REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE ZA INFORMACIJSKO VARNOST

URSIV

DELAVNICA: Priprava podjetij na NIS 2 direktivo

Predstavitev osnutka Zakona o informacijski varnosti (ZInfV-1)

Kory Golob, pomočnik direktorja urada

Ljubljana, 22. maj 2024

Pregled vsebine

- Izkušnje z NIS
- Nacionalne posebnosti v ZInfV
- Prehod v NIS 2
- Prilogi NIS 2
- Javna obravnava
- ZInfV-1 novosti in nacionalne določbe
- Člani ZInfV

Izkušnje z NIS

DIREKTIVA NIS

Direktiva (EU) 2016/1148 za visoko skupno raven varnosti

omrežij in informacijskih sistemov v Uniji

- **pomagala doseči višjo + enakomernejšo raven varnosti omrežij in informacijskih sistemov na njenem področju uporabe**
- **vendar je veliko urejanja prepuščala državam članicam (DČ)**, zato so **razlike pri njenem prenosu velike** (vpliv na notranji trg);
- **- se ne uporablja za operaterje elektronskih komunikacij in za ponudnike storitev zaupanja = za oboje posebne EU zahteve**

Medtem: potekala digitalizacija brez primere in

spremembe v okolju kibernetskih groženj

Zato: potreba po prenovi ureditve

Nacionalne posebnosti ZInfV

- ✓ **Širši nabor zavezancev**
  - ➢ **organi državne uprave (tudi s področja nacionalne varnosti)**
  - ➢ **izvajalci bistvenih storitev po zakonu, ki ureja kritično infrastrukturo**
  - ➢ **nacionalna sektorja (varstvo okolje in preskrba s hrano)**
  - ➢ **povezani subjekti (ZInfV-B)**
- ✓ **URSIV**
  - ➢ **(PNO + Enotna kontaktna točka + Inšpekcija za informacijsko varnost + SIGOV-CERT)**
- ✓ **Dve skupini CSIRT**
- ✓ **Varnostno operativni centri organov državne uprave**

Nacionalne posebnosti ZInfV

- ✓ **Nacionalni načrt odzivanja na kibernetske incidente**
- ✓ **Kibernetska obramba**
- ✓ **Koordinacija kibernetske varnosti**
- ✓ **Krizno odzivanje**
- ✓ **Ocena ogroženosti**
- ✓ **Dnevniški zapisi**

Prehod v NIS 2

Je vseevropska horizontalna zakonodaja o kibernetski varnosti

(nanaša se na različne sektorje gospodarstva in družbe)

Stopila je v veljavo 16. 1. 2023

(dvajseti dan po objavi v Uradnem listu EU, L333/142 z dne 27. 12. 2022).

Rok za njen prenos v nacionalno zakonodajo ter za notifikacijo te zakonodaje Evropski komisiji (EK) je **17. 10. 2024.**

Prehod v NIS 2

Posodoblja pravila EU o kibernetski varnosti

Zagotavlja povečanje splošne ravni kibernetske varnosti v EU.

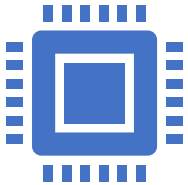
Direktiva minimalne harmonizacije - DČ lahko sprejmejo ali ohranijo določbe, ki zagotavljajo višjo raven kibernetske varnosti (skladno z obveznostmi DČ v pravu EU)

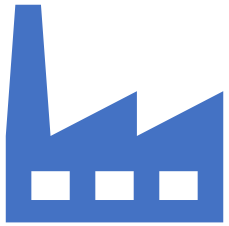
NIS 2 SE NE UPORABLJA (razen za ponudnika storitev zaupanja) za subjekte javne uprave, ki izvajajo dejavnosti na področju nacionalne in javne varnosti, obrambe ali kazenskega pregona

Direktiva NIS 2 – subjekti iz vrst Priloge I in II

BISTVENI IN POMEMBNI SUBJEKTI

Razlika z Direktivo NIS, ki je zavezance delila na: Izvajalce bistvenih storitev (**IBS**) in Ponudnike digitalnih storitev (**PDS**)





