

**STRATEGIJA KIBERNETSKE VARNOSTI
REPUBLIKE SLOVENIJE
2027–2035**

Osnutek

Oktober 2026

KAZALO

POVZETEK	4
UVOD	6
IZHODIŠČA	8
Analiza izvajanja Strategije kibernetске varnosti Republike Slovenije 2016–2025	8
Doseženo v obdobju 2016–2025	8
Ključni izzivi in nadaljnje razvojne potrebe	9
VIZIJA, PREDNOSTNI NALOGI IN CILJI	11
OKVIR UPRAVLJANJA IN ODGOVORNOSTI	11
Nosilci nalog v nacionalnem sistemu kibernetске varnosti	11
Strateške usmeritve	12
NACRT ZA KREPITEV SPLOŠNE DRUŽBENE OZAVEŠČENOSTI O KIBERNETSKI VARNOSTI	14
Strateške usmeritve	14
KREPITEV MEHANIZMOV ZA ODZIVANJE NA INCIDENTE, VKLJUČNO S SODELOVANJEM MED JAVNIM IN ZASEBNIM SEKTORJEM	15
Strateške usmeritve	15
KREPITEV NACIONALNEGA SISTEMA KIBERNETске VARNOSTI	16
Strateške usmeritve	16
KREPITEV ODPORNOSTI DRUŽBE V KIBERNETSKEM PROSTORU	18
Zaščita ključnih digitalnih infrastruktur in javnega jedra interneta	18
Strateške usmeritve	18
Digitalna identiteta in zaupanje v digitalne storitve	18
Strateške usmeritve	19
Kibernetска odpornost proizvodov in storitev z digitalnimi elementi	19
Strateške usmeritve	19
Odpornost gospodarstva ter mikro, malih in srednjih podjetij	20
Strateške usmeritve	20
KREPITEV BOJA PROTI KIBERNETSKEMU KRIMINALU	21
Strateške usmeritve	21
KREPITEV TEHNOLOŠKE ODPORNOSTI IN OBVLADOVANJE PRIHODNIH TEHNOLOGIJ	22
Prehod na postkvantno kriptografijo	22
Strateške usmeritve	22
Varna in suverena raba umetne inteligence	23
Strateške usmeritve	23
MEDNARODNO SODELOVANJE IN MEDSEBOJNA POMOČ	24
Strateške usmeritve	24
KIBERNETСКА VARNOST, ZASEBNOST IN ČLOVEKOVE PRAVICE	25
Strateške usmeritve	25

MEHANIZEM ZA OPREDELITEV USTREZNIH VIROV IN OCENO TVEGANJ.....	26
Zagotavljanje virov za izvajanje strategije.....	26
Strateška usmeritev.....	26
Opredelitev ustreznih virov.....	27
Okvir ocene ogroženosti.....	27
SPREMLJANJE, VREDNOTENJE IN POSODABLJANJE STRATEGIJE.....	28
Strateške usmeritve	28
Zunanje merilo zrelosti.....	28

POVZETEK

Strategija kibernetске varnosti Republike Slovenije 2027–2035 (v nadaljnjem besedilu: strategija) v razmerah nenehnih sprememb v kibernetском prostoru temelji na proaktivnem delovanju vseh akterjev in poudarja nujnost njihovega sodelovanja. Število priglašениh varnostnih dogodkov in kibernetских incidentov kaže na obseg zaznanih in prijavljenih primerov. Leta 2023 je bilo skupinama SI-CERT in SIGOV-CERT skupaj priglašениh 3.227 varnostnih dogodkov in kibernetских incidentov, leta 2024 5.008, leta 2025 pa 5.191. Število priglašениh primerov se je tako med letoma 2023 in 2025 povečalo za 1.964 primerov oziroma 60,9 %. Na razlago trenda vplivajo tudi spremembe zaznavanja, poročanja in obsega zavezancev, zato sam po sebi ne dokazuje sorazmernega povečanja groženj. Navedeni podatki podpirajo potrebo po nadaljnjem razvoju nacionalnih zmogljivosti za preprečevanje, zgodnje zaznavanje, obravnavo in koordinirano odzivanje na kibernetские incidente.

Pretekli varnostni pristopi, usmerjeni predvsem v zaščito pred znanimi grožnjami, ne zadoščajo več. Novo regulativno okolje, ki ga določata Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetске varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (v nadaljnjem besedilu: direktiva NIS2) in Zakon o informacijski varnosti (Uradni list RS, št. 40/25; v nadaljnjem besedilu: ZInfV-1), zahteva učinkovitejše obvladovanje kibernetских tveganj, hitro in podrobno poročanje o incidentih ter tesnejše sodelovanje in izmenjavo informacij. Strategija zato krepi koordinacijo med deležniki v Republiki Sloveniji ter sodelovanje med javnim in zasebnim sektorjem, državnimi organi in mednarodnimi partnerji. Osrednji element strategije je nenehno izboljševanje varnostnih procesov. Kibernetская varnost ni več zgolj odzivanje na incidente, temveč stalen proces prilagajanja dinamičnim in kompleksnejšim grožnjam. Strategija zato posebno pozornost namenja ozaveščanju o kibernetски varnosti ter krepitvi zmogljivosti za učinkovito zaznavanje incidentov, odzivanje nanje in okrevanje po njih. Hkrati obravnava neposredne potrebe po zagotavljanju učinkovitega odziva na incidente in po dolgoročni krepitvi odpornosti digitalnega okolja, kadrovskih zmogljivosti, zaupanja in sodelovanja med deležniki.

Na tej podlagi strategija določa štiri strateške cilje:

1. krepitev nacionalnega sistema kibernetске varnosti,
2. krepitev odpornosti družbe v kibernetском prostoru,
3. krepitev boja proti kibernetскому kriminalu,
4. krepitev tehnološke odpornosti in obvladovanje prihodnjih tehnologij.

Strategija določa temeljne usmeritve in potrebne ukrepe na strateški ravni. Akcijski načrt za izvajanje Strategije kibernetске varnosti Republike Slovenije 2027–2035 pa določa izvedbeno razčlenitev ukrepov, njihove nosilce, sodelujoče deležnike, roke izvedbe in vire financiranja. Opredeljuje tudi finančne in kadrovske posledice ter ključne kazalnike uspešnosti z viri podatkov in obdobji njihovega zajema. Sprejme ga Vlada Republike Slovenije kot izvedbeni dokument strategije.

Prvi akcijski načrt se predloži Vladi Republike Slovenije v sprejem najpozneje v šestih mesecih po sprejetju strategije. Zajema prvo triletno izvedbeno obdobje, njegovo izvajanje pa se preverja najmanj enkrat letno. Vsak ukrep ima vodilnega nosilca, sodelujoče organe in institucije, rok izvedbe, pričakovani rezultat, izhodiščno in ciljno vrednost kazalnika ter potrebne in zagotovljene vire. Vrzal med potrebnimi in

zagotovljenimi finančnimi ter kadrovskimi viri se izrecno prikaže skupaj s predlogom za njeno odpravo in oceno posledic za izvedbo ukrepa.

UVOD

Republika Slovenija je leta 2016 sprejela prvo Strategijo kibernetске varnosti Republike Slovenije, s katero je določila vizijo razvoja in systemske ureditve nacionalnega sistema zagotavljanja kibernetске varnosti. Spremenjene varnostne razmere v mednarodnem okolju, pojav novih in vse kompleksnejših kibernetских groženj, hiter tehnološki razvoj ter obsežne spremembe pravnega okvira na nacionalni ravni in ravni Evropske unije so v preteklem desetletju ustvarili potrebo po posodobitvi vizije, strateških ciljev in ukrepov za zagotavljanje kibernetске varnosti v Republiki Sloveniji. Direktiva NIS2, njen prenos v nacionalni pravni red z ZInfV-1 in drugi relevantni pravni akti Evropske unije, zlasti Akt o kibernetски odpornosti, Akt o kibernetски varnosti in Akt o kibernetски solidarnosti, pomembno spreminjajo evropski okvir kibernetске varnosti. Navedene spremembe skupaj z izkušnjami preteklega desetletja narekujejo celovito prenovo strategije, prilagojeno sodobnim varnostnim in tehnološkim izzivom ter usklajeno z evropskim pravnim in strateškim okvirom.

Od leta 2016 je Republika Slovenija dosegla pomemben napredek na področju kibernetске varnosti. Okrepila je nacionalne zmogljivosti za preprečevanje in zaznavanje incidentov ter odzivanje nanje, izboljšala medresorsko sodelovanje ter povečala ozaveščenost ključnih deležnikov. Krepitev in nadaljnja institucionalna umestitev skupin CSIRT ter sodelovanje Republike Slovenije v mednarodnih kibernetских vajah so pomembno prispevali k večji pripravljenosti in odpornosti na kibernetске grožnje. Uvedene so bile dodatne varnostne zahteve za kritično infrastrukturo, nadgrajeni protokoli za odzivanje na incidente ter uvedene nove varnostne rešitve v javni upravi in gospodarstvu. Okrepljeno je bilo sodelovanje z Evropsko unijo in državami članicami Organizacije Severnoatlantske pogodbe (NATO), Agencijo Evropske unije za kibernetско varnost (ENISA), Evropskim kompetenčnim centrom za kibernetско varnost ter drugimi partnerskimi državami in organizacijami.

