REPUBLIKA SLOVENIJA
MINISTRSTVO ZA ZDRAVJE

NAČRT ZA OKREVANJE IN ODPORNOST

Financira Evropska unija
NextGenerationEU

Predstavitev zakonodajnih obveznosti po ZinfV-1 za izvajalce v zdravstvu

Kory Golob,
Urad Vlade Republike Slovenije za informacijsko varnost

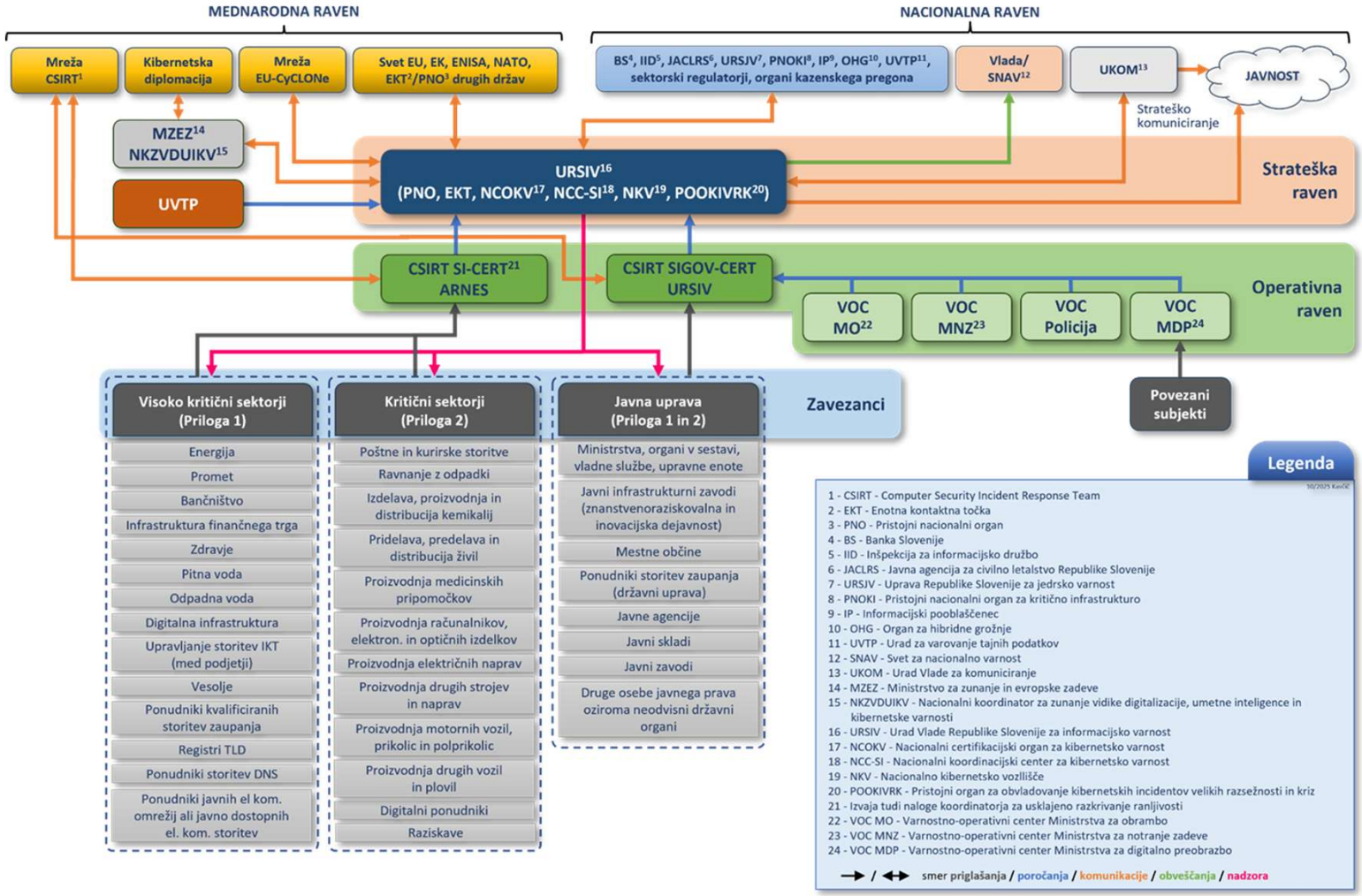
URSIV

Konferenca NOO eZdravje 2026
Brdo, 3. marec 2026

Vsebina

- Uvod
- Stanje kibernetske varnosti
- Zavezanci ZInfV-1 s poudarkom na sektor ZDRAVJE
- Obveznosti po ZInfV-1
- Vrednotenje incidentov, ocena ogroženosti in ukrepanje
- Dolžno nadzorstvo in inšpekcijski nadzor
- Zaključek