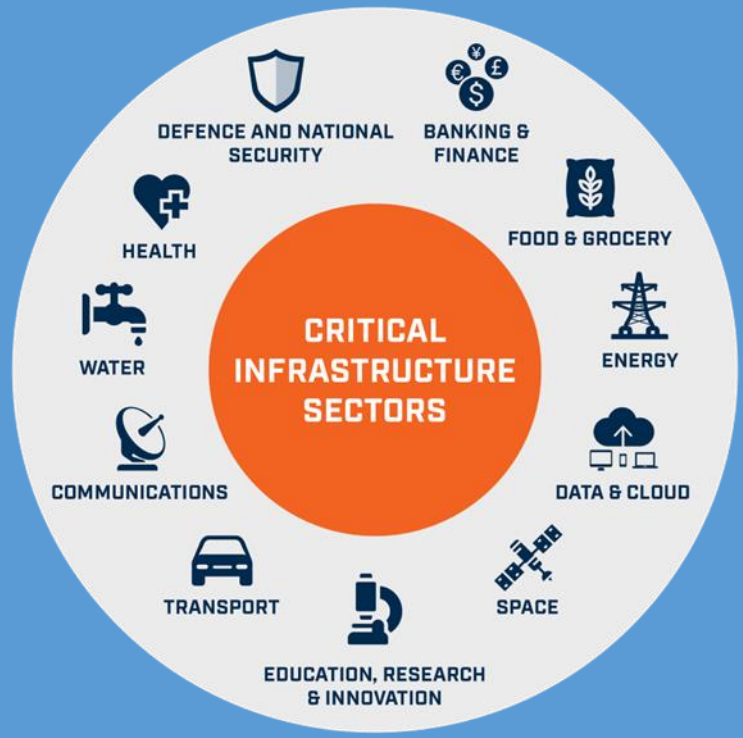
Prehod v NIS 2

- Direktiva NIS 2 **odpravlja dosedanje razlikovanje med zavezanci** po direktivi NIS (med dosedanjimi IBS in PDS) z ***uvedbo splošnega merila velikosti zavezanih subjektov.***
- **BISTVENI SUBJEKTI:** subjekti, ki izvajajo vrste dejavnosti iz Priloge I, ki **presegajo zgornje meje za srednja podjetja** iz Priporočila EU), pri čemer so določene oz. dovoljene izjeme **in so bistveni subjekti** še:
  - operaterji elektronskih komunikacij, ki so srednja podjetja,
  - ponudniki kvalificiranih storitev zaupanja, registri vrhnjih domenskih imen, ponudniki storitev DNS - ne glede na velikost;
  - subjekt, ki je edini ponudnik storitve, bistvene za državo;
  - če gre za določene subjekte javne uprave;
  - drugi subjekti iz priloge I in II, ki jih država prepozna kot bistvene in
  - če gre za subjekte prepoznane kot kritične na podlagi Direktive (EU) 2022/2557 (t.i. CER Direktiva o kritični infrastrukturi)
- **POMEMBNI SUBJEKTI: vsi** subjekti, ki izvajajo vrste dejavnosti iz Prilog I In II, **ki niso bistveni subjekti**.
- **DČ LAHKO kot BISTVENE ohranijo IBS (po NIS)** in tudi določijo subjekte javne uprave na lokalni ravni in izobraževalne ustanove.

Prilogi NIS 2

PRILOGA I VISOKO KRITIČNI SEKTORJI

1. Energija (elektrika, daljinsko ogrevanje in hlajenje, nafta, vodik)
2. Promet (zračni, železniški, vodni, cestni)
3. Bančništvo (vrsta: kreditne institucije)
4. Infrastruktura finančnega trga
5. Zdravje
6. Pitna voda
7. Odpadna voda
8. Digitalna infrastruktura
9. Upravljanje storitev IKT
10. Javna uprava (centralni nivo)
11. Vesolje



Prilogi NIS 2

PRILOGA II - DRUGI KRITIČNI SEKTORJI:

1. **Poštne in kurirske storitve**;
2. **Ravnanje z odpadki**;
3. **Izdelava, proizvodnja in distribucija kemikalij**;
4. **Pridelava, predelava in distribucija živil**;
5. **Proizvodnja** (določenih vrst: npr. medicinski pripomočki; računalniki, elektronski in optični izdelki; proizvodnja električnih naprav; proizvodnja drugih strojev in naprav; proizvodnja motornih vozil, prikolic, polprikolic; proizvodnja drugih vozil in plovil)
6. **Digitalni ponudniki** (spletne tržnice; spletni iskalniki; platforme storitev družbenega mreženja)
7. **Raziskave** (raziskovalne organizacije)