Ta strategija določa usmeritve Republike Slovenije za obdobje 2027–2035. Nadgrajuje ter utrjuje temelje, postavljene s strategijo iz leta 2016, hkrati pa težišče premika od vzpostavljanja temeljnih institucionalnih zmogljivosti in struktur k proaktivnemu, povezanemu in merljivemu modelu zagotavljanja kibernetске varnosti. Podrobnejši pregled doseženega in ugotovljenih vrzeli je predstavljen v poglavju »Analiza izvajanja Strategije kibernetске varnosti Republike Slovenije 2016–2025«.

Prednostni nalogi in strateške cilje strategija udejanja s strateškimi usmeritvami, ki se v akcijskem načrtu razčlenijo v konkretne ukrepe z merljivimi kazalniki uspešnosti.¹

Obe prednostni nalogi in štirje strateški cilji ustvarjajo pogoje za učinkovito sodelovanje različnih akterjev ter krepitev medsebojnega zaupanja, s čimer omogočajo njihov dejavni prispevek k zagotavljanju kibernetске varnosti Republike Slovenije.

Kibernetская varnost je skupna naloga vseh deležnikov. Strategija zato opredeljuje ključne akterje, njihove pristojnosti, naloge za prihodnja leta in vire, potrebne za njihovo izvajanje. Temelji na vsedružbenem pristopu, ki zahteva usklajeno delovanje vseh deležnikov. Ključna pogoja za takšno delovanje sta

¹Aksijski načrt za vsak ukrep opredeljuje odgovorni organ, sodelujoče organe, finančne in kadrovske posledice, časovnico ter ključne kazalnike uspešnosti z viri podatkov in obdobjem zajema. Aksijski načrt se po potrebi prilagodi spremembam tehnološkega, geopolitičnega in varnostnega okolja ter ugotovitvam spremljanja izvajanja strategije.

medsebojno zaupanje in učinkovita izmenjava informacij, brez katerih ni mogoče zagotavljati visoke ravni kibernetске varnosti.

Osrednjo vlogo pri usklajevanju aktivnosti na področju kibernetске varnosti ima Urad Vlade Republike Slovenije za informacijsko varnost (v nadaljnjem besedilu: URSIV), ki je pristojni nacionalni organ za informacijsko varnost. Usklajuje ukrepe na področju kibernetске varnosti in spremlja izvajanje strategije. Zagotavlja tudi njeno posodabljanje in prilagajanje spremembam varnostnega, tehnološkega in pravnega okolja. Razdelitev vlog, pristojnosti in odgovornosti je podrobneje opredeljena v poglavju »Okvir upravljanja in odgovornosti«.

Pri izvajanju strategije se bodo dosledno spoštovala načela pravne države, varstva človekovih pravic in temeljnih svoboščin, zasebnosti, zaupnosti komunikacij in varstva osebnih podatkov, skladno z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (Splošna uredba o varstvu podatkov) ter Zakonom o varstvu osebnih podatkov (Uradni list RS, št. 163/22). Ukrepi kibernetске varnosti se načrtujejo in izvajajo ob upoštevanju načel zakonitosti, namenskosti in sorazmernosti. Kadar je to glede na namen in naravo obdelave osebnih podatkov, zlasti posebnih vrst osebnih podatkov, ustrezno, se uporabljajo pristopi in tehnični ukrepi, ki dodatno varujejo zasebnost, kot so anonimizacija, agregacija in šifriranje. Ta načela so podrobneje obravnavana v poglavju »Kibernetска varnost, zasebnost in človekove pravice«.

Namen ukrepov, opredeljenih v strategiji, je zagotoviti ažurno obveščanje o novih izzivih in grožnjah na področju informacijske in kibernetске varnosti, pravočasno sprejemanje ustreznih ukrepov za zmanjševanje ranljivosti omrežnih in informacijskih sistemov, omejevanje možnosti njihovih zlorab ter zmanjševanje škode in drugih negativnih posledic zlonamernih kibernetских dejanj. Ob nastanku incidenta je treba zagotoviti odpornost informacijsko-komunikacijskih sistemov in omrežij ter njihovo čimprejšnjo povrnitev v stanje, ki omogoča varno in zanesljivo izvajanje ključnih funkcij ter neprekinjeno delovanje prizadetih organizacij oziroma čimprejšnjo ponovno vzpostavitev njihovega delovanja. Učinkovito zagotavljanje kibernetске varnosti zahteva stalno spremljanje, prepoznavanje in proaktivno odkrivanje kibernetских groženj ter zlonamernih dejavnosti različnih akterjev. Strategija zato posebej poudarja pomen kibernetске higiene posameznikov in organizacij v Republiki Sloveniji, saj njihovo odgovorno ravnanje pomembno prispeva k preprečevanju incidentov in krepi odpornost ter je temelj aktivne kibernetске obrambe.

V skladu s četrtnim odstavkom 9. člena ZInfV-1 pristojni nacionalni organ sprotno in redno, vsaj vsakih pet let, oceni strategijo na podlagi ključnih kazalnikov uspešnosti, ki izhajajo iz doseganja ciljev in prednostnih nalog strategije. Način spremljanja, vrednotenja in posodabljanja je opredeljen v poglavju »Spremljanje, vrednotenje in posodabljanje strategije«.

IZHODIŠČA

V sodobni družbi je neprekinjeno delovanje informacijsko-komunikacijskih sistemov in omrežij pogoj za delovanje družbe, gospodarstva in države. Hiter tehnološki razvoj prinaša številne koristi, hkrati pa povečuje izpostavljenost novim in vse bolj dovršenim kibernetским grožnjam. Kibernetška varnost je zato postala pomemben element nacionalne varnosti, gospodarske odpornosti in zaupanja v digitalno okolje. Republika Slovenija kot članica Evropske unije in zavezništva NATO tudi v kibernetškem prostoru uveljavlja in varuje demokratične vrednote, načela pravne države ter človekove pravice in temeljne svoboščine.

Strategija temelji na nacionalnih, evropskih in zavezniških strateških ter pravnih dokumentih s področja varnosti, digitalne preobrazbe in razvoja, zlasti na ZInfV-1, direktivi NIS2, krovni strategiji digitalne preobrazbe Slovenije do leta 2030 »Digitalna Slovenija 2030«, Strategiji razvoja Slovenije 2030, strateškem konceptu NATO ter drugih relevantnih dokumentih Evropske unije in NATO. Namen strategije je določiti usmeritve za nadaljnjo krepitev nacionalnega sistema kibernetške varnosti ter razvoj varnega, odpornega in zaupanja vrednega digitalnega okolja.

Republika Slovenija pri izvajanju strategije izhaja iz ocene nacionalne slike incidentov, groženj in tveganj, pri čemer med ključne izzive sodijo izsiljevalske kibernetške aktivnosti, zlorabe identitet, izkoriščanje ranljivosti, napredne trajne grožnje (APT), tveganja v digitalnih dobavnih verigah in kampanje socialnega inženiringa.

Kibernetška varnost obsega dejavnosti, potrebne za zaščito omrežnih in informacijskih sistemov, uporabnikov takih sistemov in drugih oseb, na katere vplivajo kibernetške grožnje. Temelji na sposobnosti zaščite, varovanja in obrambe kibernetškega prostora pred grožnjami in incidenti. Strategija temelji na načelih stalne budnosti, arhitekture ničelnega zaupanja in aktivne kibernetške zaščite ter poudarja pomen vsedružbenega pristopa, sodelovanja deležnikov in pravočasne izmenjave informacij.

Pri tem se strategija opira na ZInfV-1, s katerim je bila v slovenski pravni red prenesena direktiva NIS2. Zakon določa sodoben okvir za zagotavljanje kibernetške varnosti, ki temelji na učinkovitem obvladovanju tveganj, odgovornosti organizacij, poročanju o incidentih ter krepitevi odpornosti. Strategija v tem okviru opredeljuje vizijo in strateške cilje ter usmeritve za usklajen razvoj nacionalnih zmogljivosti za uspešno odzivanje na prihodnje izzive.

Analiza izvajanja Strategije kibernetške varnosti Republike Slovenije 2016–2025

Namen tega poglavja je pregled razvoja nacionalnega sistema kibernetške varnosti od sprejema prve strategije leta 2016 ter opredelitev ključnih vrzeli in izzivov, ki jih obravnava ta strategija. Analiza vrzeli je izhodišče za oblikovanje strateških ciljev: iz ugotovljenih vrzeli izhajajo cilji, vsak cilj se uresničuje z več ukrepi, izvajanje ukrepov in doseganje ciljev pa se meri s kazalniki uspešnosti. S tem strategija vzpostavlja sklenjen krog načrtovanja, izvajanja, preverjanja in ukrepanja.

Doseženo v obdobju 2016–2025

- Republika Slovenija je vzpostavila temeljne institucije in zmogljivosti nacionalnega sistema kibernetške varnosti, med njimi pristojni nacionalni organ za informacijsko varnost (URSIV) in skupini za odzivanje na incidente na področju računalniške varnosti oziroma skupini CSIRT (SI-CERT, ki je bil ustanovljen že leta 1995, in SIGOV-CERT).
- S sprejetjem ZInfV-1 je bil vzpostavljen prenovljen zakonodajni okvir, ki v pravni red prenaša direktivo NIS2 in razširja krog zavezancev ter zahteve za obvladovanje tveganj.