Uvod


MEDNARODNA RAVEN
NACIONALNA RAVEN
Mreža CSIRT[1]
Kibernetska diplomacija
Mreža EU-CyCLONe
Svet EU, EK, ENISA, NATO, EKT[2]/PNO[3] drugih držav
BS[4], IID[5], JACLRS[6], URSJV[7], PNOKI[8], IP[9], OHG[10], UVTP[11], sektorski regulatorji, organi kazenskega pregona
Vlada/ SNAV[12]
UKOM[13]
JAVNOST
Strateško komuniciranje
MZEZ[14] NKZVDUIKV[15]
UVTP
URSIV[16] (PNO, EKT, NCOKV[17], NCC-SI[18], NKV[19], POOKIVRK[20])
Strateška raven
CSIRT SI-CERT[21] ARNES
CSIRT SIGOV-CERT URSIV
VOC MO[22]
VOC MNZ[23]
VOC Policija
VOC MDP[24]
Operativna raven
Visoko kritični sektorji (Priloga 1)
Kritični sektorji (Priloga 2)
Javna uprava (Priloga 1 in 2)
Zavezanci
Povezani subjekti
Energija
Promet
Bančništvo
Infrastruktura finančnega trga
Zdravje
Pitna voda
Odpadna voda
Digitalna infrastruktura
Upravljanje storitev IKT (med podjetji)
Vesolje
Ponudniki kvalificiranih storitev zaupanja
Registri TLD
Ponudniki storitev DNS
Ponudniki javnih el kom. omrežij ali javno dostopnih el. kom. storitev
Poštne in kurirske storitve
Ravnanje z odpadki
Izdelava, proizvodnja in distribucija kemikalij
Pridelava, predelava in distribucija živil
Proizvodnja medicinskih pripomočkov
Proizvodnja računalnikov, elektron. in optičnih izdelkov
Proizvodnja električnih naprav
Proizvodnja drugih strojev in naprav
Proizvodnja motornih vozil, prikolic in polprikolic
Proizvodnja drugih vozil in plovil
Digitalni ponudniki
Raziskave
Ministrstva, organi v sestavi, vladne službe, upravne enote
Javni infrastrukturni zavodi (znanstvenoraziskovalna in inovacijska dejavnost)
Mestne občine
Ponudniki storitev zaupanja (državni uprava)
Javne agencije
Javni skladi
Javni zavodi
Druge osebe javnega prava oziroma neodvisni državni organi
Legenda
1 - CSIRT - Computer Security Incident Response Team
2 - EKT - Enotna kontaktna točka
3 - PNO - Pristojni nacionalni organ
4 - BS - Banka Slovenije
5 - IID - Inšpekcija za informacijsko družbo
6 - JACLRS - Javna agencija za civilno letalstvo Republike Slovenije
7 - URSJV - Uprava Republike Slovenije za jedrsko varnost
8 - PNOKI - Pristojni nacionalni organ za kritično infrastrukturo
9 - IP - Informacijski pooblaščenec
10 - OHG - Organ za hibridne grožnje
11 - UVTP - Urad za varovanje tajnih podatkov
12 - SNAV - Svet za nacionalno varnost
13 - UKOM - Urad Vlade za komuniciranje
14 - MZEZ - Ministrstvo za zunanje in evropske zadeve
15 - NKZVDUIKV - Nacionalni koordinator za zunanje vidike digitalizacije, umetne inteligence in kibernetske varnosti
16 - URSIV - Urad Vlade Republike Slovenije za informacijsko varnost
17 - NCOKV - Nacionalni certifikacijski organ za kibernetsko varnost
18 - NCC-SI - Nacionalni koordinacijski center za kibernetsko varnost
19 - NKV - Nacionalno kibernetsko vozlišče
20 - POOKIVRK - Pristojni organ za obvladovanje kibernetskih incidentov velikih razsežnosti in kriz
21 - Izvaja tudi naloge koordinatorja za usklajeno razkrivanje ranljivosti
22 - VOC MO - Varnostno-operativni center Ministrstva za obrambo
23 - VOC MNZ - Varnostno-operativni center Ministrstva za notranje zadeve
24 - VOC MDP - Varnostno-operativni center Ministrstva za digitalno preobrazbo
→ / ↔ smer priglašanja / poročanja / komunikacije / obveščanja / nadzora

