REPUBLIKA SLOVENIJA
VLADA REPUBLIKE SLOVENIJE

Gregorčičeva ulica 20–25, 1000 Ljubljana

T: +386 1 478 1000
F: +386 1 478 1607
E: gp.gs@gov.si
http://www.vlada.si/

Številka: 38600-3/2021/4
Datum: 18. 3. 2021

NACIONALNI NAČRT ODZIVANJA NA KIBERNETSKE INCIDENTE

KAZALO

KAZALO PREGLEDNIC

SEZNAM PREDPISOV

- Resolucija o strategiji nacionalne varnosti Republike Slovenije (Uradni list RS, št. 59/19)
- Strategija kibernetske varnosti (RS, februar 2016)
- Zakon o informacijski varnosti (Uradni list RS, št. 30/18)
- Zakon o elektronskih komunikacijah (Uradni list RS, št. 109/12, 110/13, 40/14 – ZIN-B, 54/14 – odl. US, 81/15 in 40/17)
- Zakon o tajnih podatkih (Uradni list RS, št. 50/06 – uradno prečiščeno besedilo, 9/10, 60/11 in 8/20)
- Uredba o informacijski varnosti v državni upravi (Uradni list RS, št. 29/18)
- Uredba o določitvi bistvenih storitev in podrobnejši metodologiji za določitev izvajalcev bistvenih storitev (Uradni list RS, št. 39/19)
- Pravilnik o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev (Uradni list RS, št. 32/19)
- Pravilnik o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave (Uradni list RS, št. 30/18)
- ISO/IEC 27035-1:2016 Information technology – Security techniques – Information security incident management — Part 1: Principles of incident management

1 UVOD

V vsakdanjem življenju se iz dneva v dan povečuje uporaba informacijskih sistemov, omrežij, pametnih naprav in interneta stvari (angl. *Internet of things* – v nadaljevanju: IoT). Uporaba modernih sistemov in tehnološko dovršenih naprav, ki so med seboj povezani v splet, vpliva tako na razvoj gospodarskih in negospodarskih dejavnosti kot tudi na vsakdanje življenje in blaginjo celotne družbe.

Hiter razvoj informacijsko-komunikacijskih tehnologij družbi prinaša velike koristi, ob tem pa močno vpliva tudi na pojav in razvoj novih tehnološko vse bolj dovršenih kibernetskih groženj. Nedvomno so že danes, v prihodnje pa bodo še bolj, kibernetski napadi ena od najpomembnejših varnostnih groženj sodobnemu svetu, kar pomeni, da se mora kibernetska varnost uvrstiti med ključne sestavne dele nacionalno varnostnega sistema.

Pomembnost kibernetske varnosti na državni ravni je poudarjena tudi v Resoluciji o strategiji nacionalne varnosti Republike Slovenije iz leta 2019, ki informacijsko-kibernetske grožnje opredeljuje tako:

»Značilnost kibernetskega okolja so globalna narava, asimetričnost in horizontalnost, kar se odraža v odsotnosti geografskih in časovnih omejitev, težavni določljivosti dejanskega vira in akterja ogrožanja ter v dejstvu, da gre lahko za aktivnost državnih in nedržavnih akterjev. Ranljivost sodobne družbe izhaja iz močne odvisnosti od neprekinjenosti in zanesljivosti delovanja informacijskih tehnologij in sistemov. Republika Slovenija je s tem izpostavljena resnim grožnjam za delovanje javnega in zasebnega sektorja ter kritične infrastrukture, zaradi česar je lahko ogroženo izvajanje ključnih funkcij države in družbe. Zagotavljanje suverenosti Republike Slovenije v kibernetskem prostoru je zato izrednega pomena.

Ključno grožnjo nacionalni informacijsko-komunikacijski infrastrukturi in kritični informacijsko-komunikacijski infrastrukturi ter podatkom znotraj njiju predstavljajo kibernetski napadi in vdori, spletno vohunjenje, kraja intelektualne lastnine, širjenje dezinformacij, kibernetski kriminal in terorizem ter druge oblike, ki imajo lahko velik negativen medpodročni vpliv na gospodarstvo in finančni sistem, delovanje političnega sistema in mednarodni ugled države, delovanje kritične infrastrukture, javno varnost, obrambno sposobnost, varnost državljanov, zagotavljanje osnovnih življenjskih dobrin ter delovanje sistema varstva pred naravnimi in drugimi nesrečami.

Vključenost Republike Slovenije v mednarodne organizacije, predvsem Evropsko unijo in Nato, povečuje interes nekaterih tujih držav in drugih akterjev ter s tem dejansko izpostavljenost države kibernetskim napadom.«

Za okrepitev celotnega sistema kibernetske varnosti in nemotenega delovanja sistemov, od katerih je odvisno delovanje celotne družbe, je Republika Slovenija februarja 2016 sprejela Strategijo kibernetske varnosti, ki je poleg zavezujočih mednarodnih dokumentov temelj za sistemsko ureditev obravnavanega področja. Na podlagi strategije je bil aprila 2018 sprejet Zakon o informacijski varnosti (v nadaljevanju: ZInfV), ki podrobneje ureja obravnavano področje. Z ZInfV je bila v notranji pravni red prenesena Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji, ki ureja obravnavano področje na ravni Evropske unije (v nadaljevanju: direktiva NIS). V pripravi so spremembe in dopolnitve te direktive, delovno poimenovane NIS2, ki bodo vplivale na nadaljnji razvoj in način dviga ravni kibernetske varnosti v Evropski uniji in pri nas.

Veljavni notranji in mednarodni normativni predpisi so ključni za vzpostavitev močnega državnega sistema kibernetske varnosti, ki bo sposoben hitrega odzivanja na varnostne grožnje in bo učinkovito zaščitil informacijsko-komunikacijsko infrastrukturo in informacijske sisteme, s čimer se bo zagotavljalo neprekinjeno delovanje tako javnega kot zasebnega sektorja, predvsem pa ključnih funkcij države in družbe v vseh varnostnih razmerah.

Najboljša zaščita proti neželenim kibernetskim aktivnostim je preventiva. Državne institucije, gospodarska podjetja in posamezniki lahko za uspešno kibernetsko varnost storijo veliko z uporabo primernih orodij in izvajanjem zaščitnih ukrepov. Za doseganje visoke ravni kibernetske varnosti pa ni dovolj samo preventiva. Dejstvo je, da neželenih kibernetskih aktivnosti oziroma kibernetskih incidentov nikoli ne bo mogoče v celoti preprečiti in odpraviti, zato je nujno treba zagotoviti ustrezne mehanizme odzivanja nanje. Državni sistem odzivanja na kibernetske incidente je sistem, ki zagotavlja pravočasno, učinkovito in uspešno zaznavanje, omejevanje in preiskovanje neželenih kibernetskih aktivnosti ter obnovitev in ponovno vzpostavitev sistema po kibernetskem incidentu.

Temelj državnega sistema odzivanja na kibernetske incidente je Nacionalni načrt odzivanja na kibernetske incidente (v nadaljevanju NOKI), ki je nastal na podlagi Strategije kibernetske varnosti in

ZInfV.[1] Pri izdelavi NOKI so bili upoštevani tudi drugi notranji in mednarodni predpisi, kot so Zakon o elektronskih komunikacijah (v nadaljevanju: ZEKom), Uredba o informacijski varnosti v državni upravi, direktiva NIS in drugi.

Ta načrt je vodilo zavezancem iz ZInfV, komu, kdaj in kako priglasiti kibernetski incident znotraj svojih sistemov. Na podlagi NOKI morajo zavezanci pripraviti interne načrte odzivanja na kibernetske incidente oziroma obstoječe načrte prilagoditi ter s tem seznaniti pristojni nacionalni organ in pristojni odzivni center. Pristojni nacionalni organ lahko s posameznimi državnimi organi, ki delujejo na področju varnosti države in imajo vzpostavljen varnostno-operativni center, sklene sporazum, ki podrobneje opredeljuje naloge, postopke in obveznosti glede na pristojnosti posameznega organa.

[1] Enajsta točka drugega odstavka 27. člena ZInfV pravi, da pristojni nacionalni organ izdela nacionalni načrt odzivanja na incidente ob upoštevanju strategije, načrtov nacionalnega CSIRT in CSIRT organov državne uprave, drugih pristojnih organov ter varnostne dokumentacije zavezancev.

2 NAMEN NACIONALNEGA NAČRTA ODZIVANJA NA KIBERNETSKE INCIDENTE

Odzivanje na kibernetske incidente je med ključnimi elementi odvračanja kibernetskih groženj in zagotavljanja državne kibernetske varnosti. V Resoluciji o strategiji nacionalne varnosti Republike Slovenije iz leta 2019 sta v delu, ki opredeljuje odzivanje na kibernetske grožnje in zlorabo informacijskih tehnologij in sistemov, poudarjeni celovitost in sistematičnost pri zaznavi, obravnavi in odzivanju na kibernetske grožnje, incidente in napade:

»Republika Slovenija bo na področju kibernetske varnosti in obrambe aktivno spremljala mednarodno dinamiko odzivanja na kibernetske grožnje ter ustrezno prilagajala nacionalno strategijo in normativno urejanje področja.

Vzpostavljen nacionalni organ za kibernetsko področje bo zagotavljal celovito upravljanje področja in koordinacijo z vsemi resorji in drugimi subjekti v vseh varnostnih razmerah. Za podporo strateškemu odločanju bo na podlagi podatkov vseh subjektov nacionalno-varnostnega sistema pripravljal analize in ocene o grožnjah in stanju na področju kibernetske varnosti. Zagotavljal bo tudi celovitost in sistematičnost pri zaznavi, obravnavi in odzivanju na kibernetske grožnje, incidente in napade.

Republika Slovenija bo zagotovila učinkovit sistem zagotavljanja kibernetske varnosti s povezanimi ukrepi na področju preprečevanja in odzivanja ter ozaveščanja vseh delov družbe. Sistem bo povezal subjekte iz javne uprave, gospodarstva in akademsko-raziskovalne sfere ter tako krepil njihovo medsebojno sodelovanje. S spodbujanjem uvedbe novih tehnologij v javnem in zasebnem sektorju bo država vzpostavila pogoje za varno delovanje kritične infrastrukture ter ključnih komunikacijsko-informacijskih sistemov. Nacionalni ukrepi se bodo ustrezno prilagajali aktualnim aktivnostim v mednarodnem okolju.