- Okrepilo se je nacionalno in mednarodno sodelovanje, vključno s sodelovanjem v mreži CSIRT in mreži EU-CyCLONe, sodelovanjem z agencijo ENISA ter udeležbo na mednarodnih vajah kibernetске obrambe.
- Povečale so se zmogljivosti za zaznavanje incidentov in odzivanje nanje; vzpostavljeno je bilo varno virtualno okolje za analizo zlonamerne kode in digitalno forenziko ter nacionalno vozlišče platforme za izmenjavo informacij o grožnjah (MISP).
- Vzpostavljeni so bili programi ozaveščanja z nacionalnim dosegom (Varni na internetu, Varni v pisarni, Točka osveščanja o varni rabi interneta), zagotovljena pa je bila tudi redna letna udeležba v evropskem mesecu kibernetске varnosti.
- Vzpostavljen je bil Nacionalni koordinacijski center za kibernetско varnost (NCC-SI), ki predstavlja osrednjo povezovalno točko za krepitev nacionalnega kibernetскоvarnostnega ekosistema in povezovanje z evropsko mrežo nacionalnih koordinacijskih centrov.
- Vzpostavljena je bila usklajena obravnava ranljivosti (CVD), uvedena pa sta bila tudi redno izdajanje javnih opozoril in ciljano obveščanje skrbnikov ranljivih sistemov.

Ključni izzivi in nadaljnje razvojne potrebe

Kljub doseženemu napredku analiza kaže naslednje ključne izzive in razvojne potrebe, ki so podlaga za nadaljnje izvajanje strateških ciljev in ukrepov te strategije:

- Splošna družbena ozaveščenost o kibernetски varnosti ostaja neenakomerna, programi ozaveščanja pa zahtevajo nadaljnjo kadrovsko in finančno krepitev.
- Kadrovske zmogljivosti skupin CSIRT in pristojnih državnih organov zahtevajo nadaljnjo krepitev glede na rast groženj in nove zakonske obveznosti.
- Mehanizmi za usklajeno odzivanje na obsežne incidente in krize ter za vključevanje zunanjih strokovnjakov zahtevajo nadaljnjo krepitev in sistematično preizkušanje.
- Izmenjava informacij med javnim in zasebnim sektorjem, zlasti z varnostno-operativnimi centri, zahteva nadaljnjo formalizacijo in vzpostavitev merljivega načina sodelovanja.
- Spremljanje sistemskih tveganj, sektorskih odvisnosti in tveganj digitalnih dobavnih verig zahteva nadaljnji razvoj in sistematično izvajanje.
- Kibernetская zrelost javne uprave ostaja neenakomerna, zlasti zaradi zastarelih sistemov, razdrobljenih varnostnih rešitev in podedovane zasnove omrežij.
- Podporo mikro, malim in srednjim podjetjem pri obvladovanju kibernetских tveganj je treba še naprej sistematično razvijati in širiti.
- Vloge in postopki sodelovanja med organi pregona, državnim tožilstvom in skupinami CSIRT pri incidentih z znaki kaznivega dejanja zahtevajo nadaljnje poenotenje in formalizacijo.
- Razvoj umetne inteligence in zaostrene geopolitične razmere zahtevajo nadgradnjo pristopa in višjo stopnjo nacionalne odpornosti.

Na podlagi navedenih vrzeli strategija nadgrajuje doseženo raven razvoja in določa usmeritve za nadaljnjo krepitev zmogljivosti, kibernetске odpornosti in boja proti kibernetickemu kriminalu. Podrobna kvantitativna ocena izhodiščnega stanja po posameznih kazalnikih se pripravi ob sprejetju akcijskega načrta, pri čemer se za vsak kazalnik določijo izhodiščna in ciljna vrednost, vir podatkov ter obdobje njihovega zajema.

VIZIJA, PREDNOSTNI NALOGI IN CILJI

Vizija Strategije kibernetске varnosti Republike Slovenije 2027–2035 je odporen, varen in zaupanja vreden kibernetски prostor, ki omogoča nemoteno delovanje države, gospodarstva in družbe ter učinkovito obvladovanje sodobnih kibernetских groženj. Strategija krepi sposobnost države za pravočasno zaznavanje groženj, učinkovito odzivanje na incidente, hitro okrevanje in dolgoročno odpornost kibernetского prostora.

Uresničevanje vizije temelji na **dveh prednostnih nalogah**:

- krepitevi splošne družbene ozaveščenosti o kibernetски varnosti in
- krepitevi pripravljenosti za odzivanje na incidente, vključno s sodelovanjem med javnim in zasebnim sektorjem.

Prednostni nalogi odgovarjata na dve ugotovljeni vrzeli: neenakomerno znanje in varnostno ravnanje uporabnikov ter nezadostno preverjeno pripravljenost za usklajen odziv in obnovo ključnih storitev. Ozaveščanje zmanjšuje verjetnost in posledice zlorab, pripravljenost pa omejuje trajanje motenj, kadar preventiva ne zadošča.

V prvem triletnem obdobju imajo prednost zagotovitev ključnih kadrovskih zmogljivosti, preizkus medresorskega kriznega odzivanja in obnove najpomembnejših storitev, osnovna varnostna higiena ciljnih skupin ter začetek izvedbe prednostnih postkvantnih ukrepov. Zaporedje ukrepov se določi glede na ogroženost, pomen storitev, medsebojne odvisnosti in razpoložljive vire; zakonsko določenih obveznosti in rokov ni mogoče odložiti z razvrščanjem strateških prednosti.

Strategija določa **štiri strateške cilje**, katerih uresničevanje usmerjajo strateške usmeritve. Te se podrobneje razčlenijo v akcijskem načrtu. Strateški cilji so:

- krepitev nacionalnega sistema kibernetске varnosti,
- krepitev odpornosti družbe v kibernetском prostoru,
- krepitev boja proti kibernetскому kriminalu,
- krepitev tehnološke odpornosti in obvladovanje prihodnjih tehnologij.

OKVIR UPRAVLJANJA IN ODGOVORNOSTI

Republika Slovenija zagotavlja visoko raven kibernetске varnosti s celovitim, usklajenim in vsedružbenim pristopom, ki temelji na jasni razdelitvi vlog, odgovornosti in pristojnosti vseh deležnikov nacionalnega sistema kibernetске varnosti. Namen tega poglavja je pregledno predstaviti razmejitev njihovih vlog, pristojnosti in odgovornosti ter način njihovega medsebojnega povezovanja in sodelovanja.

Nosilci nalog v nacionalnem sistemu kibernetске varnosti

- URSIV kot pristojni nacionalni organ usklajuje nacionalni sistem kibernetске varnosti, zagotavlja podporo zavezancem, izvaja nadzor, spremlja izvajanje strategije in zastopa Republiko Slovenijo v organih Evropske unije. Opravlja tudi naloge enotne kontaktne točke, organa za obvladovanje kibernetских kriz, nacionalnega certifikacijskega organa za kibernetскую varnost, Nacionalnega koordinacijskega centra za kibernetскую varnost (NCC-SI) in Nacionalnega kibernetского vozlišča. V

vlogi NCC-SI povezuje gospodarstvo, akademsko in raziskovalno skupnost ter javni sektor, pri tem pa podpira razvoj kompetenc, raziskav in inovacij.

- Skupini CSIRT (SI-CERT in SIGOV-CERT) zagotavljata zaznavanje, obravnavo in analizo incidentov, obravnavo ranljivosti, izmenjavo informacij o grožnjah ter tehnično podporo zavezancem in uporabnikom.
- Svet za nacionalno varnost (SNAV) skrbi za usklajevanje mnenj in ukrepov pristojnih državnih organov ter s svetovanjem vladi in ocenjevanjem varnostnih tveganj prispeva k preprečevanju, da bi kibernetiske grožnje ogrozile nacionalno varnost.
- Policija odkriva in preiskuje kazniva dejanja s področja kibernetiskega kriminala, državno tožilstvo pa usmerja predkazenski postopek in izvaja kazenski pregon. Pristojni organi sodelujejo tudi s tujimi organi v okviru svojih zakonskih pristojnosti.
- Ministrstvo za obrambo in pristojne obveščevalno-varnostne službe prispevajo k spremljanju hibridnih in naprednih groženj ter kibernetiski obrambi v okviru svojih pristojnosti.
- Pristojni sektorski in regulatorni organi izvajajo naloge po področnih predpisih, Informacijski pooblaščenec neodvisno nadzira varstvo osebnih podatkov; odgovornost za zakonito obdelavo nosijo upravljavci in obdelovalci.
- Zavezanci po ZInfV-1, kritični subjekti po zakonu, ki ureja področje kritične infrastrukture, varnostno-operativni centri, gospodarstvo, raziskovalne organizacije in civilna družba izvajajo lastne ukrepe in sodelujejo v mehanizmi izmenjave informacij.

Strateške usmeritve

- Zagotavljati jasno opredeljene vloge, odgovornosti in pristojnosti vseh deležnikov nacionalnega sistema kibernetiske varnosti.
- Zagotavljati usklajeno delovanje pristojnega nacionalnega organa, skupin CSIRT, regulatorjev, organov odkrivanja in pregona, predstavnikov obrambnega sistema ter drugih pristojnih institucij.
- Krepiti sodelovanje med javnim in zasebnim sektorjem pri preprečevanju, odkrivanju in obravnavi kibernetiskih groženj.
- Krepiti vključevanje akademske sfere, raziskovalnih organizacij in gospodarstva v razvoj nacionalnih kibernetiskih zmogljivosti.
- Krepiti nacionalno kibernetiskovarnostno skupnost in spodbujati povezovanje gospodarstva, raziskovalnih in akademskih institucij, javnega sektorja ter drugih relevantnih deležnikov pri razvoju nacionalnih kibernetiskovarnostnih zmogljivosti, kompetenc in inovacij.
- Spodbujati pravočasno in zaupanja vredno izmenjavo informacij med deležniki.
- Zagotavljati učinkovito usklajevanje s področjem kritične infrastrukture in s področjem odzivanja na hibridne grožnje.
- Zagotavljati povezovanje nacionalnega sistema kibernetiske varnosti z mehanizmi Evropske unije in NATO ter z drugimi mednarodnimi partnerji.