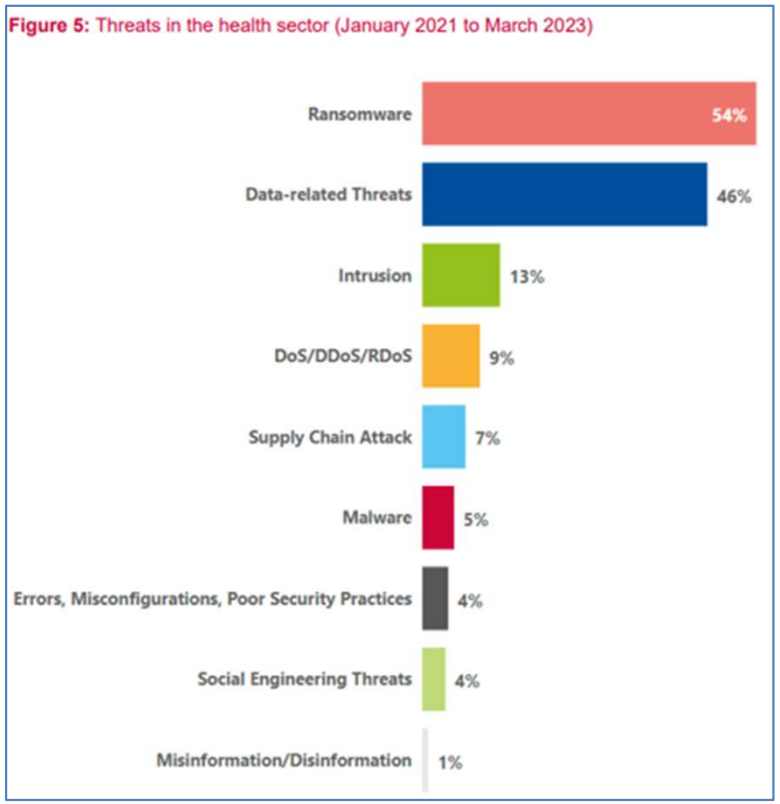
Stanje kibernetske varnosti

- Pospešena digitalizacija in velika povezljivosti družbe in gospodarstva
- Večja kompleksnost, nepredvidljivost in širša prisotnost kibernetskih groženj
- Vpliv političnega in geopolitičnega dogajanja na krajino kibernetskih aktivnosti (volitve v EP; nestalno članstvo RS v Varnostnem svetu OZN; podpora držav v povezavi z vojno v Ukrajini, konflikt v Palestini)
- V 2024/25 je bila stopnja kibernetske ogroženosti na ravni EU in RS ocejena kot VISOKO trenutno je v Republiki Sloveniji ocenjena kot SREDNJA

Stanje kibernetske varnosti

- Zdravstveni sektor je posebej izpostavljen zaradi:
  - občutljivih zdravstvenih podatkov
  - potencialnega vpliva na življenje ljudi
  - pogostih ransomware napadov

INFO: Ransomware je predstavljal 54 % analiziranih kibernetskih incidentov v zdravstvenem sektorju v obdobju 2021–2023. 83 % napadov je bilo **finančno motiviranih**, kar je posledica visoke vrednosti zdravstvenih podatkov, medtem ko je imelo 10 % napadov ideološko motivacijo. (vir: ENISA)



Stanje kibernetske varnosti

- Sektor zdravja posebej ranljiv zaradi:
  - starejših IT sistemov
  - povezanih medicinskih naprav (IoMT)
  - zunanjih ponudnikov (outsourcing IT)
  - visoke vrednosti zdravstvenih podatkov na črnem trgu

INFO: Med pandemijo **COVID-19** je napad z izsiljevalskim programjem ohromil velik del irskega zdravstvenega sistema. Odpoved vsaj nekaterih storitev v 31 od 54 bolnišnic.

NHS cyber attack led to patient death

Delayed blood test result contributed to person dying after 2024 ransomware attack

The hackers caused significan
Devlin/PA

University Hospital Brno is used to test patients for coronavirus infections – cyberattack halts the operations

rly disrupted
rformed

U TIJEKU KRIMINALISTIČKO ISTRAŽIVANJE

Hakeri srušili sustav na Rebru, oglasila se zagrebačka policija: 'Utvrđujemo okolnosti napada'

Piše HINA, četvrtak, 27.6.2024. u 14:32

UKC Maribor tarča hekerskega napada

Maribor, 07. 01. 2026 15.12 • 1 min branja • 19

V Univerzitetnem kliničnem centru (UKC) Maribor je v petek v zgodnjih jutranjih urah prišlo do hekerskega napada. "Varovalni sistemi so zaznali vdor in takoj so se začele aktivnosti za omejitev napadalca. Napad je bil prekinjen, preden je napadalec uspel ogroziti delovanje IT sistema," so povedali v UKC Maribor.

Stanje kibernetske varnosti

Kompromitacija podatkov pacientov

Kraja zdravstvenih podatkov lahko vodi v krajo identitete ali goljufijo.

Kršitev varstva osebnih podatkov

Neskladnost povzroči globe in pravne težave.

Motnje v delovanju zdravstvenih storitev

Zaklenjeni sistemi preprečijo dostop do zdravstvene dokumentacije ali naprav, ki rešujejo življenja.

Ogrožanje varnosti pacientov

Spremenjeni ali izbrisani podatki lahko vodijo do napačnih diagnoz ali napak pri zdravljenju.

Izguba zaupanja in ugleda

Okrnjen odnos med pacienti in izvajalci zdravstvenih storitev.

Finančne izgube

Operativne motnje, stroški obnovitve in tožbe.

Kraja intelektualne lastnine

Izguba raziskovalnih podatkov ali medicinskih inovacij.