Zagotavljanje učinkovitega delovanja nacionalnega sistema kibernetske varnosti in obrambe bo zahtevalo kontinuirano prilagajanje ter nadgradnjo virov, mehanizmov in procesov na strateški in izvedbeni ravni.«

NOKI poenoti postopke upravljanja kibernetskih incidentov in vsem deležnikom podaja smernice za na državni ravni usklajen odziv in za usklajevanje z zainteresiranimi stranmi pri kibernetskem incidentu, še posebej kadar kibernetski incident vpliva na storitev, ki je bistvena za ohranitev ključnih družbenih oziroma gospodarskih dejavnosti, kot jo določa ZInfV. NOKI določa skupno doktrino in strateški okvir za odzivanje celotnega kroga deležnikov – vse ravni državnega sestava (državni organi in institucije), lokalne samouprave, zasebni in neprofitni sektor (vključno z zasebnimi in javnimi lastniki ter upravljavci kritične infrastrukture). Vsi deli skupnosti, ki so vpleteni v kibernetsko varnost, morajo biti proaktivni, vključeni za čim hitrejše, pravilno in učinkovito ukrepanje ob kibernetskem incidentu.

Pristojni nacionalni organ (PNO) za kibernetsko varnost, ki vodi, upravlja in usklajuje kibernetsko varnost na državni ravni, povezuje vse deležnike kibernetske varnosti in opravlja naloge, določene z ZInfV, je v Republiki Sloveniji **Uprava Republike Slovenije za informacijsko varnost** (**URSIV**). URSIV vodi seznam kibernetskih incidentov na podlagi tedenskih in podrobnih poročil o kibernetskih incidentih, ki jih pošiljajo odzivni centri glede na svojo pristojnost.

Pristojnost glede vprašanj kibernetske varnosti, povezanih z upravljanjem kibernetskih incidentov in odzivanjem nanje, je odvisna od tega, v katerih informacijskih in komunikacijskih omrežjih se incident zgodi. Odzivni centri, ki so odgovorni za obravnavo kibernetskih incidentov in odzivanje nanje v javnem sektorju, kritični infrastrukturi in pri izvajalcih bistvenih storitev ter v omrežjih Ministrstva za obrambo (v nadaljevanju: MO), Policije in Slovenske obveščevalno-varnostne agencije (v nadaljevanju: SOVA), so:

SI-CERT – V skladu s prvim odstavkom 28. člena ZInfV je nacionalni CSIRT odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij SI-CERT pri javnem zavodu Akademska in raziskovalna mreža Slovenije. Zadolžen je za obravnavo kibernetskih incidentov v omrežjih izvajalcev bistvenih storitev (IBS), v omrežjih ponudnikov digitalnih storitev (PDS) ter za vse prostovoljne priglasitve drugih pravnih subjektov in fizičnih oseb. Pripravlja tedensko poročilo o kibernetskih incidentih pod določenim kritičnim pragom *(*angl. *threshold)* in podrobna poročila o kibernetskih incidentih, ki presežejo kritični prag, ter poročila v skladu z navodili tega načrta pošlje URSIV. Za četrtletno obdobje pripravi poročilo o izvajanju svojih nalog in ga pošlje URSIV. SI-CERT izvaja tudi nacionalni program ozaveščanja širše javnosti *Varni na internetu.*

SIGOV-CERT – V skladu s prvim odstavkom 29. člena ZInfV naloge CSIRT za organe državne uprave izvaja ministrstvo, pristojno za upravljanje informacijsko-komunikacijskih sistemov državne uprave. Odzivni center za kibernetsko varnost državne uprave je zadolžen za obravnavo kibernetskih incidentov v centralnem komunikacijskem omrežju državne uprave (HKOM) in v omrežjih organov

državne uprave (ODU), določenih v skladu z ZInfV. Pripravlja tedenska poročila o kibernetskih incidentih pod določenim kritičnim pragom *(*angl. *threshold)* in podrobna poročila o kibernetskih incidentih, ki presežejo kritični prag, ter poročila v skladu z navodili tega načrta pošlje URSIV. O kibernetskih incidentih in dogodkih v skladu z ZInfV obvešča tudi SI-CERT. Za četrtletno obdobje pripravi poročilo o izvajanju svojih nalog in ga pošlje URSIV.

SOC MO – Varnostno-operativni center MO je zadolžen za obravnavo kibernetskih incidentov v omrežjih ministrstva. Pripravlja poročila o kibernetskih incidentih v skladu z Nacionalnim načrtom odzivanja na kibernetske incidente in po potrebi sodeluje pri obravnavi incidentov drugih zavezancev.

SOC POLICIJA – Varnostno-operativni center Policije je zadolžen za obravnavo kibernetskih incidentov v svojih omrežjih. Pripravlja poročila o kibernetskih incidentih v skladu z Nacionalnim načrtom odzivanja na kibernetske incidente in po potrebi sodeluje pri obravnavi incidentov drugih zavezancev.

SOC SOVA – Varnostno-operativni center Slovenske obveščevalno-varnostne agencije je zadolžen za zaščito omrežij agencije in obravnavo kibernetskih incidentov v svojih omrežjih. Center pripravlja poročila o kibernetskih incidentih v skladu z Nacionalnim načrtom odzivanja na kibernetske incidente in po potrebi sodeluje pri obravnavi incidentov drugih zavezancev.

AKOS – Področje kibernetskih incidentov pri operaterjih elektronskih komunikacij ureja ZEKom. Agencija za komunikacijska omrežja in storitve Republike Slovenije (v nadaljevanju: AKOS) pripravlja tedenska poročila o kibernetskih incidentih pod določenim kritičnim pragom *(*angl. *threshold)* in podrobna poročila o kibernetskih incidentih, ki presežejo kritični prag, ter poročila pošlje URSIV.

Odzivni centri pri upravljanju posameznih kibernetskih incidentov po potrebi lahko sodelujejo med seboj in si izmenjujejo podatke. Za usklajevanje kibernetskih incidentov na državni ravni je zadolžena URSIV v skladu s šestim poglavjem tega dokumenta.

2.1 Cilji Nacionalnega načrta odzivanja na kibernetske incidente

NOKI je namenjeni poenotenju upravljanja kibernetskih incidentov in odzivanja nanje na državni ravni. V ta namen so pripravljeni:

- poenotena homogena taksonomija glede klasifikacije, nevarnosti in vpliva kibernetskih incidentov,
- opredelitev kibernetskih incidentov, o katerih je treba obvestiti pristojne odzivne centre in URSIV, kot je določeno v veljavni zakonodaji in po za ta namen določenih komunikacijskih poteh,
- enotna metodologija poročanja in spremljanja kibernetskih incidentov,
- enotno odzivanje deležnikov na državni ravni v primeru kritičnih incidentov.

Zavezanci, ki morajo priglasiti kibernetski incident v skladu z ZInfV, morajo poročati o tistih kibernetskih incidentih, ki so se zgodili v njihovih informacijskih infrastrukturah ali drugih informacijskih sistemih, ki vplivajo na določeno bistveno storitev ter presegajo prag, ki je določen s stopnjami učinka in žrtvami incidenta, določenimi v tem dokumentu. Priporočeno je, da zavezanci poročajo tudi o drugih kibernetskih incidentih ali kibernetskih grožnjah, ki so nižje od določenega praga, vendar pomembne za ozaveščanje in preventivo ter pripomorejo k oblikovanje celovite slike dogajanja v kibernetskem prostoru.

Pri fizičnih osebah, državljanih in drugih pravnih subjektih, ki niso zavezanci po ZInfV, je priglasitev kibernetskih incidentov prostovoljna. Vendar je priglasitev takšnih incidentov priporočljiva in vsekakor koristna, saj lahko ključno pomaga pri reševanju incidentov, preventivi in ozaveščanju. Za to ciljno populacijo je ta dokument podlaga za pripravo smernic v obliki dobrih praks.

3 OPREDELITEV IN STOPNJE KIBERNETSKIH INCIDENTOV

Jasna definicija in opredelitev stopnje kibernetskega incidenta je ključen korak v odzivu na posamezni kibernetski incident, saj so od opredelitve odvisni vsi nadaljnji koraki in postopki na vseh ravneh. Ključno je poenoteno razumevanje izrazov in sistema vrednotenja incidentov. Vsi kibernetski incidenti nimajo enakih značilnosti ali posledic, zato je treba določiti skupno klasifikacijo možnih incidentov. Za taksonomijo kibernetskih incidentov je kot podlaga uporabljena klasifikacija Evropske agencije za kibernetsko varnost (v nadaljevanju: ENISA),[2] dopolnjena s taksonomijo Nata in taksonomijo SI-CERT. Zaradi doseganja interoperabilnosti so ohranjeni angleški izrazi za kategorije in vrste incidentov.