NIS2 SCOPE – ESSENTIAL AND IMPORTANT ENTITIES

New sectors compared to NIS1

Essential entities

Important entities (unless designed as essential)

Designed or not as essential based on criticality criteria

Out of the scope, unless designed important or essential (criticality criteria)

* Defence, national security, public security, law enforcement (including the prevention, investigation, detection and prosecution of criminal offences)

Article 27.1 entities (covered by the Implementing Acts)

SECTORS & ENTITIES	MICRO (< 10)	SMALL (< 50)	MED. (< 250)	LARGE (> 250)
Annex I 1 Energy				
- ***Including electricity production (incl. nuclear), district heating and cooling, smart charging operators, and the hydrogen sector***				
Annex I 2 Transport (air, rail, road and water)				
Annex I 3 Banking sector (credit institutions)				
Annex I 4 Financial Market Infrastructures				
Annex I 5 Health				
- ***Including research and development activities of medicinal products, and manufacturing of basic pharmaceutical products and of medical devices considered as critical***				
Annex I 6 Drinking water *(excl. where the activity is only a non-essential part of the overall activity)*				
Annex I 7 Waster water *(excl. where the activity is only a non-essential part of the overall activity)*				
Annex I 8 Digital Infrastructure, including:				
- ***Cloud providers and data centres***				
- DNS providers (excl. root servers)				
- TLD name registries				
- ***Non-qualified trust service providers***				
- ***Qualified trust service providers***				
- ***Providers of electronic communications***				
Annex I 8a ICT-service management (B2B)				
Annex I 9 Public administration entities (excl. exclusion clause*, parliaments, judiciary and central banks)				
- ***Including regional entities*** (in accordance with national law)				
Annex I 10 Space				
Annex II (postal and courier services; waste management; chemicals; food; manufacturing; digital providers***; research)***				
Critical entities (Resilience of Critical Entities Directive)				
Operators of Essential Services (NIS1)				

Javna obravnava

PREDLOG PREDPISA

ZAKON O INFORMACIJSKI VARNOSTI

V MEDRESORSKO USKLAJEVANJE IN NA SVZ
15.5.2024
(pred 6 dnevi)

VRSTA PREDPISA
Predlog

EVIDENCA VLADNEGA AKTA
2023-1544-0005

PREDLAGATELJ
Urad Vlade Republike Slovenije za informacijsko varnost

Komentar lahko oddate do 31. 5. 2024.

ODDAJTE KOMENTAR

https://e-uprava.gov.si/si/drzava-in-druzba/e-demokracija/predlogi-predpisov/predlog-predpisa.html?id=16290

ZInfV-1 novosti in nacionalne določbe

Namen - sistemska ureditev področja informacijske oziroma kibernetske varnosti in zagotovitev visoke ravni kibernetske varnosti v Republiki Sloveniji na področjih, ki so bistvenega pomena za nemoteno delovanje države ter ohranitev zagotavljanja ključnih družbenih in gospodarskih dejavnosti v vseh varnostnih razmerah.

Vsebuje določbe, ki prenašajo Direktivo (EU) 2022/2555 kot tudi nacionalne določbe za doseganje namena zakona.

ZInfV-1 novosti in nacionalne določbe

Struktura zakona

I. Splošne določbe
II. Zavezanci
III. Organizacija nacionalnega sistema informacijske varnosti
IV. Ukrepi za obvladovanje tveganj in priglasitve incidentov
V. Pristojnost in registracija
VI. Izmenjava informacij
VII. Vrednotenje incidenta, ocena ogroženosti in ukrepanje
VIII. Kibernetska obramba
IX. Nadzor
X. Kazenske določbe
XI. Prehodne določbe
XII. Končna določba

ZInfV-1 novosti in nacionalne določbe

- **Razširjen obseg**: razširja se področje uporabe
- **Povečane obveznosti**: strožje zahteve glede prijave incidentov ter zahtev za izvajanje varnostnih ukrepov
- **Več sodelovanja** med državami članicami EU ob resnih varnostnih incidentih ter spodbuda za izmenjavo informacij in najboljših praks
- **Izboljšana zaščita kritične infrastrukture**
- **Večja odgovornost** ponudnikov digitalnih storitev za zagotavljanje varnosti svojih sistemov ter uvedba mehanizmov za ocenjevanje skladnosti
- **Višje globe** za subjekte, ki ne izpolnjujejo predpisanih varnostnih zahtev ali ne prijavijo varnostnih incidentov.