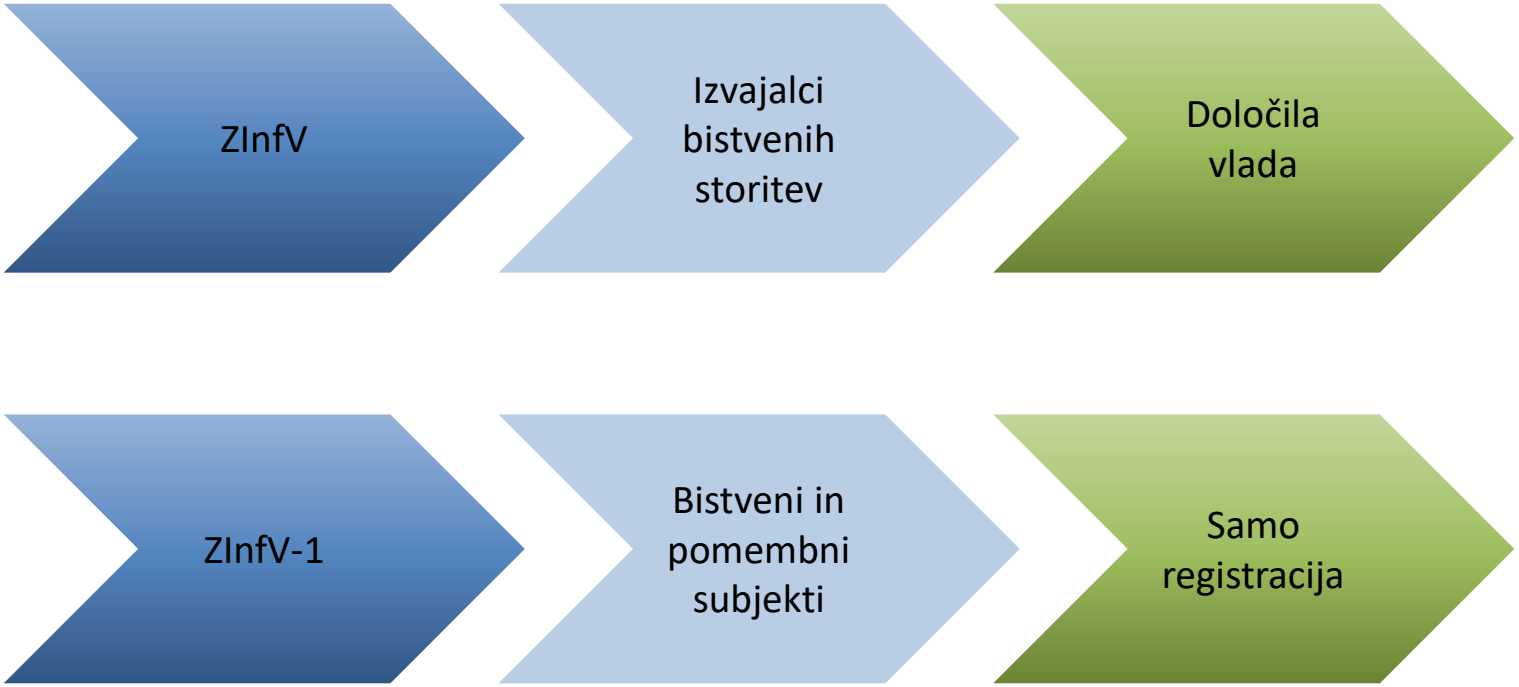
Stanje kibernetske varnosti

- Neustrezna zaščita lahko vodi do izpada nujnih zdravstvenih storitev.
- Motnje v IT sistemih lahko neposredno vplivajo na zdravstveno stanje pacientov.
- Kompromitirani podatki pomenijo kritičen vpliv na zasebnost in varnost.
- Primeri kažejo, da kibernetske grožnje zdravstvu niso več retorične – so realne in sistemske.

- Zato Direktiva NIS2 posebej poudarja:
  - varnost medicinskih naprav,
  - segmentacijo omrežij,
  - zaščito bolnišničnih sistemov,
  - varnost dobaviteljev IT rešitev.