Kategorija incidenta	Vrsta incidenta	*Incident type*	Opis
Žaljiva/zlonamerna vsebina **(Abusive Content)**	Neželena sporočila	SPAM	Neželena elektronska pošta vseh oblik, od reklam do zadetkov na loterijah. Prejemnik ni dal preverljivega dovoljenja za pošiljanje sporočila. Sporočilo je poslano kot del večje zbirke sporočil, ki imajo funkcionalno primerljivo vsebino.
	Žaljiva vsebina/žaljiv govor	Harmful Speech	Diskreditacija ali diskriminacija nekoga (npr. kibernetsko zalezovanje, rasizem in grožnje enemu ali več posameznikom).
	Spolna/nasilna vsebina	Child / Sexual / Violence / …	Otroška pornografija, poveličevanje nasilja in podobno.
Zlonamerna koda **(Malicious Code)**	Virus	Virus	Programska oprema, ki je namerno vključena ali vstavljena v sistem za škodljive namene. Za aktiviranje kode je običajno potrebna interakcija uporabnika.
	Črv	Worm	
	Trojanski konj	Trojan	
	Vohunska programska oprema	Spyware	
	Dialler	Dialler	
	Rootkit	Rootkit	
	Boti in botneti	Bot	
	Nadzorni strežnik	CnC	
	Izsiljevalski virus	Ransomware	
	Orodje za oddaljeni nadzor (RAT)	Remote Access Trojan	
Zbiranje informacij **(Information Gathering)**	Odkrivanje morebitnih tarč in ranljivosti	Scanning	Napadi, ki pošiljajo zahteve v sistem za odkrivanje šibkih točk. To vključuje tudi nekakšen postopek testiranja za zbiranje informacij o gostiteljih, storitvah in računih. Primeri: poizvedovanje po DNS, ICMP, SMTP (EXPN, RCPT itd.), skeniranje vrat.
	Prestrezanje komunikacije	Sniffing	Opazovanje in zapisovanje omrežnega prometa (prisluškovanje).
	Socialni inženiring	Social engineering	Zbiranje informacij od posameznika samega na netehnični način (npr. laži, triki, podkupnine ali grožnje).
Poizkusi vdora **(Intrusion Attempts)**	Izkoriščanje znanih ranljivosti	Exploiting known vulnerabilities	Poskus ogrožanja sistema ali motnje katere koli storitve z izkoriščanjem ranljivosti s standardiziranim identifikatorjem, kot je ime CVE (npr. preliv medpomnilnika, zadnja vrata, skriptno križišče itd.).
	Poskusi prijav, bruteforce in napadi s slovarjem	Login attempts	Več poskusov prijave (Guessing / cracking of passwords, brute force).
	Nova vrsta napada	New attack signatures	Poskusi z neznanim izkoriščanjem.

[2] Reference Incident Classification Taxonomy Task Force Status and Way Forward (ENISA, januar 2018).

Kategorija incidenta	Vrsta incidenta	*Incident type*	Opis
Vdori **(Intrusions)**	Zloraba privilegiranega uporabniškega računa	Privileged account compromise	Uspešen vdor v sistem ali aplikacijo (storitve). To lahko na daljavo omogoči znana ali nova ranljivost, pa tudi nepooblaščeni lokalni dostop. Vključuje tudi, da ste del botneta.
	Zloraba neprivilegiranega uporabniškega računa	Unprivileged account compromise	
	Napadi na aplikacijo	Application compromise	
	Bot	Bot	
Razpoložljivost **(Availability)**	Napad onemogočanja	DoS	S tovrstnim napadom se sistem bombardira s toliko paketi, da se operacije zavlečejo ali sistem zruši. Primeri DoS so poplave ICMP in SYN, napadi Teardrop in bombardiranje po pošti. DDoS pogosto temelji na napadih DoS, ki izvirajo iz botnetov, obstajajo pa tudi drugi scenariji, kot so napadi z ojačitvijo (DNS Amplification). Na razpoložljivost lahko vplivajo tudi lokalne akcije (uničenje, prekinitev oskrbe z električno energijo itd.) ali višja sila (naravne nesreče), spontane okvare ali človeške napake, ne da bi šlo za zlobo ali grobo zanemarjanje.
	Porazdeljeni napad onemogočanja	DDoS	
	Sabotaža	Sabotage	
	Izpad delovanja naprav ali omrežja	Outage (no malice)	
Varnost informacijskih virov **(Information Content Security)**	Nepooblaščeni dostop do informacij	Unauthorised access to information	Poleg lokalne zlorabe podatkov in sistemov lahko varnost informacij ogrozi uspešen kompromis med računom ali aplikacijo. Poleg tega so možni napadi, ki med prenosom prestrežejo informacije in dostopajo do njih (prisluškovanje, podvajanje ali ugrabitev). Vzrok je lahko tudi napaka med ljudmi/konfiguracijo/programsko opremo.
	Nepooblaščeno spreminjanje informacij	Unauthorised modification of information	
	Odtekanje informacij	Information disclosure / leakage	
	Uničenje informacij	Information destruction	
Goljufije **(Fraud)**	Nepooblaščeno izkoriščanje virov	Unauthorized use of resources	Uporaba virov za nepooblaščene namene, vključno s podjetji, ki prinašajo dobiček (npr. uporaba e-pošte za sodelovanje v nezakonitih pismih verig dobička ali piramidnih shemah).
	Intelektualna lastnina in avtorske pravice	Copyright	Ponudba ali namestitev kopij nelicencirane komercialne programske opreme ali drugega materiala, zaščitenega z avtorskimi pravicami (Warez).
	Kraja identitete	Masquerade	Vrsta napadov, pri katerih en subjekt nezakonito prevzame identiteto drugega, da bi imel od tega koristi.
	Phishing sporočilo	Phishing email	Maskiranje v drugo osebo, da bi prepričali uporabnika, da razkrije zasebno poverilnico.
	Phishing spletno mesto	Phishing site	Odkrite lažne spletne strani za izvedbo phishing napada.
	Spletno nakupovanje	On-line shopping	Oškodovanja pri spletnem nakupovanju, lažne spletne trgovine.
	Goljufija z vnaprejšnjim plačilom	Advance-fee fraud	Spletna goljufija, v kateri se zahteva vnaprejšnje plačilo za dostop do obljubljene finančne nagrade ali drugih storitev.
	Izsiljevanje	Extortion	Izsiljevanje z grožnjami objave občutljivih podatkov ali z grožnjami kibernetskega napada.

Kategorija incidenta	Vrsta incidenta	*Incident type*	Opis
	Druge goljufije	Scam	Vse druge oblike spletnih goljufij.
Ranljivost (Vulnerable)	Ranljivi sistemi in naprave	Vulnerable systems	Prosto dostopni in neustrezno zaščiteni sistemi in naprave, ki jih je možno zlorabiti na podlagi znanih ranljivosti. Odprti, nezaščiteni tolmači domenskih imen, svetovno berljivi tiskalniki, ranljivost, ki je razvidna iz pregledov Nessusa, podpisi virusov niso posodobljeni itd.
	Odgovorno razkrivanje	Responsible disclosure	
	Razkritje ranljivosti	Other disclosure	
Drugo (Other)	Drugo	Other	Vse incidente, ki ne sodijo v eno od opredeljenih kategorij, je treba vključiti v ta razred (če se število incidentov v tej kategoriji poveča, to kaže, da je treba sistem klasifikacije spremeniti).
Test	Test	Test	Namenjeno preizkusom.

Preglednica 1: Taksonomija kibernetskih incidentov

3.1 Opredelitev kibernetskih incidentov po Zakonu o informacijski varnosti

ZInfV v 4. členu opredeljuje ključne izraze, med katerimi so tudi:

- **INCIDENT** – vsak dogodek, ki ima dejanski negativni učinek na varnost omrežij in informacijskih sistemov,
- **KIBERNETSKA GROŽNJA** – možnost zlonamernega poskusa poškodovanja ali prekinitve računalniškega omrežja, sistema, storitev in podatkov,
- **KIBERNETSKI NAPAD** – napad prek kibernetskega prostora z namenom zlonamernega uničevanja, izpostavljanja, nadzorovanja ali spreminjanja, onemogočanja, zbiranja in oviranja katerega koli dela kibernetskega prostora, vključno glede informacij, ki so bistvenega pomena za nemoteno delovanje države.

V 21. členu ZInfV opredeljuje vrednotenje incidenta in ukrepanje. Kibernetski incidenti so razvrščeni v tri stopnje (lažji, težji in kritični), kar je podlaga za določanje praga za obvezno poročanje *(*angl. *threshold)* zavezancev:

- **LAŽJI INCIDENT** – enkraten incident, ki ima majhen negativni vpliv na zaupnost, celovitost in razpoložljivost omrežja, informacijskega sistema oziroma informacijskih storitev zavezanca. Nima večjega vpliva na nemoteno delovanje zavezanca in mu ni povzročil večje škode. Incident nima negativnega medpodročnega vpliva ali negativnega vpliva na delovanje informacijskih sistemov obrambe, notranje varnosti ter sistema zaščite in reševanja.
- **TEŽJI INCIDENT** – enkraten incident oziroma zaporedje večjega števila različnih incidentov v kratkem obdobju, ki ima velik negativni vpliv na zaupnost, celovitost in razpoložljivost omrežja, informacijskega sistema oziroma informacijskih storitev zavezanca. Incident ima pomemben vpliv na nemoteno delovanje zavezanca in mu povzroči večjo škodo ali izgubo. Ob tem ima takšen incident lahko tudi negativni medpodročni vpliv oziroma negativni vpliv na delovanje informacijskih sistemov obrambe, notranje varnosti ter sistema zaščite in reševanja, vendar na te sestave nima kritičnega vpliva.

– **KRITIČNI INCIDENT** – incident ali zaporedje incidentov, ki ima zelo velik negativni vpliv na zaupnost, celovitost in razpoložljivost omrežja, informacijskega sistema oziroma informacijskih storitev zavezanca. Incident povzroči oteženo delovanje države, še posebej informacijskih sistemov obrambe, notranje varnosti ter sistema zaščite in reševanja, oziroma delno onemogoči delovanje vsaj treh področij bistvenih storitev ali enega v celoti.

3.2 Razvrstitev kibernetskih incidentov na podlagi žrtev in učinka

Stopnja kazalnikov in njihova interakcija določata, ali je kibernetski incident pod pragom obveznega poročanja ali ne in kakšni so postopki deležnikov kibernetske varnosti. Razvrstitev kibernetskih incidentov temelji na dveh skupinah kazalnikov, s katerimi se kibernetskemu incidentu določi končna stopnja:

1. Kazalniki učinka kibernetskega incidenta – določajo stopnjo nevarnosti morebitne grožnje, ki jo pomeni kibernetski incident v informacijskih ali komunikacijskih sistemih napadenega deležnika in njegovih storitvah. Ti kazalniki temeljijo na značilnostih, ki so značilne za vrsto grožnje in njene učinke.

   Kibernetski incidenti bodo povezani z eno od naslednjih stopenj učinka:

KRITIČNA	ZELO VISOKA	VISOKA	VIŠJA	SREDNJA	MINIMALNA

   Merila, ki se uporabljajo za določitev stopnje učinka, povezane s kibernetskim incidentom, vključujejo naslednje parametre ogroženosti omrežji, informacijskih sistemov oziroma informacijskih storitev:
   - ogroženost razpoložljivosti,
   - ogroženost zaupnosti,
   - ogroženost celovitosti,
   - moteno delovanje,
   - poškodovanje ali odtujitev podatkov,
   - povzročitev škode in finančna izguba.