Usklajevanje na operativni in strateški ravni poteka prek medresorskih koordinacijskih teles in strokovnih mehanizmov sodelovanja, ki jih vodi URSIV ali v katerih sodeluje kot pristojni nacionalni organ za informacijsko varnost. Sodelovanje z osrednjim organom za odzivanje na hibridne grožnje vključuje izmenjavo ocen tveganj, opozoril in informacij o incidentih, ki lahko nakazujejo hibridno delovanje, ter usklajevanje odziva in vaj v okviru zakonskih pristojnosti.

Za izvajanje posameznega ukrepa odgovarja njegov vodilni nosilec. URSIV usklajuje izvajanje strategije in spremlja skupni napredek. Akcijski načrt razmeji upravljanje in izvajanje storitev informacijske in komunikacijske tehnologije (IKT), zagotavljanje informacijske varnosti, odzivanje na incidente ter neodvisno izvajanje nadzornih nalog. Nova koordinacijska telesa in zmogljivosti se načrtujejo na podlagi pregleda obstoječih nalog, da se prepreči njihovo podvajanje. Pristojni organi za kibernetisko varnost in odpornost kritičnih subjektov vzpostavijo usklajeno izmenjavo ocen tveganj in podatkov o incidentih ter sodelovanje pri vajah in nadzoru v okviru svojih zakonskih pristojnosti.

URSIV vodi usklajevanje nacionalnega sistema ter področij pripravljenosti za odzivanje in obvladovanja kibernetских tveganj. Za odpornost storitev odgovarjajo njihovi upravljavci ob sodelovanju pristojnih resorjev in regulatorjev. Organi, pristojni za izobraževanje, visoko šolstvo, znanost in gospodarstvo, v sodelovanju z URSIV vodijo vsebine svojih področij. Področje kibernetiskega kriminala vodita Policija in državno tožilstvo v okviru svojih pristojnosti; pri prihodnjih tehnologijah URSIV usklajuje kibernetiskovarnostni vidik, pristojni resorji in regulatorji pa izvajajo svoje naloge. Ta razdelitev ne spreminja zakonskih pristojnosti ali neodvisnosti posameznih organov.

Ob neusklajenostih, zamudah ali nezagotovljenih virih vodilni nosilec URSIV predloži obrazložitev, oceno posledic in predlog rešitve. URSIV uskladi predlog korektivnih ukrepov, nerešena vprašanja iz pristojnosti vlade pa predloži Vladi Republike Slovenije v odločitev. Spremembe rokov, obsega ukrepov ali virov se zabeležijo v akcijskem načrtu in letnem poročilu; zakonske obveznosti ostanejo zavezujoče.

NAČRT ZA KREPITEV SPLOŠNE DRUŽBENE OZAVEŠČENOSTI O KIBERNETSKI VARNOSTI

Kibernetška varnost je skupna odgovornost države, gospodarstva in posameznikov. Republika Slovenija bo zato sistematično krepila znanje ter spodbujala ravnanje, ki prebivalcem in organizacijam pomaga prepoznati kibernetška tveganja, preprečevati incidente in se nanje ustrezno odzivati.

Ozaveščanje bo prilagojeno različnim ciljnim skupinam in novim izzivom, tveganjem in grožnjam, vključno z zlorabami umetne inteligence in globokimi ponaredki. Vsebine kibernetške varnosti se bodo vključevale v vzgojno-izobraževalni sistem, vseživljenjsko učenje in usposabljanje javnih uslužbencev ter funkcionarjev.

Strateške usmeritve

- Zagotoviti usklajeno načrtovanje in izvajanje nacionalnih programov ozaveščanja ter zanje določiti odgovornosti in potrebne kadrovske ter finančne vire.
- Pripravljati razumljive in praktično uporabne vsebine za različne ciljne skupine ter jih prilagajati spremembam groženj in načinom uporabe digitalnih storitev.
- Vključevati vsebine kibernetške varnosti in varnega ravnanja v nacionalne vzgojno-izobraževalne programe ter vseživljenjsko učenje.
- Zagotavljati sistematično in redno usposabljanje o kibernetški varnosti za javne uslužbence in funkcionarje ter krepiti strokovne kompetence v državni upravi.
- Določiti nacionalne prednostne naloge raziskav in razvoja, urediti odgovorno deljenje podatkov in spodbujati vključevanje širšega kroga strokovnjakov v dejavnosti na področju kibernetške varnosti.
- Usposabljati vodstva in funkcionarje za odločanje o kibernetških tveganjih, zagotavljanju potrebnih virov in vodenju organizacij ob incidentih.
- Spremljati učinkovitost programov glede na spremembe v znanju in ravnanju ciljnih skupin ter ugotovitve uporabljati pri njihovem nadaljnjem načrtovanju.

Na področju ozaveščanja o kibernetški varnosti bo Republika Slovenija sistematično spremljala in vrednotila dobre prakse, izkušnje in spoznanja drugih držav ter mednarodnih organizacij. Posebna pozornost bo namenjena pristopom, ki so se izkazali za učinkovite pri spreminjanju vedenja uporabnikov, krepitvi kibernetške higiene in prilagajanju vsebin posameznim ciljnim skupinam.

Uspešnost ozaveščanja se meri tudi s spremembami znanja in ravnanja ciljnih skupin, ne le s številom izvedenih dejavnosti ali udeležencev. Programi se prilagodijo otrokom, starejšim, osebam z invalidnostmi in drugim digitalno ranljivim skupinam. Usposabljanje vodstev vključuje odločanje o tveganjih, zagotavljanje virov in vodenje organizacije ob incidentu.

KREPITEV MEHANIZMOV ZA ODZIVANJE NA INCIDENTE, VKLJUČNO S SODELOVANJEM MED JAVNIM IN ZASEBNIM SEKTORJEM

Republika Slovenija bo krepila pripravljenost za odzivanje na incidente in okrevanje po njih z razvojem nacionalnih zmogljivosti, standardiziranih postopkov ter sodelovanjem javnega in zasebnega sektorja. Obstoječi sistem prigrisatve incidentov pristojnima skupinama CSIRT se bo razvijal z uporabo in nadgradnjo skupne nacionalne platforme za prigrislanje incidentov, ki bo omogočala pravočasno posredovanje in izmenjavo informacij med pristojnimi organi, skupinami CSIRT, varnostno-operativnimi centri in drugimi deležniki. Platforma podpira obstoječe zakonske postopke in roke; določi se, kateri podatki se posredujejo posameznim prejemnikom, ob katerih pogojih in s kakšnimi pravicami dostopa.

Nacionalne zmogljivosti se bodo razvijale na področjih kriznega upravljanja, digitalne forenzike, analize zlonamerne kode, izmenjave informacij o grožnjah, obravnave ranljivosti in razvoja kadrov ter se bodo redno preizkušale na nacionalnih in mednarodnih vajah. Za učinkovito okrevanje bodo pripravljeni in preizkušani nacionalni načrti odzivanja na incidente in kibernetike krize, smernice in načrti neprekinjenega poslovanja. Pri obvladovanju incidentov velikih razsežnosti, kriz in incidentov s čezmejnimi učinki bo Republika Slovenija sodelovala s posameznimi partnerskimi državami ali mednarodnimi organizacijami, predvsem z EU in NATO, in po potrebi uporabila njihove in druge mehanizme mednarodne pomoči.

Načrtovanje novih zmogljivosti mora izhajati iz dokazljive vrzeli. Nacionalna kibernetika rezerva naslavlja potrebo po dodatnih strokovnjakih ob povečanem obsegu incidentov. Predlog nacionalnega vozlišča za digitalno forenziko naslavlja usklajevanje strokovne podpore in varne obravnave digitalnih dokazov, predlog situacijskega centra pa skupno spremljanje razmer. Pred vzpostavitvijo se opredelijo nosilec, pravna podlaga, stroški in razmerja do Nacionalnega kibernetikega vozlišča, skupin CSIRT ter obstoječih policijskih in obrambnih zmogljivosti. Tehnična obravnava incidenta in kazenskoprosesno zavarovanje dokazov morata ostati jasno razmejena.

Strateške usmeritve

- V nacionalnem načrtu odzivanja opredeliti merila za stopnjevanje odziva, aktivacijo dodatnih zmogljivosti in mednarodne pomoči ter razmejitev tehničnega, operativnega in strateškega odločanja.
- Vzpostaviti nacionalno vozlišče za digitalno forenziko in usklajen protokol za obravnavo incidentov z znaki kaznivega dejanja ob sodelovanju skupin CSIRT, Policije in državnega tožilstva.
- Vzpostaviti in ohranjati učinkovit nacionalni sistem odzivanja na incidente, incidente velikih razsežnosti in krize na podlagi načrta, ki se redno preizkuša in prilagaja glede na pridobljena spoznanja, da se zagotovi učinkovitost postopkov.
- Okrepiti kadrovske in strokovne zmogljivosti nacionalnih skupin CSIRT ter vzpostaviti nacionalno kibernetiko rezervo za aktivacijo dodatnih strokovnjakov za posamezne zahtevne incidente.
- Krepiti izmenjavo informacij in sodelovanje med skupinami CSIRT in varnostno-operativnimi centri ter razviti nacionalni okvir za koordinirano razkrivanje ranljivosti.
- Zagotoviti pripravo, usklajevanje in redno preizkušanje postopkov odzivanja ter načrtov neprekinjenega poslovanja in okrevanja po informacijskih incidentih oziroma dogodkih ter redno izvajanje vaj.
- Okrepiti nacionalni sistem za zagotavljanje kibernetike obrambe, v katerega so lahko poleg subjektov javne uprave vključeni tudi subjekti iz gospodarstva, raziskovalno-razvojne organizacije, znanstvene institucije, interesna združenja in posamezniki.