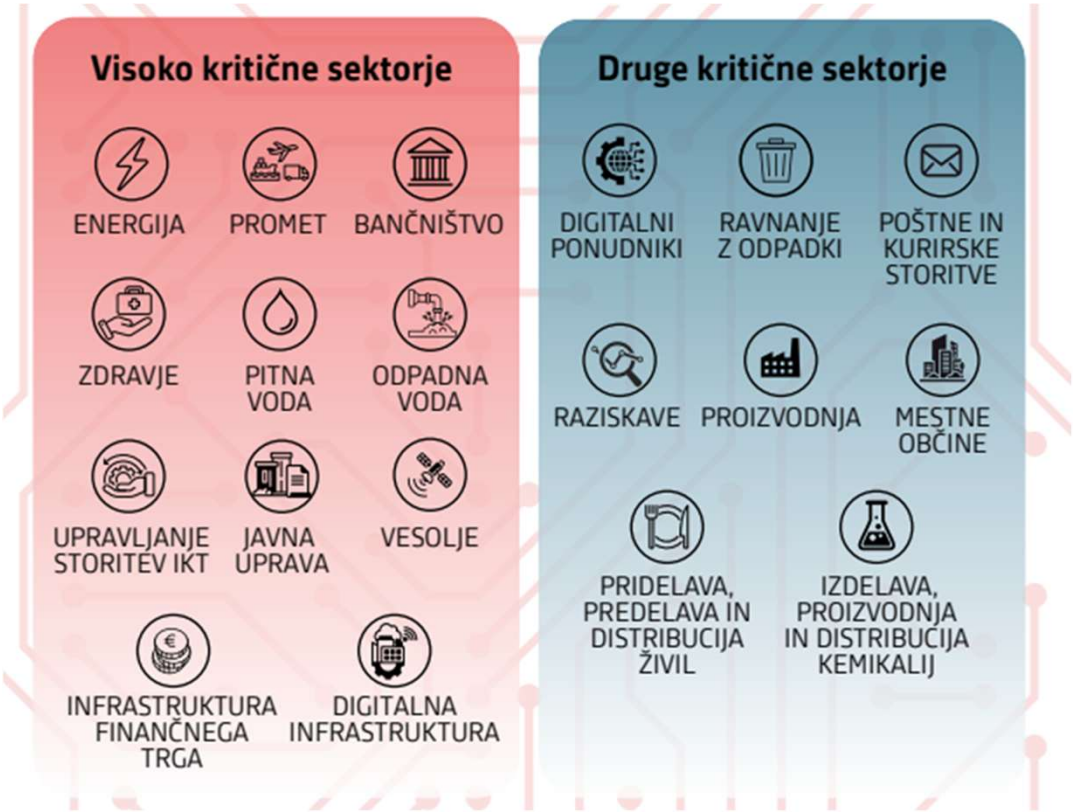
Zavezanci po ZInfV-1

ZInfV vs. ZInfV-1



Zavezanci po ZInfV-1

So subjekti, ki spadajo med vrste subjektov iz Prilog 1 ali Priloge 2 ZInfV-1.



Zavezanci po ZInfV-1

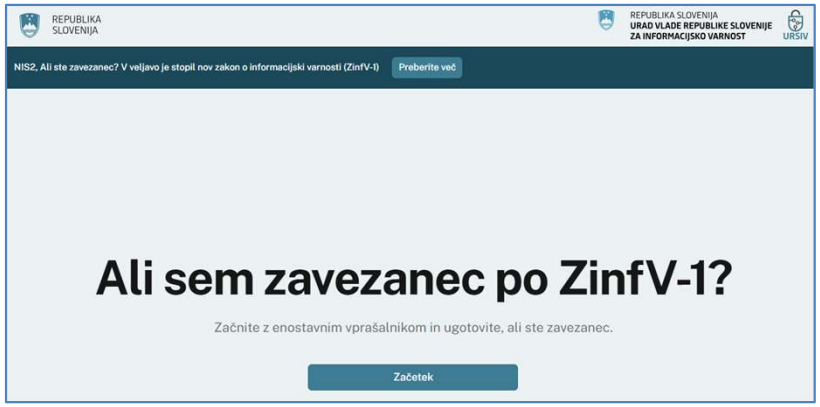
Priloga 1 / Visoko kritični sektorji

5. Zdravje

- izvajalci zdravstvene dejavnost
- referenčni laboratoriji EU
- subjekti, ki izvajajo raziskovalne in razvojne dejavnosti na področju zdravil
- subjekti, ki proizvajajo farmacevtske surovine in preparate
- subjekti, ki proizvajajo medicinske pripomočke, ki se štejejo za kritične
- subjekti, ki imajo dovoljenje za promet z zdravili na debelo

Zavezanci po ZInfV-1

- Samoregistracija
  - storitev / vrsta subjekta (priloga 1 in priloga 2)
  - velikost (50 zaposlenih; 10 mio EUR letni promet ali 10 mio EUR letna bilančna vsota)
- Odločba vlade
- Določanje po ZKI-1
- 23. člen ZVOP-2



POMNI: Samoregistracija je bistvena razlika med ZInfV in ZInfV-1. Kljub določitvi z odločbo vlade subjekt opravi samoregistracijo.