ZInfV-1 novosti in nacionalne določbe

- Zakon bo nadomestil ZInfV in posegel v ZEKom-2
- Bistveni in pomembni subjekti opravijo samoregistracijo
- Usklajenosti s področnim zakonom, ki ureja kritično infrastrukturo
- Ohranja strategijo kibernetske varnosti
- URSIV ostaja pristojni nacionalni organ
- Bolj jasno določi enotno kontaktno točko
- Ureja nacionalni okvir za obvladovanje kibernetskih kriz (nacionalni načrt, EU-CyCLONe)

6. člen (zavezanci)

(1) Subjekti, ki spadajo v področje uporabe tega zakona po 3. členu tega zakona, so zavezanci po tem zakonu in se delijo na bistvene in pomembne subjekte.

(2) Za namene tega zakona se šteje, da so bistveni subjekti:

1.subjekti vrste iz Priloge I, ki imajo vsaj 250 zaposlenih in letni promet vsaj 50 milijonov evrov ali letno bilančno vsoto vsaj 43 milijonov evrov;
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 oziroma letno bilančno vsoto vsaj 10 milijonov evrov;
4. subjekti javne uprave na državni ravni;
5. vsi drugi subjekti vrste iz Prilog I ali II, ki jih na podlagi 2. do 5. točke drugega odstavka 3. člena tega zakona in na predlog pristojnega nacionalnega organa določi vlada;
6. subjekti, ki so določeni kot kritični na podlagi zakona, ki ureja kritično infrastrukturo;
7. subjekti, ki so bili v skladu z Zakonom o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23) določeni kot izvajalci bistvenih storitev pred 16. januarjem 2023;
8. subjekti iz sektorja 9. Upravljanje storitev IKT Priloga I in niso subjekti iz točk 1 do 7 tega odstavka, ki jih na podlagi poimenskega seznama, ki ga pristojni organi po zakonu, ki ureja izvajanje Uredbe (EU) 2022/2554, posredujejo pristojnemu nacionalnemu organu, določi vlada.

(3) Za namene tega zakona se šteje, da so pomembni subjekti:

- subjekti vrste iz Prilog I ali II vključno s tistimi, ki jih na podlagi 2. do 5. točke drugega odstavka 3. člena tega zakona in na predlog pristojnega nacionalnega organa določi vlada z odločbo in
- drugi subjekti oziroma organi iz 3. člena tega zakona,

ki se ne štejejo za bistvene subjekte na podlagi prejšnjega odstavka.

(4) Ne glede na določbo 7. točke drugega odstavka tega člena Banka Slovenije ni zavezanec po tem zakonu.

7. člen (samoregistracija in seznam zavezancev)

(1) Pristojni nacionalni organ vzpostavi mehanizem za samoregistracijo zavezancev iz prejšnjega člena tega zakona.

(2) Zavezanci iz prejšnjega člena tega zakona se morajo registrirati preko mehanizma za samoregistracijo iz prejšnjega odstavka v desetih delovnih dneh od dneva, ko so nastopile okoliščine, na podlagi katerih izpolnjujejo merila iz prejšnjega člena. Ob tem podajo vsaj naslednje informacije o:

- ***imenu in naslovu, kontaktnih podatkih, matični številki ter elektronskem naslovu zavezanca za vročanje;***
- ***dodeljenih blokih javnih naslovov IP;***
- ***kontaktni osebi za informacijsko varnost in njenem namestniku ter njune kontaktne podatke vključno z elektronskimi naslovi in telefonskimi številkami;***
- ***ustreznem sektorju in podsektorju iz Priloge I ali II, v katerem zavezanec izvaja vrste storitev iz teh prilog ali kategorijo zavezancev, ki niso vključeni v navedenih prilogah, so pa zavezanci na podlagi določb tretjega do sedmega odstavka 3. člena tega;***
- ***seznamu držav članic Evropske unije, kjer opravljajo storitve, ki spadajo na področje uporabe tega zakona ter***
- ***registriranih številkah avtonomnih sistemov in vseh domenskih imenih, ki jih zavezanec uporablja pri poslovanju.***

(3) Zavezanci iz prejšnjega člena tega zakona z uporabo mehanizma za samoregistracijo nemudoma sporočijo morebitne spremembe podatkov, ki so jih predložili na podlagi prejšnjega odstavka, v vsakem primeru pa v desetih delovnih dneh od datuma spremembe. V primeru, da subjekt, ki se je samoregistriral na podlagi prejšnjega odstavka ugotovi, da ne spada več med zavezance iz prejšnjega člena tega zakona, o tem in razlogih za takšno ugotovitev obvesti pristojni nacionalni organ, ki preveri navedbe in ob potrditvi razlogov v mehanizem za samoregistracijo vnese podatek o takšni spremembi.