- Pred aktivacijo dodatnih strokovnjakov v okviru nacionalne kibernetске rezerve oziroma njihove vključitve v nacionalni sistem kibernetске obrambe urediti pogoje vključitve, preverjanje usposobljenosti, varovanje podatkov, odgovornost in financiranje in razmerje do obstoječih zmogljivosti.

Nacionalni načrt komuniciranja ob incidentih se uskladi z načrtom odzivanja ter pripravi in vzdržuje ob sodelovanju URSIV, pristojne vladne službe za komuniciranje in drugih pristojnih deležnikov. Določi odgovornosti za obveščanje javnosti, usklajevanje sporočil in dostopne kanale ob izpadu običajnih komunikacij.

KREPITEV NACIONALNEGA SISTEMA KIBERNETSKE VARNOSTI

Krepitev nacionalnega sistema kibernetске varnosti zajema razvoj upravljavskih, organizacijskih in tehničnih zmogljivosti, procesov in mehanizmov za zgodnje zaznavanje, preprečevanje, obravnavo in omejevanje posledic kibernetских groženj ter obnovo prizadetih sistemov in storitev po incidentih. Nacionalni sistem temelji na načelih porazdeljene odgovornosti in usklajenega delovanja. Posamezni državni organi, skupine CSIRT, regulatorji, zavezanci in drugi deležniki so odgovorni za zagotavljanje kibernetске varnosti, pristojni nacionalni organ pa zagotavlja strateško koordinacijo, skupno situacijsko zavedanje, medsektorsko sodelovanje in usklajeno odzivanje na obsežne incidente ter krize. Delovanje nacionalnega sistema kibernetске varnosti temelji na učinkovitem usklajevanju, redni, varni in zaupanja vredni izmenjavi informacij med pristojnim nacionalnim organom, skupinami CSIRT, zavezanci in drugimi deležniki ter jasno določenih pristojnostih, postopkih odločanja in odgovornostih.

Želeno stanje do leta 2035: odgovornosti nacionalnih deležnikov so jasno razmejene, izmenjava informacij deluje po dogovorjenih pravilih, usklajen odziv na obsežne incidente in krize pa je redno preizkušen ter izboljšán na podlagi ugotovljenih pomanjkljivosti.

Strateške usmeritve

- Krepiti nacionalno situacijsko zavedanje ter varno in pravočasno izmenjavo informacij o grožnjah, ranljivostih in incidentih, vključno s sektorskimi mehanizmi izmenjave, ob upoštevanju načela najmanjšega potrebnega razkritja podatkov.
- Spodbujati in podpirati prostovoljno izmenjavo uporabnih informacij o kibernetски varnosti med subjekti, vključno z izkušnjami in pridobljenimi spoznanji, z uporabo standardiziranih postopkov, varnih komunikacijskih poti in ustreznih tehničnih orodij.
- Krepiti delovanje in zmogljivosti Nacionalnega kibernetского vozlišča kot povezovalne točke za izmenjavo informacij, analitično podporo, zgodnje opozarjanje ter koordinacijo med nacionalnimi, sektorskimi, regulatornimi in evropskimi strukturami.
- Spodbujati preventivne dejavnosti in ukrepe kibernetске zaštite za prebivalstvo, gospodarstvo in javni sektor z namenom krepitev varnega ravnanja ter odpornosti omrežnih in informacijskih sistemov, organizacijskih procesov in storitev, pomembnih za delovanje družbe, gospodarstva in države.
- Krepiti preventivno odkrivanje ranljivosti, upravljanje izpostavljenosti, spremljanje groženj ter zaščito ključnih informacijskih sistemov, spletnih storitev in portalov.

- Preventivno odkrivanje in usklajeno razkrivanje ranljivosti se izvajata po vnaprej določenih pravilih glede pooblastil, obsega preverjanja, zaupnosti podatkov in rokov obveščanja. Spodbujajo se raziskave v dobri veri ter jasni dogovori med raziskovalci, upravljavci in pristojnimi skupinami CSIRT ob spoštovanju veljavne zakonodaje in preprečevanju škode.
- Vzpostaviti situacijski center kibernetске obrambe za zaznavanje in spremljanje kibernetских groženj ter izvajanje postopkov za omejitev njihovih posledic.
- Razvijati in vzdrževati nacionalno karto sistemskih tveganj in jo povezati s presojo ključnih dobaviteljev ter z vključevanjem in natančno opredelitvijo kibernetskovarnostnih zahtev pri javnem naročanju proizvodov in storitev IKT, vključno s certificiranjem za kibernetско varnost, ustreznim šifriranjem in uporabo odprtokodnih proizvodov za kibernetско varnost.
- Krepi obrambo in odpornost informacijskega prostora.

KREPITEV ODPORNOSTI DRUŽBE V KIBERNETSKEM PROSTORU

Kibernetska odpornost pomeni sposobnost prebivalstva, sistemov in organizacij, da prepoznajo in predvidijo grožnje, prenesejo motnje, ohranijo ključne funkcije, pravočasno obnovijo delovanje, upoštevajo pridobljene izkušnje in spoznanja ter se prilagodijo novim tveganjem. Posebna pozornost je namenjena javnim storitvam, pomembnim za prebivalstvo, zlasti socialni varnosti, zdravstvu in drugim ključnim storitvam, pri katerih so načrti neprekinjenega poslovanja in okrevanja po incidentih sestavni del obvladovanja tveganj.

Želeno stanje do leta 2035: upravljavci prednostnih storitev dokazljivo ohranjajo ključne funkcije oziroma obnovijo delovanje v določenem sprejemljivem času. Prebivalci in podjetja bolje obvladujejo osnovne varnostne prakse, prednostne infrastrukturne in dobavne odvisnosti pa se sistematično obravnavajo.

Zaščita ključnih digitalnih infrastruktur in javnega jedra interneta

Ključne digitalne infrastrukture in javno jedro interneta predstavljajo temelj za delovanje digitalne družbe, gospodarstva in javnega sektorja. Zaradi medsebojne povezanosti in odvisnosti storitev lahko motnje v teh sistemih povzročijo takojšnje kaskadne učinke na vse sektorje, zato Republika Slovenija njihovo zaščito obravnava kot prednostno nalogo v okviru krepitve odpornosti družbe.

Strateške usmeritve

- Krepiti odpornost ključnih digitalnih infrastruktur, osnovnih internetnih storitev in osrednjega komunikacijskega omrežja državne uprave.
- Krepiti odpornost in posodabljanje arhitekturo omrežja HKOM z ustrezno segmentacijo, centraliziranim upravljanjem zaščitnih mehanizmov in večjo odpornostjo proti kibernetiskim grožnjam.
- Krepiti odpornost sistemov DNS, usmerjanja, nacionalne vrhnje domene in drugih temeljnih internetnih storitev.
- Pri zaščiti javnega jedra odprtega interneta se upoštevajo tudi odvisnosti od čezmejnih povezav, zlasti raznolikost povezav, rezervne poti ter sodelovanje z upravljavci in partnerskimi državami.
- Spremljati tveganja v digitalnih dobavnih verigah ter izboljševati situacijsko zavedanje o sistemskih tveganjih in odvisnostih.
- Zagotoviti pravočasen, usklajen in obvladovan prehod javne uprave, kritične infrastrukture in zavezanecv po ZInfV-1 na kvantno odporno kriptografijo ob vzpostavitvi trajne kriptografske agilnosti.
- Spodbujati sodelovanje med upravljavci ključnih digitalnih infrastruktur ter upoštevati evropske in mednarodne dobre prakse.

Posebna pozornost se nameni varnosti operativnih tehnologij in industrijskih krmilnih sistemov, vključno z ločevanjem omrežij, nadzorom oddaljenih dostopov in varnim vzdrževanjem ob upoštevanju neprekinjenosti in fizične varnosti procesov. Za ključne storitve se določijo sprejemljivi časi obnove in dopustna izguba podatkov, redno se preizkuša obnova iz zaščitene varnostnih kopij in načrtuje minimalno delovanje ob daljšem izpadu električne energije, komunikacij ali skupnih digitalnih storitev.

Digitalna identiteta in zaupanje v digitalne storitve

Varna digitalna identiteta in zaupanje v digitalne storitve sta temelj digitalne družbe, gospodarstva in elektronskega poslovanja. Ker so zlorabe identitet med pogostimi kibernetскими incidenti, bo Republika Slovenija krepila odpornost identitetnih sistemov ter zagotavljala izvajanje evropskega in nacionalnega okvira za elektronsko identifikacijo in storitve zaupanja, vključno z uredbo eIDAS (angl. *electronic identification, authentication and trust services* – elektronska identifikacija, avtentikacija in storitve zaupanja) ter evropskim okvirom za digitalno identiteto, ki vključuje evropsko denarnico za digitalno identiteto.