Obveznosti po ZInfV-1

Ukrepi za obvladovanje tveganj in priglasitev incidentov

- Odgovornost
- Usposabljanje in izobraževanje
- Varnostna dokumentacija
- Ukrepi za obvladovanje tveganj
- Zagotavljanje integritete kadrov pred, med in po zaposlitvi
- Ohranjanje dnevniških zapisov skladno z zakonodajo
- Varnost dobavne verige
- Ocena in samoocena skladnosti
- Priglasitev incidentov

Obveznosti po ZInfV-1

- **ZInfV-1** stopil v veljavo **19. 6. 2025**
- **zavezanci iz ZInfV (IBS, ODU)** imajo rok za uskladitev varnostne dokumentacije in varnostnih ukrepov z ZInfV-1 **do 19. 6. 2026**
- **bistveni in pomembni subjekti (novi)** imajo rok za uskladitev varnostne dokumentacije in varnostnih ukrepov z ZInfV-1 **do 19. 12. 2026**
- **operaterji po ZEKom-2** (ki so zavezanci) imajo rok za uskladitev varnostne dokumentacije in varnostnih ukrepov z ZInfV-1 **do 19. 6. 2026**

Obveznosti po ZInfV-1

Upravljanje (20. člen ZinfV-1)

Odgovorna oseba mora:

- ✅ odobriti ustreznost ukrepov za obvladovanje tveganj
- 🤦 zagotoviti redna usposabljanja svojim zaposlenim
- 👁️ nadzirati izvajanje ukrepov za obvladovanje tveganj
- 💡 opraviti usposabljanja za prepoznavanje tveganj (na štiri leta)
- ⚠️ prevzeti odgovornost za neizpolnjevanje obveznosti

Obveznosti po ZInfV-1

Varnostna dokumentacija (21. člen ZInfV-1)

📘 Varnostne politike – Splošna in področne politike za upravljanje varnosti

🗒️ Popis sredstev – Popis informacijskih sredstev in podatkov ter določenih upravljavcev.

⚖️ Analiza tveganj – Opredelitev sprejemljive ravni tveganj in uporabljene metodologije.

🔄 Načrt neprekinjenega poslovanja:

- Ocena vpliva na poslovanje
- Minimalna raven poslovanja
- Upravljanje varnostnih kopij
- Vloge in odgovornosti

POMNI: Dokumentirani sistem upravljanja varovanja informacij in sistem upravljanja neprekinjenega poslovanja temeljita **na pristopu upoštevanja vseh nevarnosti**.

Obveznosti po ZInfV-1

Varnostna dokumentacija (21. člen ZInfV-1)

🛠️ Načrt obnovitve sistemov – Postopki in odgovornosti za obnovitev po motnji.

🚨 Načrt odzivanja na incidente:

- Obveščanje skupine CSIRT
- Sistem zaznave in odziva
- Opis vlog in odgovornosti

🔐 Načrt varnostnih ukrepov – Zagotavljanje zaupnosti, celovitosti, avtentičnosti in razpoložljivosti.

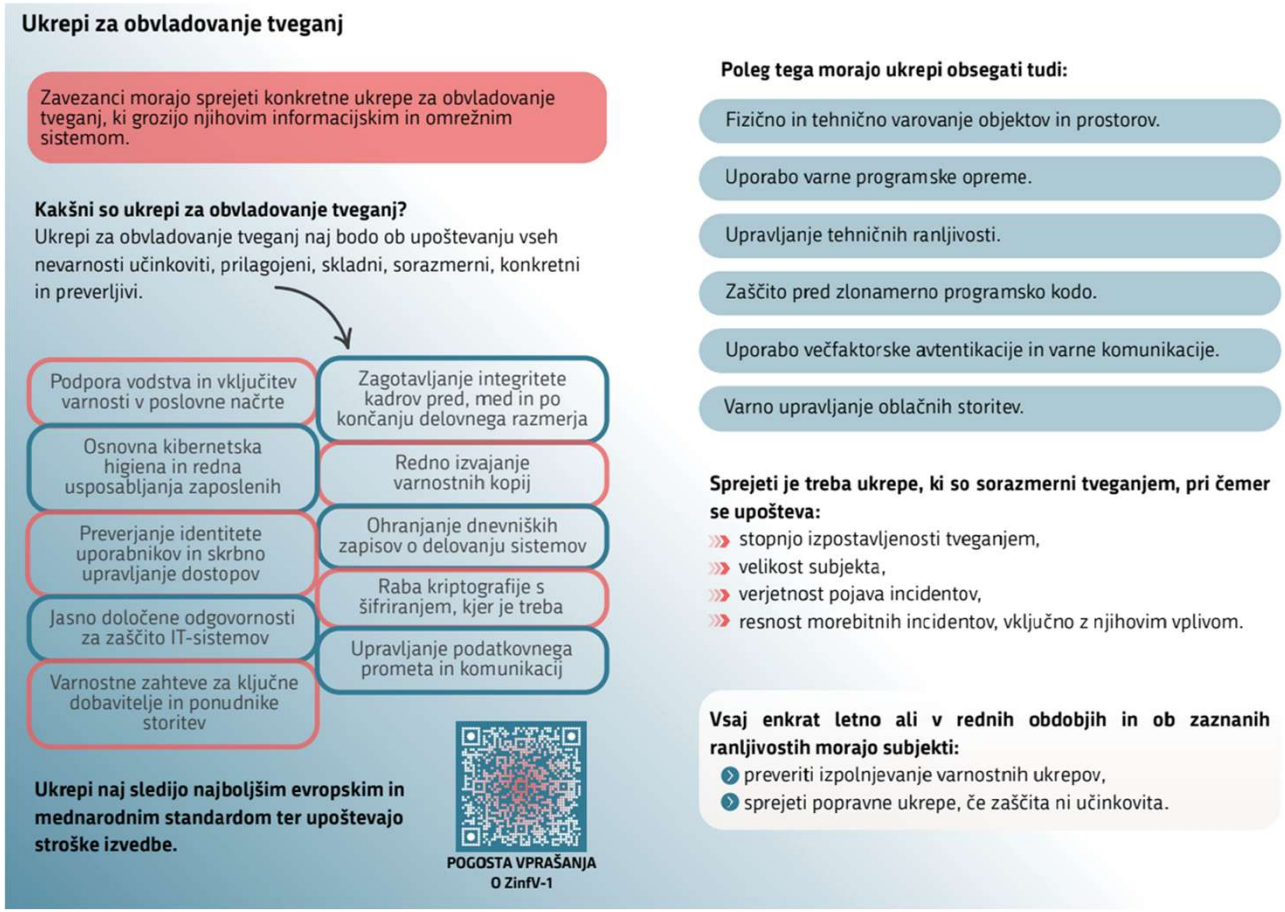
📈 Presoja učinkovitosti:

- Kazalniki učinkovitosti
- Analiza zbranih podatkov

INFORMACIJA: URSIV je pripravil **vzorčno varnostno dokumentacijo** za mala in srednja podjetja.

Obveznosti po ZInfV-1

Ukrepi za obvladovanje kibernetskih tveganj (22. člen ZInfV-1)



Obveznosti po ZInfV-1

Preverjanje preteklosti (23. člen ZInfV-1)

- Z namenom zagotavljanja integritete kadrov pred, med in po zaposlitvi bistveni ali pomembni subjekt lahko ob upoštevanju ocene tveganja preveri preteklost **zaposlenih** in **kandidatov za zaposlitev** na delovnih mestih, pomembnih za opravljanje storitev subjekta, ki imajo ali bodo imeli pooblastilo za neposredni ali oddaljeni dostop do njegovih ključnih informacijskih sistemov.
- Preverjanje preteklosti se opravi **za zadnjih pet let**.

POMNI: Zavezanec **lahko preveri** preteklost tudi za **zaposlene pri pogodbenih izvajalcih**

Obveznosti po ZInfV-1

Dnevniški zapisi (24. člen ZInfV-1)

- Hramba dnevniških zapisov je pomembna, ker zagotavlja **sledljivost** delovanja informacijskih sistemov ter omogoča učinkovito **odkrivanje** in **preiskovanje** varnostnih incidentov in napak.
- Predstavlja ključen **dokazni vir** pri revizijah in preverjanju skladnosti z zakonodajo ter internimi varnostnimi zahtevami.
- Pravilna hramba logov povečuje odgovornost uporabnikov in izboljšuje upravljanje informacijskih tveganj.

POMNI: Zavezanec hrani dnevniške zapise za **najmanj šest mesecev**, lahko pa tudi za daljše obdobje

Obveznosti po ZInfV-1

Ocena in samoocena skladnosti (25. člen ZInfV-1)

Oceno skladnosti izvedejo bistveni subjekti:

- najmanj na dve leti,
- revizija/notranja revizija
- poročilo o skladnosti

Samoocena skladnosti izvedejo pomembni subjekti:

- najmanj na dve leti preverjanje dokumentacije in ukrepov
- lahko tudi notranja revizija

INFO: **Vprašalnik za samooceno** je objavljen na spletni strani URSIV.

OPOMBA: Inšpektor lahko **odredi tudi izvedbo revizije skladnosti** s predpisi s področja informacijske in kibernetske varnosti.

Obveznosti po ZInfV-1

Obveznost preglašanja in obveščanja (29. člen ZInfV-1)

- Zavezanci imajo obveznost priglasitve **pomembnih incidentov.**
- Prijava ni kaznovanje, temveč pomoč pri obravnavi in zaščiti širšega kibernetskega EU prostora.
- Pravočasne informacije o incidentu lahko pomagajo vam za nadaljnje poslovanje ali drugim organizacijam za preprečitev škode.

DEFINICIJA: **Pomemben incident:**
– 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**.

Obveznosti po ZInfV-1

Postopek priglasitve pomembnih incidentov (30. člen ZInfV-1)

- nemudoma/v 24 urah: prvo, "**zgodnje sporočilo**" o zaznavi pomembnega incidenta

- v 72 urah: **formalna priglasitev** incidenta (trenutno obrazec Priloga E iz NOKI)

- vmesna poročila: po potrebi, če incident še traja ali se razvija

- končno poročilo: najpozneje v enem mesecu po priglasitvi / rešitvi incidenta

INFO: URSIV pripravlja **platformo** za priglasitev incidentov in obveščanje.