19. člen (upravljanje)

(1) Odgovorne osebe pravnih oseb oziroma člani poslovodnih organov (v nadaljnjem besedilu: odgovorne osebe), ki so bistveni ali pomembni subjekti, so odgovorni za izvajanje ukrepov za obvladovanje tveganj za kibernetsko varnost v skladu z določbami tega zakona.

(2) Odgovorne osebe iz prejšnjega odstavka odobrijo ukrepe za obvladovanje tveganj za kibernetsko varnost, ki jih subjekt izvaja zaradi izpolnjevanja obveznosti, določenih s tem zakonom, in nadzirajo njihovo izvajanje.

(3) Odgovorne osebe iz prvega odstavka tega člena se morajo izobraževati oziroma usposabljati na področju obvladovanja tveganj kibernetske varnosti in njihovega vpliva na dejavnosti oziroma storitve, ki jih izvaja subjekt.

(4) Odgovorne osebe zagotavljajo redno usposabljanje zaposlenim, da pridobijo dovolj znanj in spretnosti, ki jih usposobi za prepoznavanje in ocenjevanje tveganj in za oceno praks obvladovanja tveganj za kibernetsko varnost ter njihovega vpliva na storitve, ki jih opravlja ta subjekt.

(5) Ne glede na prejšnji odstavek odgovorne osebe zagotavljajo, da imajo vsi skrbniki informacijsko komunikacijskih sistemov zavezanca obveznost rednega letnega usposabljanja, da pridobijo in ohranijo raven znanj in spretnosti, ki jih usposobi za prepoznavanje in ocenjevanje tveganj in za oceno praks obvladovanja tveganj za kibernetsko varnost ter njihovega vpliva na storitve, ki jih opravlja ta subjekt.

(6) Pristojni nacionalni organ je pristojen za usposabljanje odgovornih oseb iz prvega odstavka tega člena. Program, način in izvajalce izvajanja usposabljanja ter način usposabljanja odgovornih oseb na področju informacijske varnosti, predpiše vlada.

20. člen (varnostna dokumentacija bistvenih in pomembnih subjektov)

(1) Bistveni in pomembni subjekti za zagotavljanje visoke ravni informacijske in kibernetske varnosti in odpornosti svojih omrežnih in informacijskih sistemov vzpostavijo in vzdržujejo dokumentiran sistem upravljanja varovanja informacij ter sistem upravljanja neprekinjenega poslovanja, ki temeljita na pristopu upoštevanja vseh nevarnosti in morata obsegati najmanj:

1. natančen in posodobljen popis informacijskih in drugih sredstev ter podatkov, potrebnih za nemoteno delovanje omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev ter določitev njihovih upravljavcev;
2. analizo obvladovanja tveganj, vključno z določitvijo sprejemljive ravni tveganja in opisano uporabljeno metodologijo;
3. politiko in načrt neprekinjenega poslovanja, vključno z oceno vpliva na poslovanje, navedbo postopkov zagotavljanja neprekinjenega poslovanja, določitvijo minimalne ravni poslovanja, upravljanjem varnostnih kopij in določitvijo vlog ter odgovornosti;
4. načrt obnovitve in ponovne vzpostavitve delovanja omrežnih in informacijskih sistemov, ki jih potrebujejo za svoje delovanje ali opravljanje storitev, vključno z opisom odgovornosti in postopkov za obnovitev delovanja teh sistemov po dogodku, ki povzroči prekinitev njihovega delovanja;
5. načrt odzivanja na incidente s protokolom obveščanja pristojnega CSIRT, vključno z opisom sistema za zaznavo in odziv na incidente informacijske varnosti ter opisom vlog in odgovornosti za odzivanje na incidente;
6. načrt varnostnih ukrepov za zagotavljanje celovitosti, avtentičnosti, zaupnosti in razpoložljivosti omrežnih in informacijskih sistemov oziroma za obvladovanje tveganj za kibernetsko varnost, ki upoštevajo in področne posebnosti bistvenega ali pomembnega subjekta;
7. politiko s postopki za oceno učinkovitosti varnostnih ukrepov za obvladovanje tveganj za informacijsko in kibernetsko varnost, vključno z določitvijo kazalnikov učinkovitosti in izvedeno analizo zbranih podatkov.