Strateške usmeritve

- Spodbujati uporabo varne elektronske identifikacije, avtentikacije in večfaktorske avtentikacije v javnem in zasebnem sektorju ter med prebivalci.
- Krepiti odpornost sistemov digitalne identitete in storitev zaupanja, vključno z neprekinjenim poslovanjem ter zaščito pred zlorabami in tveganji umetne inteligence.
- Izvajati evropske in nacionalne pobude na področju digitalne identitete, zlasti uvedbo evropske denarnice za digitalno identiteto.
- Povečevati zaupanje uporabnikov v digitalne javne storitve z enotnim upravljavskim okvirom varnostnih zahtev za digitalne storitve v javni upravi.

Kibernetaska odpornost proizvodov in storitev z digitalnimi elementi

To podpoglavje obravnava potrebo po sistematični krepitvi kibernetiske odpornosti proizvodov in storitev z digitalnimi elementi, ki se uporabljajo v gospodarstvu, javnem sektorju in vsakdanjem življenju. S tem dopolnjuje ukrepe za ocenjevanje zrelosti, izvajanje vaj ter varnostne presoje in certificiranje. Izhodišče je Akt o kibernetiski odpornosti, ki določa horizontalne kibernetiskovarnostne zahteve za proizvode z digitalnimi elementi na trgu Evropske unije.

Akt o kibernetiski odpornosti ureja proizvode z digitalnimi elementi v okviru svojega področja uporabe; njegove zahteve se ne razširjajo samodejno na vse digitalne storitve. Certificiranje po Aktu o kibernetiski varnosti in ugotavljanje skladnosti po Aktu o kibernetiski odpornosti se obravnavata ločeno. Pri izvajanju se upošteva postopna uporaba Uredbe (EU) 2024/2847: določbe o priglasitvi organov za ugotavljanje skladnosti od 11. junija 2026, obveznosti poročanja iz 14. člena od 11. septembra 2026 in splošna uporaba od 11. decembra 2027.

Strateške usmeritve

- Spodbujati načelo varnosti že v zasnovi in privzete varnosti pri razvoju, nabavi, uporabi in vzdrževanju proizvodov ter storitev z digitalnimi elementi.
- Krepiti odgovornost proizvajalcev, ponudnikov, uvoznikov, distributerjev in uporabnikov za kibernetisko odpornost digitalnih proizvodov in storitev.
- Spodbujati varnostne zahteve, testiranje, obvladovanje ranljivosti in varne posodobitve ter uporabo relevantnih evropskih in mednarodnih standardov, ustreznih postopkov ugotavljanja skladnosti ter po potrebi evropskih certifikacijskih shem za kibernetisko varnost.

- Krepi odpornost digitalnih dobavnih verig ter izmenjavo informacij o ranljivostih, tveganjih in incidentih med pristojnimi organi, gospodarstvom, raziskovalno skupnostjo in drugimi deležniki.
- Pri upravljanju dobavnih verig se obravnavajo tudi koncentracija pri posameznih ponudnikih, podizvajalci, storitve v oblaku in odvisnost od zunanjih upravljavcev. V nabavnih in pogodbenih zahtevah se glede na tveganje določijo varnostna podpora v celotnem življenjskem ciklu, obveščanje o ranljivostih in incidentih, preverljivost izpolnjevanja zahtev ter pogoji za prenos podatkov in zamenjavo ponudnika. Načrtuje se pravočasna zamenjava nepodprtih sistemov. Za izvajanje pravil o odpornosti proizvodov se zagotovijo jasna razmejitve pristojnosti ter usklajene zmogljivosti za nadzor trga, ugotavljanje skladnosti in podporo gospodarskim subjektom.

Odpornost gospodarstva ter mikro, malih in srednjih podjetij

Gospodarstvo, zlasti mikro, mala in srednja podjetja, ima pomembno vlogo pri krepitvi nacionalne odpornosti v kibernetnem prostoru. Republika Slovenija bo spodbujala razvoj znanj in kompetenc, uporabo ustreznih ukrepov za obvladovanje tveganj, sodelovanje med deležniki ter odpornost dobavnih verig in varno uporabo novih digitalnih tehnologij, vključno s pravočasno pripravo na prehod na postkvantno kriptografijo. Za manjša podjetja bo ta prehod izvedljiv predvsem prek ponudnikov in dobaviteljev IKT, zato bo podpora usmerjena v razumljive smernice, ozaveščanje in zahteve pri nabavi, ne v gradnjo lastnih kriptografskih zmogljivosti.

Strateške usmeritve

- Spodbujati razvoj odpornega, varnega in konkurenčnega digitalnega gospodarstva ter zagotavljati posebno podporo mikro, malim in srednjim podjetjem pri krepitvi njihove kibernetne odpornosti, razvoju kompetenc in prilagajanju novim tehnološkim in regulativnim zahtevam.
- Spodbujati partnerstva med gospodarstvom, industrijo, raziskovalnimi organizacijami in javnim sektorjem za razvoj rešitev, prenos znanja in krepitev inovacij.
- Podpirati gospodarstvo, zlasti mikro, mala in srednja podjetja, pri pripravi na prehod na postkvantno kriptografijo z ozaveščanjem o tveganju zajemanja podatkov za poznejše dešifriranje, dostopnimi smernicami in spodbujanjem zahtev po kriptografski agilnosti v odnosih z dobavitelji.
- Podpora se prilagodi velikosti, dejavnosti in tveganjem podjetij, tudi kadar niso zavezanci po ZInfV-1. Prednost imajo dostopne osnovne varnostne rešitve, pomoč pri odpravljanju ugotovljenih vrzeli ter povezovanje raziskovalnih rezultatov s praktično uporabo v gospodarstvu. NCC-SI podpira vključevanje slovenskih deležnikov v nacionalne in evropske raziskovalne, razvojne in inovacijske pobude ter spodbuja prenos, pilotiranje in uvajanje uspešnih kibernetkovarnostnih rešitev v gospodarstvu in javnem sektorju. Mikro, malim in srednjim podjetjem ter zagonskim podjetjem omogoča povezovanje z raziskovalno-razvojnimi okoljem, dostop do strokovnih kompetenc in možnosti financiranja ter vključevanje v evropski kibernetkovarnostni ekosistem.
- Podpirati akademske in raziskovalne institucije pri razvoju in izboljševanju orodij kibernetne varnosti in varne omrežne infrastrukture ter spodbujati njihovo uvajanje.

KREPITEV BOJA PROTI KIBERNETSKEMU KRIMINALU

Kibernetski kriminal predstavlja pomembno grožnjo nacionalni varnosti, ki zaradi hitrega tehnološkega razvoja, vse večje digitalizacije in izrazite čezmejne narave zahteva celovit in usklajen odziv države. Republika Slovenija bo zato krepila sodelovanje med pristojnimi državnimi organi, zasebnim sektorjem in mednarodnimi partnerji ter razvijala zmogljivosti za preprečevanje, odkrivanje in pregon kibernetskega kriminala.

Želeno stanje do leta 2035: organi odkrivanja, preiskovanja in pregona razpolagajo z ustreznimi strokovnimi zmogljivostmi in usklajenimi postopki za obravnavo digitalnih dokazov. Čezmejno sodelovanje je učinkovitejše, žrtvam pa so na voljo razumljiva navodila za prijavo, ohranitev dokazov in dostop do pomoči.

Strateške usmeritve

- Krepi sodelovanje med organi odkrivanja in pregona, državnim tožilstvom, skupinami CSIRT, regulatorji in drugimi pristojnimi deležniki pri preprečevanju, odkrivanju in pregonu kibernetskega kriminala.
- Krepi zmogljivosti za preiskovanje kibernetskega kriminala in digitalnih prevar ter za sledenje protipravno pridobljenemu digitalnemu premoženju in njegov zasег.
- Razvijati zmogljivosti za zaznavanje in obravnavo novih oblik kibernetskega kriminala ter krepiti sodelovanje z zasebnim sektorjem.
- Krepi zaščito otrok in drugih ranljivih skupin pred spletnimi zlorabami in drugimi oblikami kibernetskega kriminala.
- Krepi mednarodno sodelovanje pri preprečevanju, preiskovanju in pregonu kibernetskega kriminala.

KREPITEV TEHNOLOŠKE ODPORNOSTI IN OBVLADOVANJE PRIHODNIJH TEHNOLOGIJ

Med osrednjimi tehnološkimi prehodi, ki zaznamujejo obdobje izvajanja strategije, sta prehod na postkvantno kriptografijo in razvoj umetne inteligence. Prvi prehod zahteva zamenjavo kvantno ranljivih kriptografskih mehanizmov, zlasti za izmenjavo ključev in elektronsko podpisovanje ter ustrezno prilagoditev zaščite podatkov. Umetna inteligenca se lahko uporablja za izvajanje zlonamernih kibernetских aktivnosti za obrambo pred njimi, hkrati pa ustvarja nove ranljivosti in tveganja. Oba prehoda presegata posamezno organizacijo in zahtevata usklajeno obravnavo, zato ju strategija obravnava kot samostojen strateški cilj. Strategija bo obenem sistematično spremljala razvoj drugih nastajajočih tehnologij ter pravočasno ocenjevala njihove učinke na nacionalno kibernetično varnost in odpornost.