Vrednotenje incidenta, ocena ogroženosti in ukrepanje

URSIV kot pristojni nacionalni organ, skladno s 37. členom ZInfV-1 na podlagi podatkov in informacij, ki se nanašajo na varnost omrežij in informacijskih sistemov, izdela oceno ogroženosti kibernetske varnosti v Republiki Sloveniji.

⚠️ URSIV glede na pridobljene podatke in upoštevaje aktualne trende kibernetskih incidentov v Republiki Sloveniji ter širše dogajanje na kibernetskem področju ocenjuje, da je ogroženost srednja.

Spremljajte
(37. člen ZINfV-1)

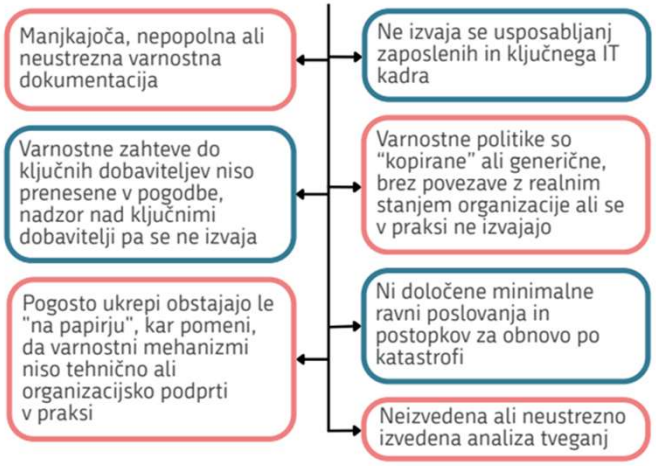
Ocena ogroženosti kibernetske varnosti v Republiki Sloveniji

POMNI: Gre za **nacionalne določbe** ZInfV-1.

Dolžno nadzorstvo in inšpekcijski nadzor

Potek inšpekcijskega nadzora

Pogoste ugotovitve inšpekcijskega nadzora



Inšpekcija spodbuja preventivni pristop – bolje pripravljena organizacija pomeni manj težav ob nadzoru in višjo raven zaščite pred kibernetskimi grožnjami.

Status zavezanca sam po sebi ne pomeni skladnosti z zakonom – organizacija mora sprejete ukrepe tudi dejansko izvajati in jih preverjati.

Nasvet 1: Poskrbite, da so vsi vaši dokumenti usklajeni z zahtevami ZInfV-1 in da so ukrepi kibernetske varnosti dokumentirani, uvedeni in preverljivi v praksi.

Nasvet 2: S ključnimi dobavitelji oziroma pogodbenimi partnerji sklenite anekse k veljavnim pogodbam, v katerih boste od njih zahtevali izvajanje predpisanih varnostnih ukrepov in omogočili izvajanje dolžnega nadzorstva.

Akcijski načrt EU za izboljšanje kibernetske varnosti bolnišnic in ostalih ponudnikov zdravstvenih storitev

PREPREČEVANJE

- Smernice o ukrepih kibernetske varnosti
- Ocenjevanje zrelosti in testiranje pripravljenosti
- Vavčerji za kibernetsko varnost
- Kibernetska varnost dobavne verige
- Usposabljanje za razvoj veščin in mreža direktorjev za informacijsko varnost (CISO) v zdravstvenem sektorju

ZAZNAVANJE

- Skupna evropska storitev za zgodnje zaznavanje kibernetskih groženj v zdravstvenem sektorju
- Podpora za evropske zdravstvene ISAC (Information Sharing and Analysis Centers)
- Katalog znanih eksplicitnih ranljivosti (Known Explicited Vulnerabilities - KEV)

ODZIVANJE

- Posebna storitev hitrega odzivanja v sklopu kibernetske rezerve EU
- Zbirke ukrepov za odzivanje na incidente
- Vaje kibernetske varnosti

OKREVANJE

- Naročniška storitev za obnovitev po izsiljevalski programski opremi – razširjena zbirka orodij za dešifriranje
- Priporočilo za prijavo plačil izsiljevalski programski opremi

ODVRAČANJE

- Orodje kibernetske diplomacije
- Direktiva o napadih na informacijske sisteme in Budimpeštanska konvencija
- Mednarodno sodelovanje: CRI, G7

Evropski podporni center za kibernetsko varnost za bolnišnice in ponudnike zdravstvenih storitev (ENISA)

Svetovalni odbor za kibernetsko varnost v zdravstvu

Nacionalni akcijski načrti

Zaključek

CYBER HYGIENE PRACTICES

- 1/ PROTECT YOUR SYSTEMS & MEDICAL DEVICES
- 2/ PROTECT YOUR NETWORKS
- 3/ MIND THE SECURITY OF SMARTPHONES & E-CARE
- 4/ KEEP PATIENT RECORDS SAFE
- 5/ TAKE INCIDENTS SERIOUSLY
- 6/ MANAGE THE ICT SUPPLY CHAIN
- 7/ CYBER-EDUCATE YOUR STAFF
- 8/ PHYSICAL SECURITY

Hvala za pozornost.