Če je iz rezultatov opravljene samoocene skladnosti razvidno, da pomembni subjekt izpolnjuje zahteve, predpisane s tem zakonom, ta sestavi izjavo o skladnosti, pri čemer ta vsebuje potrebne elemente samoocenjevanja skladnosti, ki omogočajo izvedbo ponovljivosti opravljene ocene.

Če je iz rezultatov opravljene samoocene skladnosti razvidno, da pomembni subjekt ne izpolnjuje predpisanih zahtev, ta sestavi izjavo o ugotavljanju neskladnosti, v kateri navede ugotovljene neskladnosti in način njihove odprave z roki za izvedbo.

Pomembni subjekti torej morajo izvesti samooceno skladnosti na način in v rokih, predpisanih v tretjem, četrtem in petem odstavku 25. člena zakona. Odsotnost ali pomanjkljivost takšne ocene pomeni kršitev, za katero bo predpisana globa, inšpektor pa bo v primeru, da sploh ne bo izvedena, kot inšpekcijski ukrep lahko izrekel tudi izvedbo revizije skladnosti. Samoocene ni potrebno predložiti PNO, temveč je to del dokumentacije zavezanca.

20. Kdo je v Sloveniji pristojen za izvedbo inšpekcije če je subjekt skladen z ZinfV-1?

Inšpekcija za informacijsko varnost, ki je samostojna notranja organizacijska enota URSIV, je pristojna za izvajanje inšpekcijskega nadzora nad zavezanci iz ZinfV-1.

21. Na podlagi 58. člena ZinfV-1, so v roku šestih mesecev od uveljavitve zakona vsi subjekti, ki so bili pred 16. januarjem 2023 določeni kot izvajalci bistvenih storitev, dolžni sprejeti ukrepe na podlagi tega zakona. Ali obstaja seznam, v katerem se da preveriti, katera podjetja so bila pred 16. januarjem 2023 določena za izvajalca bistvenih storitev?

URSIV ima seznam izvajalcev bistvenih storitev. Seznam ni javno objavljen.

22. Ali je podjetje, ki sodelujejo z ministrstvom, obvezna izvedba GAP analize skladnosti z Direktivo NIS 2.

Izvedba GAP analize na podlagi Direktive NIS 2 ni obvezna, niti ni obvezna po novem ZInfV-1. Ta določa le, da bodo morali zavezanci, ki so že zdaj določeni kot zavezanci na podlagi obstoječega ZInfV, izpolnjevati kriterije glede zahtev, ukrepov in varnostne dokumentacije iz novega ZInfV-1 v enem letu od uveljavitve novega zakona. Kako bodo podjetja ugotavljala razliko v skladnosti med ZInfV in ZInfV-1 (z GAP analizo ali kako drugače), ni posebej predpisano in je prepuščeno presoji zavezancev samih.