20. člen (varnostna dokumentacija bistvenih in pomembnih subjektov)

(2) Bistveni in pomembni subjekti določijo obseg sistema upravljanja in varovanja informacij ter neprekinjenega poslovanja ob upoštevanju rezultatov analize vpliva na poslovanje, kateri mora obsegati najmanj tista informacijska, komunikacijska in druga sredstva, podatke ter procese, ki so potrebni za njihovo delovanje ali opravljanje storitev;

(3) Če ima bistveni ali pomembni subjekt za zagotavljanje varnosti svojih omrežij in informacijskih sistemov že izdelano varnostno dokumentacijo na podlagi drugih predpisov, jo dopolni skladno s tem zakonom.

(4) Vlada lahko podrobneje določi vsebino in strukturo varnostne dokumentacije način izvajanja obveznosti iz tega člena. Pri tem vlada upošteva tudi morebitne dokumente ali tehnična priporočila ENISA, Skupine za sodelovanje in dokumente Evropske komisije.

21. člen (ukrepi za obvladovanje tveganj za kibernetsko varnost bistvenih in pomembnih subjektov)

(1) Bistveni in pomembni subjekti morajo sprejeti ustrezne, učinkovite in sorazmerne tehnične, operativne in organizacijske ukrepe za zagotavljanje celovitosti, avtentičnosti, zaupnosti in razpoložljivosti omrežnih in informacijskih sistemov oziroma za obvladovanje tveganj za varnost omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev ter za preprečevanje ali zmanjšanje vpliva incidentov na prejemnike svojih storitev in druge storitve (v nadaljevanju: varnostni ukrepi).

(2) Varnostni ukrepi morajo temeljiti na pristopu upoštevanja vseh nevarnosti, katerega namen je zaščita omrežnih in informacijskih sistemov ter njihovega fizičnega okolja pred incidenti, in morajo obsegati najmanj:

1. podporo vodstva subjekta pri zagotavljanju informacijske in kibernetske varnosti in vključitvijo področja informacijske in kibernetske varnosti v letni načrt poslovanja oziroma letni program dela;
2. zagotavljanje integritete kadrov v povezavi z informacijsko varnostjo pred zaposlitvijo, med zaposlitvijo in ob prenehanju ali spremembi zaposlitve;
3. osnovne prakse kibernetske higiene in usposabljanje na področju informacijske in kibernetske varnosti;
4. varnost človeških virov, preverjanje identitete uporabnikov, zagotavljanje ravni dostopnosti informacij in upravljanje pooblastil za dostop;
5. izvajanje in upravljanje varnostnih kopij podatkov;
6. zagotavljanje in ohranjanje dnevniških zapisov o delovanju omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev, njihovih uporabnikov in administratorjev za obdobje najmanj šestih mesecev, lahko pa tudi za daljše obdobje, kadar iz analize obvladovanja tveganj in ocene sprejemljive ravni tveganj izhaja, da bi bilo tveganja ustrezno obvladovati z daljšo hrambo dnevniških zapisov. Ohranjanje dnevniških zapisov se zagotavlja primarno na ozemlju Republike Slovenije, sekundarno pa se lahko zagotavlja na ozemlju Evropske unije, razen subjektov s področja digitalne infrastrukture, bančništva in infrastrukture finančnega trga, kateri lahko ohranjanje dnevniških zapisov v celoti zagotavlja na ozemlju Evropske unije;

21. člen (ukrepi za obvladovanje tveganj za kibernetsko varnost bistvenih in pomembnih subjektov)