2. Kazalniki vplivnega področja kibernetskega incidenta (žrtve) – pomenijo napadene »žrtve«, število napadenih »žrtev«, oceno morebitnih posledic kibernetskega incidenta za funkcije in dejavnosti prizadetega deležnika ter morebitno škodo na premoženju.

   Kibernetski incidenti bodo povezani z eno od naslednjih stopenj vpliva/učinka:

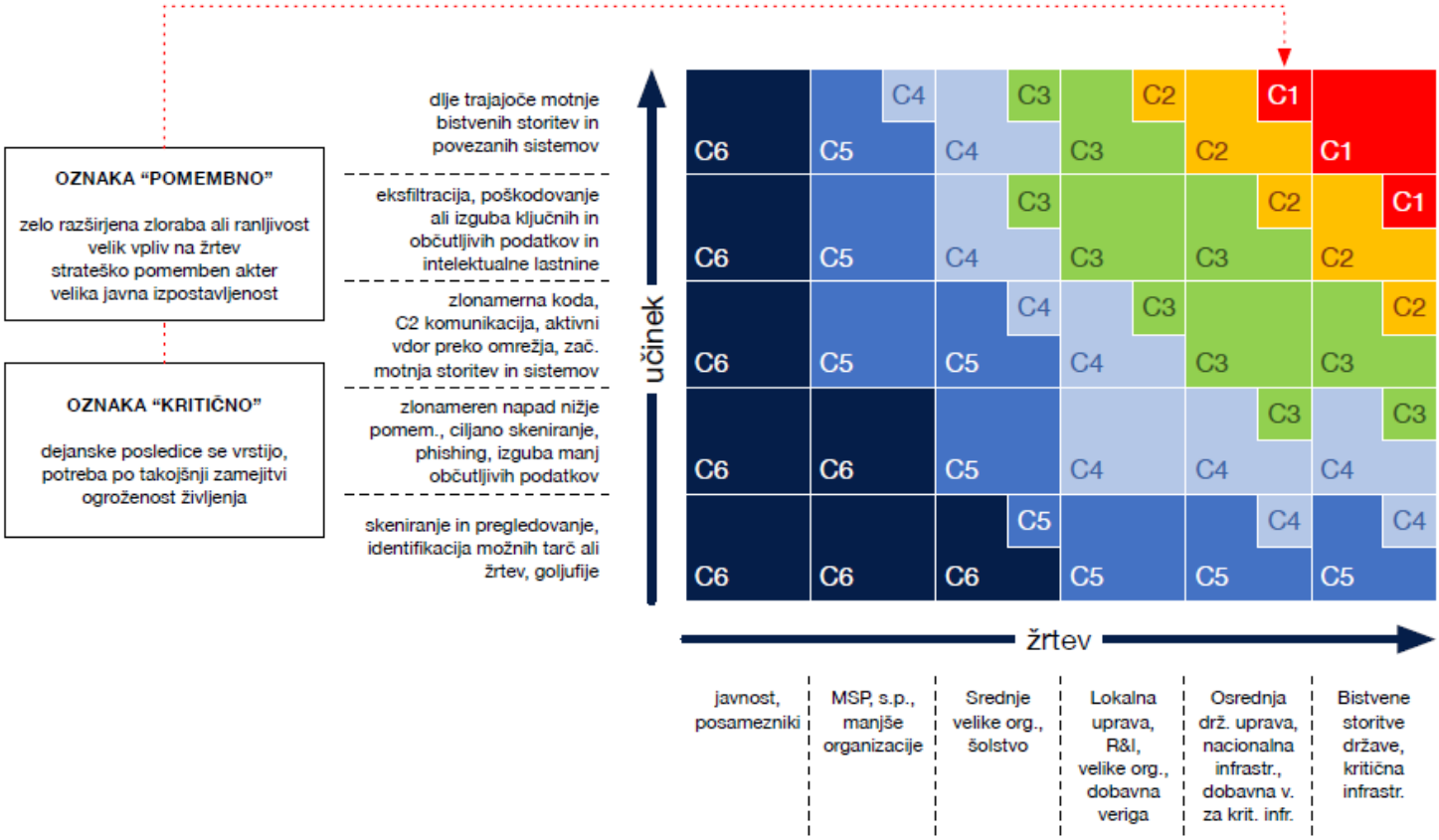
KRITIČNA	ZELO VISOKA	VISOKA	SREDNJA	NIZKA	NEZNATNA

   Merila, ki se uporabljajo za določitev stopnje vpliva, povezane s kibernetskim incidentom, zajemajo naslednje parametre:
   - vpliv na določeno število uporabnikov prek zavezanca,
   - prekinitev zagotavljanja običajne storitve organizacije,
   - negativni medresorski vpliv,
   - učinki na zagotavljanje bistvenih storitev ali kritične infrastrukture,
   - onemogočeno delovanje informacijskih sistemov obrambe, notranje varnosti ter sistema zaščite in reševanja,
   - vpliv na varnost države ali varnost državljanov.

3.3 Podrobno stopnjevanje kibernetskih incidentov in prag obveznega poročanja

Podrobno stopnjevanje in dodatna razdelitev stopenj incidentov iz ZInfV pripomore k lažjemu in podrobnejšemu razvrščanju ter določanju praga in časovnega okvira za poročanje. Podrobno stopnjevanje je povzeto in prilagojeno po kategorizaciji incidentov, ki jih že uporablja SI-CERT[3] in so tako že preizkušeni v praksi. V preglednici 2 je opredeljena podrobna razvrstitev kibernetskih incidentov v korelaciji s stopnjo kibernetskih incidentov po ZInfV.

Kibernetski incidenti se razvrščajo v odnosu med napadenim deležnikom (žrtvijo kibernetskega incidenta) in stopnjo nevarnosti (učinkom kibernetskega incidenta). Preglednica 2 prikazuje povezavo med kazalniki pri določanju stopnje kibernetskega incidenta.



Preglednica 2: Povezava med kazalniki pri določanju stopnje kibernetskega incidenta

[3] Kategorizacija incidentov SI-CERT je povzeta in prilagojena po dokumentu »National Cyber Incident Categorisation« britanskega centra za kibernetsko varnost NCSC-UK, UK Crown Copyright ©, predstavljenega na mreži CSIRT.

Zavezanci v skladu z ZInfV brez nepotrebnega odlašanja priglasijo kibernetske incidente SI-CERT ali SIGOV-CERT, ki določata stopnje incidentov in o tem obvestita PNO. Državni organi z lastnimi SOC (MO, Policija, SOVA) o kibernetskem incidentu s pomembnim vplivom obvestijo PNO, ki incidentu določi stopnjo. Odzivni centri in PNO se pri določanju stopnje incidenta lahko posvetujejo med seboj in uskladijo.

STOPNJEVANJE V SKLADU Z ZInfV	STOPNJEVANJE NA PODLAGI KAZALNIKOV	OPIS INCIDENTA
KRITIČNI	**KRITIČNI INCIDENT (C1)**	Incident povzroči oteženo delovanje države, še posebej informacijskih sistemov obrambe, notranje varnosti ter sistema zaščite in reševanja. Povzročanje resne motnje delovanja osrednjih državnih storitev, motnja stabilnosti države. Ima velik negativni vpliv na omrežja in informacijske sisteme oziroma informacijske storitve zavezancev.
TEŽJI	**ZELO POMEMBNI INCIDENT (C2)**	Zaznan negativni vpliv na občutljive podatke in delovanje državne in kritične infrastrukture, ki je opredeljena v 5. in 6. členu ZInfV. Zaznan velik negativni vpliv na omrežja in informacijske sisteme oziroma informacijske storitve zavezancev. Negativno vpliva na delovanje informacijskih sistemov obrambe, notranje varnosti ter sistema zaščite in reševanja.
	POMEMBNI INCIDENT (C3)	Možen vpliv na izvajalce bistvenih storitev, dele državne infrastrukture in dobavno verigo za kritično infrastrukturo. Možen negativni medpodročni vpliv.
LAŽJI	**SREDNJI INCIDENT (C4)**	Zaznan majhen negativni vpliv na omrežja in informacijske sisteme oziroma informacijske storitve zavezancev. Vpliv na izvajalce bistvenih storitev ali vpliv na gospodarstvo in dele državne uprave ali dobavno verigo.
	LAŽJI INCIDENT (C5)	Možen vpliv na omrežja in informacijske sisteme oziroma informacijske storitve zavezancev ali priprave na napad na gospodarstvo ali državno infrastrukturo.
KIBERNETSKA GROŽNJA	**VARNOSTNI DOGODEK (C6)**	Zaznane kibernetske aktivnosti, ki nimajo vpliva na omrežja in informacijske sisteme oziroma informacijske storitve zavezancev. Zaznan ali možen vpliv na posamezne fizične osebe ali posamezna podjetja v državi, ki niso zavezanci.

Preglednica 3: Podrobna razvrstitev kibernetskih incidentov

3.4 Določitev praga za poročanje in časovni okvir poročanja

Obvezno poročanje zavezancev o kibernetskih incidentih je določeno v skladu z ZInfV. Zavezanec poroča o vseh incidentih, pri katerih je prišlo ali obstaja možnost, da bo prišlo do dejanskega negativnega vpliva na omrežje, informacijske sisteme, podatke in informacije ali storitve zavezanca.

Kibernetski incidenti se razvrstijo v eno od kategorij od C1 do C6, poročanje je obvezno za vse incidente razen za incidente stopnje C6, za katere ni verjetno, da lahko preidejo v višjo stopnjo.

Zavezanci naj priglašajo tudi incidente stopnje C6, kjer dejanskega vpliva na omrežja, informacijske sisteme ali storitve zavezancev ni, saj se tako lahko širijo informacije o zlonamerni programski opremi, preprečuje širjenje in nastanek novih podobnih kibernetskih incidentov ter omogoča odzivnim centrom in PNO izdelava celovitih analiz stanja kibernetske varnosti v državi. V preglednici 4 so prikazani pragi obveznega poročanja.