Želeno stanje do leta 2035: prednostni sistemi so prešli na postkvantno odporno zaščito skladno z razvrstitvijo tveganj in evropskimi časovnimi mejniki. Pri varnostno pomembni uporabi umetne inteligence so tveganja preverljivo obvladovana skozi celoten življenjski cikel, z določenim človeškim nadzorom in varnimi nadomestnimi postopki.

Prehod na postkvantno kriptografijo

Razvoj kvantnega računalništva zahteva pravočasen prehod na postkvantno kriptografijo, zlasti za zaščito podatkov, za katere je treba zaupnost zagotavljati dolgo obdobje. Strategija določa usmeritve za ta prehod v skladu z evropskim časovnim okvirom do leta 2035.

Strateške usmeritve

- Zagotoviti pravočasen in usklajen prehod na postkvantno kriptografijo.
- Opredeliti prednostne sisteme, podatke in storitve, pri katerih je potrebna postkvantno odporna zaščita.
- Spodbujati kriptografsko agilnost pri razvoju, posodabljanju in nabavi informacijskih sistemov.
- Razvijati nacionalne strokovne zmogljivosti na področju kriptografije.
- Slediti evropskim in mednarodnim usmeritvam ter časovnim mejnikom na področju postkvantne kriptografije.

Nacionalni načrt prehoda vključuje popis kriptografskih sredstev in odvisnosti, razvrstitev sistemov po tveganju, zahteve za dobavitelje ter preizkušanje združljivosti in obnove delovanja. Pri časovnem načrtovanju se upošteva evropski časovni načrt, po katerem države članice do konca leta 2026 pripravijo nacionalne načrte in začnejo prehod, do konca leta 2030 zaključijo prehod v kritični infrastrukturi in pri drugih primerih uporabe z visokim tveganjem, do konca leta 2035 pa prehod vseh preostalih sistemov v čim večji meri. Poleg zaupnosti podatkov se obravnavajo elektronski podpisi, digitalna potrdila in dolgoročno preverjanje pristnosti. Gre za usmeritve evropskega časovnega načrta, ne za enoten zakonski rok za vse sisteme. Nacionalni načrt določi konkretne mejnike po tveganjih, odgovorne nosilce, vire, spremljanje napredka in obravnavo utemeljenih odstopanj. Priprava načrta in začetek prehoda v letu 2026 potekata neodvisno od sprejetja strategije za obdobje 2027–2035.

Varna in suverena raba umetne inteligence

Umetna inteligenca predstavlja pomembno priložnost za krepitev kibernetске varnosti, hkrati pa prinaša nova tveganja. Republika Slovenija bo spodbujala njeno varno, odgovorno in suvereno uporabo ter krepila zmogljivosti za obvladovanje povezanih tveganj.

Suverenost pri uporabi umetne inteligence pomeni predvsem zmožnost nadzora nad podatki, dostopi, ponudniki in delovanjem sistemov ter obvladovanje odvisnosti in možnost zamenjave rešitve. Kibernetскоvarnostne zahteve se izvajajo usklajeno s pristojnimi organi za umetno inteligenco in veljavnimi predpisi; kibernetска strategija sama ne določa novih pristojnosti za splošni nadzor sistemov umetne inteligence.

Strateške usmeritve

- Vzpostaviti upravljanje uporabe umetne inteligence v državnih sistemih.
- Zagotoviti varno, odgovorno in sledljivo uporabo umetne inteligence.
- Pred uvedbo oceniti varnostna tveganja sistemov umetne inteligence.
- Spodbujati uporabo umetne inteligence za krepitev kibernetске varnosti.
- Krepiti tehnološko odpornost ter znanja in kompetence za varno uporabo umetne inteligence.

Upravljanje tveganj umetne inteligence zajema celoten življenjski cikel sistemov, varovanje učnih in vhodnih podatkov, preverjanje ponudnikov in modelov ter preprečevanje razkrivanja varovanih podatkov in zlorab povezanih orodij. Za uporabo pri varnostno pomembnih odločitvah se določijo človeški nadzor, beleženje odločitev, omejitve pooblastil in možnost varne ustavitve oziroma prehoda na nadomestne postopke. Učinkovitost rešitev se preverja tudi ob zavajajočih ali zlonamernih vhodnih podatkih.

MEDNARODNO SODELOVANJE IN MEDSEBOJNA POMOČ

Prečna vsebina, ki podpira uresničevanje vseh prednostnih nalog in strateških ciljev

Republika Slovenija krepi svojo kibernetiko varnost tudi z dejavnim sodelovanjem v Evropski uniji in zavezništvu NATO ter drugih mednarodnih in regionalnih okvirih. Pri tem sodeluje pri oblikovanju politik, pravil in skupnih odzivov, izmenjuje informacije in strokovno znanje ter razvija zmogljivosti za čezmejno sodelovanje ob pomembnih incidentih in krizah. Mednarodno sodelovanje tako prispeva k nacionalni odpornosti in k varnosti širšega okolja, katerega del je tudi Slovenija.

Strateške usmeritve

- Dejavno sodelovati pri oblikovanju evropskih in mednarodnih politik, pravil, standardov in ukrepov na področju kibernetike varnosti ter pri njihovem izvajanju.
- Krepi vključevanje Republike Slovenije v evropski kibernetikovarnostni kompetenčni ekosistem Evropskega kompetenčnega centra za kibernetiko varnost (ECCC) in evropske mreže nacionalnih koordinacijskih centrov ter spodbujati vključevanje slovenskih deležnikov v evropske pobude, partnerstva in projekte.
- Izpolnjevati zaveze v okviru Evropske unije in zavezništva ter prispevati k skupni kibernetiki odpornosti.
- Krepi bilateralno in multilateralno sodelovanje med pristojnimi organi, vključno z varno in pravočasno izmenjavo informacij ter strokovnega znanja.
- Vzpostaviti in redno preizkušati postopke za zaprošanje za mednarodno pomoč, njeno sprejemanje in zagotavljanje mednarodne pomoči ob pomembnih incidentih in krizah.
- Zagovarjati odgovorno ravnanje držav v kibernetičnem prostoru.
- Podpirati usklajene mednarodne odzive na zlonamerne kibernetike dejavnosti in prizadevanja proti širjenju ter neodgovorni uporabi komercialnih orodij za vdore.

KIBERNETSKA VARNOST, ZASEBNOST IN ČLOVEKOVE PRAVICE

Kibernetika varnost se zagotavlja ob spoštovanju človekovih pravic in temeljnih svoboščin, zasebnosti, varstva osebnih podatkov in zaupnosti komunikacij. Vsi ukrepi se izvajajo na jasni pravni podlagi ter ob ustreznih varovalkah za zaščito pravic posameznikov in posameznih družbenih skupin. Zahteve in obveznosti glede kibernetike varnosti morajo biti zato sorazmerne, namenske, utemeljene na tveganjih ali vplivu grožnje na družbo ter prilagojene posebnostim posameznih družbenih skupin.

Strateške usmeritve

- Zagotavljati zakonito, sorazmerno in odgovorno izvajanje dejavnosti na področju kibernetike varnosti.
- Pri načrtovanju in izvajanju ukrepov zagotavljati spoštovanje človekovih pravic in temeljnih svoboščin; morebitne omejitve morajo imeti pravno podlago, biti nujno sorazmerne ter podvržene ustreznemu nadzoru in pravnemu varstvu.
- Krepiti zaupanje prebivalcev in organizacij v digitalno okolje ter digitalne storitve.
- Upoštevati načela varstva osebnih podatkov in zasebnosti pri načrtovanju in izvajanju kibernetikovarnostnih ukrepov.
- Spoštovati zasebnost posameznika v kibernetickem prostoru ter ozaveščati o njenem pomenu in spodbujati njeno varovanje z ustrezno kibernetiko higieno.
- Zagotavljati preglednost in sledljivost odločitev pri uporabi naprednih tehnologij in umetne inteligence.
- Razvijati zmogljivosti za varno uporabo novih tehnologij ob spoštovanju temeljnih pravic.

MEHANIZEM ZA OPREDELITEV USTREZNIH VIROV IN OCENO TVEGANJ

Učinkovita zaščita digitalne infrastrukture in nemoteno delovanje ključnih storitev zahtevata sistematično opredelitev virov in oceno tveganj. Republika Slovenija bo vzpostavila mehanizem za pripravo ocene ogroženosti. Ocena bo temeljila na oceni tveganj, mehanizem pa bo omogočil opredelitev ustreznih virov. Mehanizem bo omogočil bolj učinkovito upravljanje kibernetских groženj na nacionalni ravni.

Mehanizem bo omogočal prednostno razvrščanje ukrepov glede na stopnjo ogroženosti, pomen storitev za delovanje države in gospodarstva ter razpoložljive kadrovske, tehnične in finančne vire. Tako se bodo omejeni viri usmerjali predvsem v zaščito najpomembnejših sistemov, storitev, sektorjev in nacionalnih odvisnosti.

Zagotavljanje virov za izvajanje strategije

Za izvajanje strategije je treba zagotoviti ustrezne kadrovske, organizacijske, tehnične in finančne vire. Sredstva za njeno izvajanje se zagotovijo iz državnega proračuna, sredstev Evropske unije, lastnih sredstev izvajalcev ter drugih zakonitih virov financiranja. Pri tem se spodbuja sodelovanje javnega in zasebnega sektorja ter raziskovalnih in akademskih institucij.