7. upravljanje omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev z določitvijo ustrezne odgovornosti za njihovo zaščito;
8. politike in postopke v zvezi z uporabo kriptografije in po potrebi šifriranjem;
9. upravljanje prometa in komunikacij;
10. varnost dobavne verige z določitvijo ustreznih minimalnih zahtev povezanih s kibernetsko varnostjo za ključne dobavitelje ali ponudnike storitev, ki se nanašajo na odnose med posameznim subjektom in njegovimi neposrednimi dobavitelji ali ponudniki storitev;
11. fizično in tehnično varovanje prostorov in dostopov do prostorov, kjer so ključni deli omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev;
12. varnostne mehanizme v posamezni aplikativni programski opremi za izvajanje dejavnosti, vključno z varnostjo pri pridobivanju, razvoju in vzdrževanju omrežnih in informacijskih sistemov ter obravnavanjem in razkrivanjem ranljivosti;
13. upravljanje in preprečevanje izrab tehničnih ranljivosti;
14. zaščita pred zlonamerno programsko kodo, zaznavanje poskusov vdorov in preprečevanje incidentov;
15. uporabo večfaktorske avtentikacije ali rešitev neprekinjene avtentikacije, kadar je to potrebno zaradi obvladovanja tveganj za kibernetsko varnost in
16. uporabo varovanih glasovnih, video in besedilnih komunikacij in varnih sistemov za komunikacije v sili znotraj subjekta, kadar je glede na dejavnost subjekta to primerno.

25. člen (obveznost priglašanja in obveščanja)

(1) Bistveni in pomembni subjekti pristojni skupini CSIRT brez nepotrebnega odlašanja v skladu s prvim in drugim odstavkom 26. člena tega zakona in nacionalnim načrtom odzivanja iz drugega odstavka 11. člena tega zakona 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 znatne operativne motnje pri opravljanju storitev ali finančne izgube;**
- **je vplival ali bi lahko vplival na druge fizične ali pravne osebe s povzročitvijo precejšnje premoženjske ali nepremoženjske škode.**

(2) Pri vrednotenju pomembnosti incidenta bistveni in pomembni subjekti upoštevajo prizadetost omrežnih in informacijskih sistemov, zlasti njihov pomen pri zagotavljanju storitev subjekta, resnost in tehnične značilnosti kibernetske grožnje in njihovega vpliva na uporabnike, obstoječe ranljivosti, ki se izkoriščajo, ter izkušnje subjekta s podobnimi incidenti. Bistveni in pomembni subjekti pri priglašanju iz prejšnjega odstavka upoštevajo morebitne izvedbene akte Evropske komisije iz prvega pododstavka enajstega odstavka 23. člena Direktive (EU) 2022/2555, s katerimi ta podrobneje določi vrsto informacij, obliko in postopek priglasitve ter prostovoljne priglasitve in obvestila.

(3) Ponudniki storitev DNS, registri TLD imen, ponudniki storitev računalništva v oblaku, ponudniki storitev podatkovnih centrov, ponudniki omrežij za dostavo vsebine, ponudniki upravljanih storitev, ponudniki upravljanih varnostnih storitev, kot tudi ponudniki spletnih tržnic, spletnih iskalnikov in platform za storitve družbenega mreženja, pri priglašanju iz prejšnjega odstavka, upoštevajo izvedbene akte Evropske komisije iz drugega pododstavka enajstega odstavka 23. člena Direktive (EU) 2022/2555, v katerih so zanje podrobneje določeni primeri, ko se incident šteje za pomembnega.

(4) Bistveni in pomembni subjekti iz prvega odstavka tega člena, ki niso subjekti iz prejšnjega odstavka upoštevajo morebitne izvedbene akte Evropske komisije iz drugega pododstavka enajstega odstavka 23. člena Direktive (EU) 2022/2555, v katerih so zanje podrobneje določeni primeri, ko se incident šteje za pomembnega. Če Evropska komisija takšnih izvedbenih aktov ne sprejme, se za te subjekte upošteva metodologija za določitev pomembnosti incidenta, kot je opredeljena v nacionalnem načrtu odzivanja.

(5) Bistveni in pomembni subjekti pristojni skupini CSIRT sporočijo vse potrebne informacije, da le-ta določi čezmejni vpliv pomembnega incidenta. V primeru pomembnega čezmejnega ali medsektorskega pomembnega incidenta se ustrezna informacija pravočasno posreduje enotni kontaktni točki v skladu s 26. členom tega zakona.