C1	C2	C3	C4	C5	C6 – verjetnost prehoda v višjo stopnjo	C6
OBVEZNO POROČANJE					OBVEZNO POROČANJE	Prostovoljno tedensko poročanje (priporočljivo)

Preglednica 4: Prag obveznega poročanja

Časovni okvir priglasitve incidenta je pomemben tako za zavezance kot za poročanje odzivnih centrov URSIV. Vsi deležniki poročajo o stanju kibernetskega incidenta v treh stopnjah:

1. **začetno poročanje** (prva informacija) – poročanje o zaznavi kibernetskega incidenta v omrežju ali informacijskih sistemih in sprejetje prvih ukrepov;

2. **vmesno poročanje** – lahko jih je več, odvisno od trajanja incidenta. Poroča se o trenutnem stanju kibernetskega incidenta, s trenutnimi dostopnimi podatki in sprejetimi ukrepi, ter o poteku reševanja incidenta. Namenjeno tudi podajanju zahtevkov odzivnemu centru, URSIV ali drugim državnim službam za sodelovanje pri odpravi težav in sanaciji posledic;

3. **končno poročanje** – po zaključku incidenta se pripravi končno poročilo o poteku incidenta z vsemi podatki o incidentu, sprejetih ukrepih, posledicah, načrtu za sanacijo in odpravljanje posledic ter o ukrepih za preprečevanje ponovitve dogodka.

V preglednici 5 je prikazan časovni okvir poročanja zavezancev odzivnima centroma SI-CERT in SIGOV-CERT.

Stopnja incidenta	**Začetno poročanje** (od zaznave incidenta)	**Vmesno poročanje** (od zaznave incidenta)	**Končno poročanje** (po zaključenem incidentu)
C1	Nemudoma	Vsakih 6 ur	10 dni
C2		V 12 urah	5 dni
C3		V 24 urah	72 ur
C4		Po potrebi	48 ur
C5		Po potrebi	48 ur
C6	/	/	1 x tedensko

Preglednica 5: Okvir poročanja zavezancev odzivnemu centru

V preglednici 6 je prikazan časovni okvir poročanja odzivnega centra URSIV-u.

Stopnja incidenta	**Začetno poročanje** (od zaznave incidenta)	**Vmesno poročanje** (od zaznave incidenta)	**Končno poročanje** (po zaključenem incidentu)
C1	Nemudoma	Po potrebi	10 dni
C2	Nemudoma	Po potrebi	5 dni
C3	Nemudoma	Po potrebi	72 ur
C4	V 24 urah	/	1 x tedensko
C5	/	/	1 x tedensko
C6	/	/	1 x tedensko

Preglednica 6: Okvir poročanja odzivnega centra URSIV-u

4 POROČANJE O KIBERNETSKIH INCIDENTIH

Upravljanje kibernetskih incidentov je ključno za zagotavljanje visoke stopnje kibernetske varnosti. Pravilno in pravočasno odzivanje na kibernetske incidente zagotovi kolikor je mogoče minimalen vpliv kibernetskega incidenta, zmanjša posledice incidenta ter omogoči primerno odpravljanje posledic in vračanje informacijskih sistemov v običajno stanje delovanja.

4.1 Zaznava in priglasitev kibernetskega incidenta

Neželene kibernetske aktivnosti v sistemih so lahko zaznane na več načinov, pri tem je pomembno, da se pravočasno zaznajo, priglasijo in se pravilno ukrepa.

Neželene kibernetske aktivnosti lahko zaznajo:

1. zavezanec, ki zazna incident v svojih sistemih ali na podlagi informacije subjekta, s katerim poslovno ali kakor koli drugače sodeluje;
2. odzivni centri, ki s svojimi rednimi nalogami pregledovanja omrežij v skrbništvu in odkrivanja nepravilnosti zaznavajo grožnje in incidente;
3. fizične osebe ali podjetja, ki na ranljivost naletijo naključno ali v procesu odgovornega razkrivanja;
4. partnerji v okviru mednarodnega sodelovanja, ki vključuje izmenjavo informacij s partnerskimi državami, mednarodnimi organizacijami ali tujimi podjetji.

Podrobnejši načini zaznavanja neželenih kibernetskih aktivnosti je opisan v podpoglavju 5.2 tega dokumenta. Ne glede na to, kdo incident zazna in kako, morata zavezanec in odzivni center izmenjati vse podatke, ki so potrebni za primerno nadaljnje upravljanje kibernetskega incidenta.

Za pravilno upravljanje in obravnavo kibernetskega incidenta je treba imeti natančne podatke in informacije o njem. Zato mora zavezanec v prvem poročilu odzivnemu centru poslati vse podatke, ki so mu v tistem trenutku dostopni in bodo omogočili določiti primarno stopnjo incidenta ter nadaljnje ukrepe za upravljanje kibernetskega incidenta. **Zavezanec mora priglasiti kibernetski incident odzivnemu centru nemudoma, takoj po njegovi zaznavi.** Prvo informacijo o kibernetskem incidentu lahko sporoči na kakršen koli način, ki zagotavlja hitro, zanesljivo in varno pošiljanje potrebnih informacij (telefon, e-pošta, faks, kurir ipd.). **V 24 urah mora zavezanec odzivnemu centru poslati podrobno poročilo, ki mora vsebovati vse podatke iz preglednice 7, ki so v danem trenutku na voljo. Priporočeno je, da podatke pošlje na vzorčnem obrazcu (priloga E).** Pri izpolnjevanju poročila lahko sodeluje z odzivnim centrom.

V preglednici 7 so predstavljeni sestavni deli prvega poročila o kibernetskem incidentu, ki ga mora zavezanec odzivnemu centru poslati v 24 urah (priporočeno v prilogi E).

PRVE INFORMACIJE O KIBERNETSKEM INCIDENTU	
Podatki	**Vsebina**
ZADEVA	Splošni opis incidenta, s katerim bodo povezani vsi nadaljnji dokumenti v zvezi s tem incidentom.
IBS/PDS/ODU	Ime zavezanca, ki ga je kibernetski incident prizadel.
SEKTOR	Strateški sektor, v katerem deluje zavezanec (zdravstvo, energija, državna uprava in drugo).
DATUM IN ČAS NASTANKA INCIDENTA	Čim bolj natančna časovna opredelitev nastanka incidenta.
DATUM IN ČAS ZAZNAVE INCIDENTA	Čim bolj natančna časovna opredelitev, kdaj je bil incident zaznan v sistemu.

OPIS INCIDENTA	Kratek opis zaznave in trenutnega stanja v zvezi s kibernetskim incidentom.
TAKSONOMIJA (klasifikacija) INCIDENTA	Ocenjena klasifikacija in vrsta incidenta v skladu s preglednico 1.
OGROŽENA STORITEV	Navedba, katera storitev zavezanca je ogrožena.
OCENA STOPNJE NEVARNOSTI	Primarna ocena stopnje nevarnosti, ki jo pomeni incident, in kaj je morebiti ogroženo (informacijski sistem, omrežje, informacije, storitev in drugo).
OCENA MOŽNEGA VPLIVA	Primarna ocena možnega vpliva incidenta (obseg in področje) in morebitni mednarodni vpliv.
STOPNJA INCIDENTA	Glede na merila predlagana ocena stopnje kibernetskega incidenta.
OPOMBE	Zapis vseh drugih podatkov, ki bi lahko koristili v nadaljnjem upravljanju kibernetskega incidenta.

Preglednica 7: Prvo poročilo zavezanca o kibernetskem incidentu

Poleg podatkov iz preglednice 7 zavezanec sporoči odzivnemu centru tudi vse druge informacije o kibernetskem incidentu, ki jih ima v času sporočanja prve informacije na voljo in bi bile v pomoč pri upravljanju incidenta. Vsa nadaljnja komunikacija poteka glede na ocenjeno stopnjo kibernetskega incidenta in po navodilih odzivnega centra ali pristojnega nacionalnega organa. Pristojni CSIRT in PNO obravnavata incidente in podatke v skladu z ZInfV kot zaupne. Podrobnosti žrtve napada bodo razkrite samo v primeru zakonskih zahtev, v primeru podajanja varnostnih napotkov glede kibernetskega incidenta pa se oblikujejo anonimizirani tehnični zapisi, ki se delijo z javnostjo v skladu s podpoglavjem 4.5 tega dokumenta. Po dogovoru s pristojnim CSIRT in PNO se, kadar zavezanec to želi, zaradi zaščite strank ali posla lahko objavijo podrobni podatki o kibernetskem incidentu in napadenem zavezancu.

4.2 Vmesna poročila in končno poročanje

Odzivni center po prejeti prvi informaciji začne obravnavati incident in mu določi zvezno referenčno številko. Na podlagi prvega poročila opravi analizo informacij in po potrebi od zavezanca zahteva dodatne informacije. Na podlagi analize prvega poročila in z dodatnim sodelovanjem z zavezancem odzivni center določi stopnjo incidenta, ki se med upravljanjem incidenta glede na pridobljene podatke lahko spremeni.

Zavezanec glede na stopnjo incidenta in v skladu s časovnim okvirom iz preglednice 5 poroča odzivnemu centru z vmesnimi poročili in ob zaključku incidenta z zaključnim poročilom o kibernetskem incidentu. Vsebina vmesnega in končnega poročila o kibernetskem incidentu je predstavljena v preglednici 8. Priporočeno je, da vmesno in zaključno poročilo zavezanec pošlje na obrazcu iz priloge E.