Pri načrtovanju in uporabi nacionalnih in evropskih virov financiranja se zagotavlja njihova usklajenost s prednostnimi nalogami strategije ter spodbuja usmerjanje sredstev v razvoj nacionalnih kibernetikovarnostnih zmogljivosti, kompetenc, raziskav in inovacij ter krepitev kibernetiske odpornosti gospodarstva.

Nosilci ukrepov so odgovorni za načrtovanje potrebnih virov ob upoštevanju ocene ogroženosti in ocene tveganj, prednostnih nalog strategije, razvoja kibernetских groženj ter potreb po krepitvi odpornosti države, gospodarstva in družbe.

Konkretni ukrepi, njihovi nosilci in sodelujoči deležniki, roki izvedbe, potrebni in zagotovljeni viri financiranja, finančne in kadrovske posledice ter ključni kazalniki uspešnosti se določijo v akcijskem načrtu.

Pri pripravi in izvajanju akcijskega načrta se preveri tudi morebitni vpliv predlaganih rešitev na že dosežene mejnike in cilje Načrta za okrevanje in odpornost ter zagotovi, da njihovo izvajanje ne posega v že izvedene reforme oziroma ne ustvarja tveganja za njihovo razveljavitev. . Preverjanje se opravi že pri pripravi novih strateških rešitev, zlasti pri posegih v že vzpostavljene institucionalne in tehnične zmogljivosti.

Pri načrtovanju in uporabi virov se upoštevajo načela učinkovitosti, gospodarnosti, sorazmernosti in dolgoročne vzdržnosti, posebna pozornost pa se namenja razvoju strokovnih kadrov ter krepitvi nacionalnih zmogljivosti na področju kibernetiske varnosti.

Strateška usmeritev

- Zagotavljati pogoje za dolgoročno vzdržen razvoj kadrovskih, organizacijskih, tehničnih in finančnih zmogljivosti, potrebnih za izvajanje strateških ciljev ter krepitev kibernetiske odpornosti Republike Slovenije.

Opredelitev ustreznih virov

Naložbe v kibernetško varnost so naložbe v odpornost države, gospodarstva in družbe. Zmanjšujejo tveganje incidentov in stroške njihove obravnave, hkrati pa krepijo zaupanje v slovenski digitalni prostor, produktivnost, inovativnost ter razvoj visokotehnoloških podjetij in strokovnih kadrov.

Ustrezni viri za zagotavljanje kibernetške varnosti vključujejo kadre, tehnično infrastrukturo in finančna sredstva. Kadrovske viri obsegajo pridobivanje, razvoj in zadrževanje strokovnjakov za kibernetško varnost, tehnično-infrastrukturni viri zajemajo varnostne tehnologije, sisteme in orodja, finančno-proračunski viri pa omogočajo njihovo dolgoročno zagotavljanje.

Kadrovske načrtovanje temelji na pregledu potrebnih kompetenc, delovnih obremenitev in zahtev neprekinjenega delovanja. Vključuje razvoj in zadrževanje strokovnjakov, mentorstvo, načrtovanje nasledstva na ključnih delovnih mestih ter krepitev lastnega znanja za vodenje in nadzor zunanjih izvajalcev. Pri projektih financiranih zmogljivostih se že ob odločitvi o naložbi opredelijo prihodnji upravljavci, stroški vzdrževanja in obnove ter viri za delovanje po koncu projekta.

Okvir ocene ogroženosti

Ocena ogroženosti bo temeljila na stalnem spremljanju kibernetških groženj, ranljivosti in njihovih vplivov na delovanje države, gospodarstva ter ključnih storitev. Upoštevala bo tudi stanje kibernetške varnosti v drugih državah članicah EU in NATO ter širše geopolitično dogajanje. Upoštevala bo glavne kategorije kibernetških groženj, ranljivosti informacijskih in operativnih tehnologij, tveganja digitalnih dobavnih verig, odvisnosti od zunanjih izvajalcev in čezmejnih storitev ter možne kaskadne učinke med sektorji.

Na tej podlagi se bodo določali prednostni varnostni ukrepi in priporočila, kot so večfaktorska avtentikacija, upravljanje privilegiranih dostopov, segmentacija omrežij, varnostno kopiranje, zaščita storitev v oblaku in ustrezno šifriranje. Redne varnostne presoje, testi robustnosti, simulacije incidentov in vaje bodo omogočali stalno spremljanje, posodabljanje in izboljševanje metodologije, na podlagi katere se pripravlja ocena ogroženosti, in obvladujejo tveganja.

Nacionalna ocena ogroženosti izhaja iz pregleda ključnih storitev, njihovih informacijskih in drugih podpornih sredstev ter medsebojnih in čezmejnih odvisnosti. Za prednostna tveganja se določijo nosilec obravnave, ukrepi in preostalo tveganje. Ocena se posodablja po potrebi oziroma ob pomembnih spremembah in po večjih incidentih ter je podlaga za razporejanje virov, pripravo sektorskih ukrepov in scenarijev vaj.

SPREMLJANJE, VREDNOTENJE IN POSODABLJANJE STRATEGIJE

Izvajanje strategije se spremlja na podlagi ključnih kazalnikov uspešnosti, rednega poročanja in periodičnega vrednotenja doseganja strateških ciljev. Skladno z ZInFV-1 pristojni nacionalni organ strategijo redno, najmanj vsakih pet let, oceni glede na doseganje ciljev in prednostnih nalog.

URSIV vzpostavi pregleden mehanizem spremljanja napredka, ki omogoča sprotno preverjanje izvajanja ukrepov, doseganja ciljnih vrednosti kazalnikov ter pravočasno prepoznavanje zamud, odstopanj in potreb po prilagoditvah. Za vsak kazalnik se v akcijskem načrtu določita vir podatkov in obdobje zajema. URSIV o izvajanju strategije letno poroča Vladi Republike Slovenije. Poročilo vključuje pregled doseganja kazalnikov, oceno izvajanja akcijskega načrta, ugotovljena odstopanja in predloge za prilagoditve.

Spremljanje poleg izvedenih aktivnosti vključuje njihove učinke: sposobnost obnove ključnih storitev v načrtovanem času, odpravljanje prednostnih ranljivosti, izboljšanje varnostne zrelosti in zmanjševanje kadrovske vrzeli. Kazalniki imajo enotno metodologijo, odgovornega skrbnika, izhodiščno leto in vmesne ciljne vrednosti. Število prijavljenih incidentov se presoja ob upoštevanju sprememb v zaznavanju incidentov in poročanju o njih, saj povečanje samo po sebi ne pomeni slabše varnosti. Za ukrepe, pri katerih prihaja do zamud, se določijo korektivni ukrepi in novi roki. Javno se objavi povzetek napredka brez varovanih ali varnostno občutljivih podatkov.

Strateške usmeritve

- Spremljati izvajanje strategije na podlagi merljivih kazalnikov z opredeljenimi viri podatkov in obdobji zajema.
- Zagotavljati redno poročanje o izvajanju strategije in doseganju ciljev.
- Spremljati razvoj nacionalnih kibernetских zmogljivosti in njihove zrelosti.
- Redno preverjati ustreznost ciljev glede na razvoj groženj, tehnologij in mednarodnega okolja.
- Ugotovitve vaj, incidentov, ocen tveganj in mednarodnih pregledov sistematično vključevati v posodabljanje akcijskega načrta ter nadaljnje izboljševanje nacionalnega sistema kibernetiske varnosti.

Celovito vmesno vrednotenje se izvede najpozneje leta 2030, zaključno vrednotenje pa ob koncu obdobja leta 2035. Ob pomembnih spremembah tveganj, tehnologij ali pristojnosti se predčasno preveri potreba po posodobitvi strategije. V vrednotenje se vključijo nosilci ukrepov ter predstavniki gospodarstva, raziskovalne skupnosti in civilne družbe.

URSIV o sprejetju strategije obvesti Evropsko komisijo v treh mesecih. Pri posredovanju in javni objavi se varujejo podatki, ki so pomembni za nacionalno varnost, in drugi varovani podatki v skladu z veljavnimi predpisi.

Zunanje merilo zrelosti

Republika Slovenija bo poleg ključnih kazalnikov uspešnosti svojo zrelost spremljala tudi z uporabo okvira ENISA National Capabilities Assessment Framework 2.0 (okvir za ocenjevanje nacionalnih zmogljivosti), ki omogoča strukturirano samooceno nacionalnih kibernetских zmogljivosti ter podpira primerljivo spremljanje napredka in pripravo na prostovoljne medsebojne strokovne preglede po direktivi NIS2.

Kot dopolnilni kazalnik se spremljata tudi vrednost in struktura indeksa National Cyber Security Index (NCSI), ki omogoča mednarodno primerjavo nacionalnih kibernetiskovarnostnih zmogljivosti na podlagi javno dostopnih dokazil in katerega spremljanje kot kazalnik predvideva Krovna strategija digitalne preobrazbe Slovenije do leta 2030 »Digitalna Slovenija 2030«. Pri vrednotenju se upoštevajo rezultati po posameznih področjih indeksa, ne le skupna uvrstitev Republike Slovenije.

Ena prvih nalog v okviru izvajanja akcijskega načrta bo ocena izhodiščnega stanja po opredeljenem okviru, na podlagi katere se bodo določile ciljne stopnje zrelosti. Pri tem se ocenijo tudi potrebni in razpoložljivi finančni ter kadrovski viri, saj je ustrezno zagotavljanje teh virov eden ključnih pogojev za doseganje načrtovanih stopenj zrelosti.