26. člen (postopek priglasitve pomembnih incidentov)

(1) Bistveni in pomembni subjekti za namen priglasitve pomembnih incidentov iz prvega in drugega odstavka prejšnjega člena pristojni skupini CSIRT predložijo:

1. brez nepotrebnega odlašanja, v vsakem primeru pa v 24 urah po zaznavi pomembnega incidenta, zgodnje opozorilo, iz katerega je po potrebi razvidno, ali je bil pomemben incident domnevno povzročen z nezakonitim ali zlonamernim dejanjem ali bi lahko imel čezmejni vpliv;
2. brez nepotrebnega odlašanja, v vsakem primeru pa v 72 urah po zaznavi pomembnega incidenta, priglasitev incidenta, s katero se po potrebi posodobijo informacije iz točke ena in navede začetna ocena pomembnega incidenta, vključno z njegovo resnostjo in vplivom ter, kadar so na voljo, kazalniki ogroženosti;
3. na zahtevo skupine CSIRT vmesno poročilo o ustreznih posodobitvah stanja;
4. končno poročilo, najpozneje v enem mesecu po predložitvi priglasitve incidenta iz točke dva, ki vključuje naslednje:
   - **podroben opis incidenta, vključno z njegovo resnostjo in vplivom;**
   - **vrsto grožnje ali temeljnega vzroka, ki je verjetno sprožil incident;**
   - **izvedene blažilne ukrepe in take ukrepe v teku;**
   - **po potrebi čezmejni vpliv incidenta;**
5. v primeru pomembnega incidenta, ki je ob predložitvi končnega poročila iz točke štiri še vedno v teku, priglasitveni subjekt predloži poročilo o napredku, končno poročilo pa najpozneje en mesec po razrešitvi incidenta.

(2) Ne glede na določbo 2. točke prejšnjega odstavka mora ponudnik storitev zaupanja v zvezi s pomembnimi incidenti, ki vplivajo na zagotavljanje njegovih storitev, o tem brez nepotrebnega odlašanja, v vsakem primeru pa v 24 urah po zaznavi pomembnega incidenta, uradno obvesti pristojno skupino CSIRT.

31. člen (prostovoljna priglasitev)

(1) Zavezani subjekti lahko poleg obvezne priglasitve iz 26. člena tega zakona skupinam CSIRT prostovoljno priglasijo incidente, kibernetske grožnje in skorajšnje incidente in jim predložijo ustrezne informacije. Pri prostovoljni priglasitvi se glede skupine CSIRT, ki se ji priglaša, smiselno uporabljata drugi in tretji odstavek 12. člena tega zakona.

(2) Subjekti, ki niso zavezanci po tem zakonu, ne glede na to, ali spadajo na področje uporabe tega zakona, lahko prostovoljno priglasijo pomembne incidente, kibernetske grožnje in skorajšnje incidente skupini CSIRT SI-CERT in ji predložijo ustrezne informacije.

(3) Prostovoljna priglasitev iz prvega in prejšnjega odstavka skupine CSIRT obravnavajo v skladu s postopkom iz 26. člena tega zakona. Pri prostovoljnem poročanju za priglasitveni subjekt ne veljajo nikakršne dodatne obveznosti, kar pa ne vpliva na preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj.

(4) Pristojni skupini CSIRT po potrebi informacije o priglasitvah, prejetih v skladu s tem členom, kadar je potrebno, posredujejo pristojnemu nacionalnemu organu v vlogi enotne kontaktne točke, pri čemer poskrbijo za zaupnost in ustrezno varstvo informacij, ki jih je posredoval priglasitveni subjekt.

(5) Pristojni skupini CSIRT pred prostovoljnimi priglasitvami lahko prednostno obravnavata obvezne priglasitve. Pri določanju vrstnega reda obdelave prostovoljnih priglasitev upoštevata vpliv prostovoljno priglašenih incidentov na neprekinjeno izvajanje storitev zavezanih subjektov ter morebitni čezmejni vpliv.

(6) Prostovoljne priglasitve, ki nimajo vpliva ali imajo zanemarljiv vpliv na izvajanje storitev zavezanih subjektov in imajo zanemarljiv čezmejni vpliv, se obdela le, kadar takšna obdelava skupinama CSIRT ne pomeni nesorazmernega ali neupravičenega bremena.

(7) Prostovoljna priglasitev ustreznih informacij iz tega člena se lahko izvaja tudi po namenski digitalni platformi iz desetega odstavka 26. člena tega zakona.

Hvala za pozornost.