VMESNO/KONČNO POROČILO O KIBERNETSKEM INCIDENTU	
Podatki	**Vsebina**
REFERENČNA ŠTEVILKA INCIDENTA	Referenčna številka kibernetskega incidenta, ki jo določi odzivni center in je vezana na vse dokumente o konkretnem kibernetskem incidentu.
ZADEVA	**Enaka kot v prvem poročilu** – splošni opis incidenta, s katerim bodo povezani vsi nadaljnji dokumenti v zvezi s tem incidentom.
IBS/PDS/ODU	Ime zavezanca, ki ga je kibernetski incident prizadel.
SEKTOR	Strateški sektor, v katerem deluje zavezanec (zdravstvo, energija, državna uprava in drugo).
DATUM IN ČAS NASTANKA INCIDENTA	Čim bolj natančna časovna opredelitev nastanka incidenta.
DATUM IN ČAS ZAZNAVE INCIDENTA	Čim bolj natančna časovna opredelitev zaznave incidenta v sistemu.
OPIS INCIDENTA	Podroben opis poteka in stanja v zvezi z njim.
NAPADENA TEHNOLOŠKA SREDSTVA	Tehnični podatki o številu in vrsti sredstev, ki jih je prizadel kibernetski incident (naslovi IP, operacijski sistemi, aplikacije, strežniki in drugo).
NEDELUJOČE/ MOTENE STORITVE	Navedba, katere storitve IBS/PDS/ODU so motene ali nedelujoče, in predvideni čas do ponovne vzpostavitve teh storitev.
VZROK INCIDENTA	Vzrok kibernetskega incidenta, če je znan (odpiranje sumljive datoteke, povezovanje naprave USB, dostop do zlonamernega spletnega mesta in drugo).
TAKSONOMIJA (klasifikacija) INCIDENTA	Klasifikacija in vrsta incidenta v skladu s preglednico 1.
OCENA STOPNJE NEVARNOSTI	Ocena stopnje nevarnosti zaradi incidenta in navedba, kaj vse je lahko ogroženo (informacijski sistem, omrežje, informacije, storitev in drugo).
OCENA MOŽNEGA VPLIVA	Vpliva incidenta (obseg in področje).
STOPNJA INCIDENTA	Glede na merila ocena stopnje kibernetskega incidenta.
ČEZMEJNI VPLIV INCIDENTA	Ali ima kibernetski incident vpliv na katero drugo državo (katero, kakšen, kolikšen).
AKCIJSKI NAČRT IN PROTIUKREPI	Do zdaj sprejeti protiukrepi za širjenje in nadaljevanje kibernetskega incidenta ter ukrepi za odpravo kibernetskega incidenta. Nadaljnji načrtovani protiukrepi in ukrepi v zvezi s kibernetskim incidentom.

ŠKODA, POVZROČENA S KIBERNETSKIM INCIDENTOM	Ocenjena materialna škoda ali škoda, povzročena imenu zavezanca.
POTREBNO ZA ODPRAVO INCIDENTA	Tehnično osebje in tehnična sredstva, ki so potrebna za odpravo incidenta in jih zavezanec neposredno nima na voljo. Predvideno število dni za odpravo kibernetskega incidenta.
ČASOVNI OKVIR ODPRAVE POSLEDIC	Ocena, koliko časa po zaključenem incidentu bo zavezanec potreboval, da bo odpravil posledice incidenta in stanje (sistemov, omrežij, storitev in drugo) povrnil nazaj v običajno, torej kot je bilo pred kibernetskim incidentom.
PRILOGE	Seznam priloženih dokumentov, ki bodo pomagali prepoznati vzrok težave ali njeno razrešitev (posnetki zaslona, datoteke z izpisi omrežnega prometa, elektronska pošta, dnevniški izpisi in drugo).
OPOMBE	Zapis vseh drugih podatkov, ki bi lahko koristili v nadaljnjem upravljanju kibernetskega incidenta.

Preglednica 8: Vmesno/končno poročilo o kibernetskem incidentu

Zavezanec pri vmesnem poročanju izpolni polja v preglednici 8, za katera ima v trenutku poročanja podatke. Druge podatke pošljejo nemudoma, ko se pridobijo, če je to nujno potrebno za pravilno upravljanje incidenta ali končno poročilo.

4.3 Obveščanje pristojnega nacionalnega organa o kibernetskem incidentu

Odzivni centri morajo o kibernetskih incidentih obveščati URSIV, ki vodi skupni seznam kibernetskih incidentov na državni ravni. O kibernetskih incidentih se URSIV obvešča v časovnem okviru glede na stopnjo incidenta v skladu s preglednico 6.

Preglednica 9 – V prvem obveščanju pristojnega nacionalnega organa o kibernetskem incidentu odzivni center sporoči podatke iz preglednice 9. Priporočljivo je, da poročanje izvede na vzorčnem obrazcu (priloga F).

PRVE INFORMACIJE O KIBERNETSKEM INCIDENTU	
Podatki	**Vsebina**
REFERENČNA ŠTEVILKA INCIDENTA	Referenčna številka kibernetskega incidenta, ki jo določi odzivni center in je vezana na vse dokumente o konkretnem kibernetskem incidentu.
ZADEVA	Splošni opis incidenta, s katerim bodo povezani vsi nadaljnji dokumenti v zvezi s tem incidentom.
IBS/PDS/ODU	Ime zavezanca, ki ga je kibernetski incident prizadel.
DATUM IN ČAS NASTANKA INCIDENTA	Čim bolj natančna časovna opredelitev nastanka incidenta.
DATUM IN ČAS ZAZNAVE INCIDENTA	Čim bolj natančna časovna opredelitev zaznave incidenta v sistemu.

STOPNJA INCIDENTA	Glede na merila predlagana ocena stopnje kibernetskega incidenta.
POTREBA ASISTENCE URSIV	Predlog morebitne potrebe po asistenci pristojnega nacionalnega organa pri upravljanju kibernetskega incidenta (kakšna in v kolikšni meri). Navedba, ali je potrebna aktivacija nekaterih državnih sestavov, služb in organov, ki bi lahko pomagali pri reševanju in odpravi posledic kibernetskega incidenta.
OPOMBE	Zapis vseh drugih podatkov, ki bi lahko koristili pri nadaljnjem upravljanju kibernetskega incidenta.

Preglednica 9: Prvo obveščanje pristojnega nacionalnega organa o kibernetskem incidentu

Ključno pri obveščanju nacionalnega pristojnega organa je, da je pravočasno seznanjen z dogajanjem v kibernetskem prostoru in o kibernetskih incidentih, da se lahko pravočasno in v potrebni meri vključi v upravljanje kibernetskega incidenta ter aktivira morebitne druge potrebne državne institucije. URSIV lahko po prejemu prve informacije od odzivnega centra po potrebi zahteva dodatne informacije o kibernetskem incidentu.

URSIV mora o incidentu stopnje C1 nemudoma obvestiti vlado in Svet za nacionalno varnost (v nadaljevanju: SNAV) ter v skladu z ZInfV tudi Policijo in NCKU. Glede na presojo ustreznih okoliščin lahko vlado, SNAV, Policijo in NCKU obvesti tudi o incidentu stopnje C2, kadar obstaja možnost, da ta preraste v incident stopnje C1.

4.4 Incident v sistemih, ki obravnavajo TAJNE podatke

O kibernetskih incidentih in napadih na informacijske sisteme, v katerih se obravnavajo tajni podatki, je treba obvestiti organ, ki je določil tajni podatek, in nacionalni varnostni organ – Urad Republike Slovenije za tajne podatke (v nadaljevanju: UVTP). Pri tem je treba dosledno upoštevati določila zakonodaje s področja varovanja tajnih podatkov.

UVTP skrbi za izvajanje mednarodnih pogodb in sprejetih mednarodnih obveznostih, ki jih je v zvezi z varovanjem tajnih podatkov sprejela ali sklenila Republika Slovenija. Tako tudi na področju kibernetske varnosti sodeluje z varnostnimi organi tujih držav in mednarodnih organizacij ter usklajuje dejavnosti za zagotavljanje varnosti slovenskih tajnih podatkov v tujini in tujih tajnih podatkov na območju Republike Slovenije. UVTP v skladu s svojimi zakonskimi pristojnostmi o kibernetskih incidentih, v katere so vpleteni tuji tajni podatki, obvesti ustrezni tuji varnostni organ države ali mednarodne organizacije.

Prag za obvezno poročanje zavezancev o kibernetskih incidentih v informacijskih sistemih, v katerih se obravnavajo tajni podatki, in časovni okvir poročanja sta enaka kot v podpoglavju 3.4.

Poročanje je obvezno za vse incidente, označene s stopnjo C5 in višje, ter za tiste incidente stopnje C6, za katere obstaja velika verjetnost, da lahko preidejo v višjo stopnjo.

Poleg sestavnih delov prvega poročila o kibernetskem incidentu je treba dodatno poslati še:
- podatke, potrebne za opredelitev tajnega podatka (opis medija, ki vsebuje tajni podatek, vključno s stopnjo tajnosti podatka, šifro in datumom dokumenta, lastnikom in kratko vsebino, prejemniki tajnega podatka),
- kratek opis okoliščin, v katerih so bili zlorabljeni tajni podatki, in če je znano, število oseb, ki so ali bi lahko imele dostop do tajnega podatka,
- podatek, ali je bil lastnik podatkov obveščen,
- podatke o postopkih in ukrepih, ki so bili izvedeni, da se prepreči nadaljnja zloraba tajnih podatkov.

Če zloraba tajnega podatka kaže na sum storitve kaznivega dejanja, je treba o tem nemudoma obvestiti Policijo ali drug pristojni organ.

Poročilo o kibernetskem incidentu ali napadu na informacijske sisteme, v katerih se obravnavajo tajni podatki, se mora označiti z ustrezno stopnjo tajnosti v skladu z Zakonom o tajnih podatkih (v nadaljevanju: ZTP). Stopnja tajnosti mora biti enaka stopnji tajnosti zlorabljenih tajnih podatkov.

4.5 Obveščanje javnosti o kibernetskem incidentu

Javnost mora biti o kibernetskem incidentu obveščena pravočasno, celovito in objektivno, na način, ki je dostopen in razumljiv vsem. Z rednim obveščanjem in komuniciranjem prispevamo k umirjenemu reševanju kriznih razmer, ozaveščanju prebivalstva in preprečevanju težjih posledic za posameznika, družbo in gospodarstvo. V ospredju mora biti dostopnost do informacij za vsakega posameznika, ne glede na socialni status ali druge okoliščine, vključujoč ranljive skupine.

Pri presoji o obsegu in načinih obveščanja javnosti je treba upoštevati načela zagotavljanja varnosti, varovanja podatkov o preiskavi incidenta, potrebe po ozaveščanju in varovanju osebnih podatkov prebivalstva ter načela preprečevanja škodovanja dobremu imenu zavezanca, ki ga je kibernetski incident prizadel. Zaradi teh razlogov je ključno, da je prvo sporočilo za javnost oziroma prva informacija, ki je poslana v javnost prek komunikacijskih kanalov, usklajena med URSIV, odzivnim centrom, ki incident obravnava, ter zavezancem, ki ga je incident prizadel.

Pri obveščanju javnosti gre lahko za obveščanje splošne javnosti po tradicionalnih in družbenih medijih za obveščanje posameznih zavezancev ali posameznega sektorja zavezancev. Posamezni zavezanci ali sektor zavezancev se obvešča predvsem zaradi preprečevanja širjenja kibernetskega incidenta ter za opozarjanje na trenutno dogajanje v kibernetskem prostoru in kibernetske incidente, ki jih morebiti lahko ogrožajo. O tem posameznega zavezanca ali sektor obveščata usklajeno URSIV in odzivni center.

V primeru obveščanja javnosti o kibernetskih incidentih se URSIV in odzivni center obvezno posvetujeta z zavezancem, pri katerem se je kibernetski incident zgodil, o tem, kako in v kolikšni meri se bo javnost obvestila, da se bo dosegel cilj primerne obveščenosti in hkrati ohranilo dobro ime zavezanca. Usklajeno obveščanje javnosti o kibernetskih incidentih se izvede zaradi naslednjih razlogov:

- obveščanje zaradi ozaveščanja in opozarjanja na pretekle incidente – gre za seznanjanje javnosti s preteklimi izkušnjami, nevarnostmi in ukrepi za preprečevanje nastanka novih kibernetskih incidentov;

- obveščanje zaradi preprečevanja stopnjevanja incidenta – gre za obveščanje javnosti o trenutnem kibernetskem incidentu, ki se že upravlja in zanj obstaja nevarnost, da preide v višjo stopnjo, kot je trenutno, na kar lahko vplivajo tudi aktivnosti javnosti v kibernetskem prostoru;

- obveščanje zaradi nevarnosti novih enakih ali podobnih dogodkov – gre za obveščanje javnosti o kibernetskem incidentu, ki se trenutno upravlja, je ustavljen oziroma je v zaključnih fazah upravljanja in zanj obstaja nevarnost, da bi se zaradi aktivnosti javnosti razširil ali ponovil še pri katerem od zavezancev.

Prvo sporočilo za javnost in vsa nadaljnja sporočila na državni ravni oblikuje in pošlje v objavo URSIV v sodelovanju z odzivnim centrom.

Z javnostjo, mediji in zavezanci o kibernetskih incidentih stopenj od C6 do C4 komunicirata odzivni center in URSIV.

O kibernetskih incidentih stopenj C3, C2 in C1 se v obveščanje javnosti poleg URSIV in odzivnega centra vključijo tudi drugi državni organi glede na svoje pristojnosti za področje kibernetskega napada.

Komunikacijske aktivnosti morajo potekati usklajeno. Vodilno vlogo prevzame Urad Vlade Republike Slovenije za komuniciranje, ki zagotavlja usklajevanje kriznega komuniciranja med ministrstvi in vladnimi službami ter opravlja naloge v skladu s svojimi pristojnostmi.

Pri obveščanju javnosti o kibernetskih incidentih stopenj C3, C2 in C1 imajo ob upoštevanju Zakona o medijih posebno vlogo mediji, ki morajo po predpisih in na zahtevo državnih organov, javnih podjetij in zavodov brez odlašanja in brezplačno objaviti nujno sporočilo v zvezi z resno ogroženostjo življenja, zdravja ali premoženja ljudi, povezano z resnim tveganjem za življenje, zdravje ali premoženje ljudi ter z ogrožanjem kulturne in naravne dediščine ter varnosti države.

V takih primerih so za takojšnje posredovanje sporočil državnih organov javnosti pristojni:
– Televizija Slovenija,
– Radio Slovenija,
– Slovenska tiskovna agencija,
– po potrebi tudi drugi mediji.

4.6 Izmenjava informacij med deležniki, ki delujejo v sistemih kibernetske varnosti na državni ravni

Izmenjava in deljenje informacij znotraj skupnosti kibernetske varnosti sta ključna za učinkovito preprečevanje in reševanje nastalih kibernetskih incidentov. Izmenjava informacij poteka na rednih sestankih koordinacijske skupine za kibernetska vprašanja, ki jo vodi URSIV. Nujne informacije, ki lahko pripomorejo k preprečitvi kibernetskega incidenta ali so v pomoč pri ozaveščanju zavezancev, lahko posamezni deležniki izmenjujejo med seboj po določenih komunikacijskih kanalih.

Deljenje informacij, ki bi kakor koli pripomogle k zagotavljanju varnosti države in preprečitvi kritičnega kibernetskega incidenta, je obvezno za vse deležnike. Koordinacijska skupina določi način in informacije, ki morajo biti nujno deljene med posameznimi deležniki v skupnosti kibernetske varnosti.

Izmenjava podatkov mora znotraj koordinacijske skupine in med deležniki na državni ravni potekati v skladu z ZTP ter zaupnostjo informacij. Podrobnosti izmenjave informacij med deležniki se določijo z dvostranskimi ali večstranskimi sporazumi med posameznimi deležniki.

SI-CERT in SIGOV-CERT znotraj mreže CSIRT informacije izmenjujeta po sistemu »Traffic Light Protocol«[4] (v nadaljevanju: TLP), ki je podrobneje opisan v prilogi G. TLP ni zakonsko zavezujoč predpis. Gre za mednarodno priporočilo industrijskega standarda, zato je primeren za uporabo pri komunikaciji v mreži CSIRT in z zavezanci ter se že uspešno uporablja.

[4] Protokol TLP je dosegljiv na povezavi https://www.first.org/tlp/.

5 UPRAVLJANJE KIBERNETSKIH INCIDENTOV

Upravljanje kibernetskih incidentov je organiziran sklop ukrepov in aktivnosti, ki so usmerjeni v čim boljšo zaščito, torej preprečevanje nastanka kibernetskih incidentov. Kadar se kibernetski incidenti kljub temu zgodijo, pa je učinkovito upravljanje ključno za čim hitrejšo obnovo omrežij, sistemov in storitev ter normalnega delovanja zavezancev.

Upravljanje kibernetskih incidentov je sestavljeno iz več faz. Za uspešno in učinkovito preprečevanje kibernetskih incidentov in odzivanje nanje je treba izvajati ukrepe v vseh fazah, vendar so nekatere faze ali posamezni ukrepi lahko vključeni kot del drugih faz ali pa so posamezne faze obravnavane hkrati. V posameznih fazah upravljanja kibernetskih incidentov so zapisane osnovne naloge, ki jih izvajajo deležniki kibernetske varnosti, vendar pa morajo biti pri določanju svojih nalog fleksibilni in jih po lastni presoji lahko razširijo.

Faze upravljanja kibernetskega incidenta so:

- PRIPRAVA (angl. *Preparatio*n)
- ZAZNAVANJE (angl. *Detection*)
- ZAMEJITEV *(*angl. *Containment)*
- UBLAŽITEV *(*angl. *Mitigation)*
- OBNOVITEV/OKREVANJE *(*angl. *Recovery)*
- FAZA ZAKLJUČKA INCIDENTA (angl. *Post incident activities*)

5.1 Faza priprav

To je faza, v kateri se deležniki kibernetske varnosti pripravljajo na neželene dogodke v kibernetskem prostoru. Za učinkovito obvladovanje kibernetskih incidentov so ključni dobra pripravljenost ter predhodna usposabljanja in urjenja v odzivanju na kibernetske incidente.

Faza priprav se izvaja pri vsakem posameznem deležniku samostojno z izdelavo načrtov odzivanja in imenovanjem pristojnih skupin za odzivanje na incidente, z nadgrajevanjem strojne opreme, posodabljanjem programske opreme, usposabljanjem zaposlenih in drugo, pa tudi v obliki skupnih priprav, ki se izvajajo z usposabljanji in kibernetskimi vajami na državni ravni, v katerih se preigravajo različni scenariji odzivanja na kibernetske incidente. Deležniki v fazi priprav izdelajo sezname oseb za stike, postopkovnike, sheme omrežij, mrežnih diagramov, sezname kritičnih sredstev, dokumentacijo operacijskih sistemov, aplikacij, protokolov, vrat, protivirusne zaščite, sistemov za zaznavanje in preprečevanje vdorov in podobno.

PREDVIDENE OSNOVNE NALOGE:

- URSIV – ozaveščanje na državni ravni, spremljanje mednarodnih sestavov in mednarodno sodelovanje (EU, Nato, ITU, OVSE, dvostranski sporazumi in drugo), posodabljanje politike državne kibernetske varnosti, usklajevanje upravljanja kibernetske varnosti in kibernetskih incidentov na državni ravni, sprejemanje ukrepov za preprečevanje kibernetskih incidentov, organizacija usposabljanj in vaj na državni ravni, sodelovanje na mednarodnih usposabljanjih in vajah ter druge naloge, ki pripomorejo k boljši pripravljenosti na kibernetske incidente.
- SI-CERT – ozaveščanje splošne javnosti in zavezancev, opozarjanje zavezancev in javnosti na ranljivosti in pretekle kibernetske incidente, tako domače kot tuje, spremljanje kibernetskih aktivnosti v državnih omrežjih (SIX), sodelovanje pri usklajevanju upravljanja kibernetske varnosti in kibernetskih incidentov, svetovanje glede ukrepov za preprečevanje kibernetskih incidentov, sodelovanje pri organizaciji usposabljanj in vaj na državni ravni, sodelovanje na mednarodnih usposabljanjih in vajah ter druge naloge, ki pripomorejo k boljši pripravljenosti na kibernetske incidente.

- SIGOV-CERT – ozaveščanje organov državne in javne uprave, opozarjanje organov državne in javne uprave na ranljivosti in pretekle kibernetske incidente, tako domače kot tuje, spremljanje kibernetskih aktivnosti v omrežjih državne in javne uprave (HKOM), sodelovanje pri usklajevanju upravljanja kibernetske varnosti in kibernetskih incidentov, svetovanje glede ukrepov za preprečevanje kibernetskih incidentov, sodelovanje pri organizaciji usposabljanj in vaj na državni ravni, sodelovanje na mednarodnih usposabljanjih in vajah ter druge naloge, ki pripomorejo k boljši pripravljenosti na kibernetske incidente.

- SOCi – ozaveščanje organov, za katere so zadolženi, opozarjanje organov, za katere so zadolženi, na ranljivosti in pretekle kibernetske incidente, tako domače kot tuje, spremljanje kibernetskih aktivnosti v omrežjih, ki jih nadzorujejo (MO, Policija, SOVA), sodelovanje pri usklajevanju upravljanja kibernetske varnosti in kibernetskih incidentov, svetovanje glede ukrepov za preprečevanje kibernetskih incidentov, sodelovanje pri organizaciji usposabljanj in vaj na državni ravni, sodelovanje na mednarodnih usposabljanjih in vajah ter druge naloge, ki pripomorejo k boljši pripravljenosti na kibernetske incidente.

- AKOS – ozaveščanje telekomunikacijskih operaterjev, opozarjanje na ranljivosti in pretekle kibernetske incidente, tako domače kot tuje, sodelovanje pri usklajevanju upravljanja kibernetske varnosti in kibernetskih incidentov ter druge naloge, ki pripomorejo k boljši pripravljenosti na kibernetske incidente.

- ZAVEZANCI – nadgrajevanje strojne in posodabljanje programske opreme, usposabljanje zaposlenih s področja kibernetske varnosti, ozaveščanje zaposlenih in obveščanje o preteklih kibernetskih incidentih, posodabljanje in usklajevanje lastnih varnostnih dokumentov v skladu z dokumenti na državni ravni, sodelovanje z URSIV in odzivnim centrom, sodelovanje na državnih in mednarodnih usposabljanjih in vajah.

V fazi priprav je ključno usklajeno sodelovanje vseh deležnikov kibernetske varnosti s ciljem dobre in uporabne operativne priprave na morebitne kibernetske incidente, ki lahko vplivajo na posameznega zavezanca ali kibernetsko varnost države. Boljše so preventivna dejavnost in priprave na področju kibernetske varnosti, boljše in lažje bo odzivanje v vseh naslednjih fazah upravljanja kibernetskih incidentov.

5.2 Faza zaznavanja

Faza zaznavanja oziroma identifikacije je faza, v kateri sta ključna pravočasno odkrivanje in prepoznavanje vseh morebitnih kibernetskih incidentov, ki lahko kakor koli škodujejo zavezancem. Pri tem je pomembno zavedanje, da niso vsi kibernetski dogodki tudi kibernetski incidenti, vendar je ključno, da se vse kibernetske aktivnosti v omrežju zaznajo in pravilno opredelijo.

Znake za pojav incidentov razvrščamo v dve skupini, »znanilce« in »kazalnike«. Znanilec je tehnični znak ali dogodek v informacijskem sistemu, da se incident lahko pripeti v prihodnosti, kazalnik pa, da se je incident zgodil ali se dogaja. Na te pojave nas lahko opozarjajo:

- sproženi alarmi (senzorji za preprečevanje in odkrivanje vdorov, zaščita pred škodljivo kodo, sistemi za analizo dnevniških datotek, programska oprema za preverjanje integritete datotek, druge naprave za spremljanje),
- dnevniške datoteke (v operacijskih sistemih, aplikacijah, omrežnih napravah in prometu),
- javno dostopne informacije (informacije o novih ranljivostih in izrabljanjih informacijskega in komunikacijskega sistema),
- osebe ali organizacije (uporabniki, sistemski in omrežni skrbniki sistema, obveščevalno-varnostni organi, druge skupine za odzivanje na računalniške in omrežne incidente).

Zaznavanje kibernetskih dogodkov in identifikacija kibernetskih incidentov temeljita na naslednjih točkah:

- zaznavanje in spremljanje aktivnosti v omrežjih, sistemih in aplikacijah,

- zbiranje situacijskih informacij in odkrivanje nepravilnosti ter zaznavanje negativnega vplivanja,
- izvedba rednega monitoringa sistema in sprotne analize stanja,
- primerne zmogljivosti za odkrivanje kibernetskih incidentov in njihovo upravljanje,
- pravočasno obveščanje odzivnih centrov o kibernetskih incidentih,
- zbiranje in varna hramba dnevniških zapisov in drugih dokazov o kibernetskem incidentu,
- izmenjevanje informacij z zavezanci znotraj sektorja za morebitno dodatno pravočasno odkrivanje enakih ali podobnih kibernetskih incidentov,
- obveščanje javnosti zaradi preprečevanja širjenja ali stopnjevanja kibernetskega incidenta.

PREDVIDENE OSNOVNE NALOGE:

- ZAVEZANCI – prek svojih zmogljivosti informacijske varnosti ali pogodbenih izvajalcev spremljajo svoja omrežja, sisteme in aplikacije ter zaznavajo vse nepravilnosti v njih, opredelitev kibernetskih incidentov ter druge naloge, ki pripomorejo k zaznavanju in identifikaciji kibernetskih incidentov.

- ODZIVNI CENTRI – s svojimi zmogljivostmi spremljajo referenčna omrežja, za katera so pristojni, in zaznavajo morebitne nepravilnosti ter o njih obveščajo zavezance, usklajeno z zavezanci zaznavajo in identificirajo morebitne kibernetske incidente, nudijo strokovno tehnično pomoč zavezancem pri upravljanju kibernetskih incidentov.

Faza zaznavanja je ključna za zavezance, saj lahko s pravočasno in uspešno zaznavo kibernetskega incidenta začnejo izvajati njegovo primerno in učinkovito upravljanje ter preostale faze upravljanja kibernetskih incidentov. Hitrejši in uspešnejši sta zaznava in identifikacija kibernetskega incidenta, boljše bo njegovo nadaljnje upravljanje ter manjše bodo njegove posledice. V tej fazi je zelo pomembno, da se vsi morebitni (digitalni) podatki v zvezi z incidentom, ki se bodo morda uporabili kot dokaz v primeru suma storitve kaznivega dejanja, ustrezno zavarujejo in varno hranijo.[5]

5.3 Faza zamejitve

Po zaznavi in identifikaciji kibernetskega incidenta je ključno njegovo omejevanje, ki pa mora že vsebovati rezultate predtem izvedene analize glede morebitnega vpliva incidenta na omrežje zavezanca in predvidenega medsektorskega vpliva. Glavna prednostna naloga v fazi omejevanja je omejiti vpliv kibernetskega incidenta na omrežja in sisteme zavezanca, preprečevati širjenje incidenta ter omejevati vpliv na storitve zavezanca.

V fazi zamejitve se opravi **prva analiza** razpoložljivih informacij o kibernetskem incidentu, izvede se primarna ocena nevarnosti in vpliva ter določita primarna stopnja kibernetskega incidenta in prednostno področje upravljanja. V fazi omejevanja se ugotavljajo tudi možni vplivi kibernetskega incidenta na poslovanje in izvajanje bistvenih storitev zavezanca ter se glede na to sprejemajo določeni ukrepi za omejevanje vpliva kibernetskega incidenta.

Omejevanje kibernetskih incidentov temelji na naslednjih točkah:
- spremljanje aktivnosti v omrežjih, sistemih in aplikacijah,
- zbiranje situacijskih informacij in odkrivanje razširjenosti kibernetskega incidenta,
- zbiranje in varna hramba dnevniških zapisov in drugih dokazov o kibernetskem incidentu,
- določanje nevarnosti, vpliva in primarne stopnje kibernetskega incidenta,
- prvo obveščanje odzivnih centrov o kibernetskih incidentih,
- izmenjevanje informacij z zavezanci znotraj sektorja za morebitno dodatno pravočasno odkrivanje enakih ali podobnih kibernetskih incidentov,
- obveščanje javnosti zaradi preprečevanja širjenja ali stopnjevanja kibernetskega incidenta.

[5] Tovrstni podatki, dokazi so nujni pri preiskovanju posameznega kibernetskega incidenta, ki ima zakonske znake kaznivega dejanja. Ustrezno zavarovanje in varna hramba teh podatkov, dokazov je aktivnost, ki se izvaja v vseh fazah upravljanja kibernetskega incidenta.

PREDVIDENE OSNOVNE NALOGE:

- ZAVEZANCI – prek svojih zmogljivosti informacijske varnosti ali pogodbenih izvajalcev spremljajo svoja omrežja, sisteme in aplikacije, začetek obravnave, primarna ocena nevarnosti in vpliva ter stopnjevanje incidenta, prvo poročanje odzivnemu centru, zavarovanje in hranjenje zapisov in dokazov o incidentu, po lastni presoji o kibernetskem incidentu obveščanje Policije ter izvajanje drugih nalog, ki pripomorejo k zamejitvi kibernetskih incidentov.

- ODZIVNI CENTRI – s svojimi zmogljivostmi spremljajo referenčna omrežja, za katera so pristojni, in zaznavajo morebitne nepravilnosti ter o njih obveščajo zavezance, nudijo strokovno tehnično pomoč zavezancem pri upravljanju kibernetskih incidentov, o kibernetskih incidentih v okviru časovnih norm za posamezno stopnjo kibernetskega incidenta obveščajo URSIV, po potrebi obveščanje javnosti.

- URSIV – sprejemanje prve informacije o kibernetskem incidentu, glede na stopnjo incidenta usklajuje njegovo upravljanje, po potrebi obvešča vlado in SNAV, pri čezmejnem vplivu kibernetskega incidenta o tem obvešča državo, na katero incident vpliva, glede na stopnjo incidenta po potrebi obvešča tudi Nacionalni center za krizno upravljanje (NCKU) in Policijo, po potrebi obveščanje javnosti.

Faza omejevanja je pomembna, saj se v tej fazi lahko preprečita širjenje incidenta, njegovo stopnjevanje in zmanjšajo posledice. Uspešnejše je omejevanje kibernetskega incidenta in njegovega vpliva, manjše bodo posledice in škoda, ki jih povzroči kibernetski incident. Faza omejevanja se običajno združi ali tesno povezuje z naslednjo fazo, fazo ublažitve.

5.4 Faza ublažitve

Faza ublažitve je **nadaljevanje ukrepov iz faze omejevanja**. Fazi omejevanja in ublažitve se običajno prekrivata in dopolnjujeta. V fazi ublažitve se izvajajo ukrepi, ki blažijo vpliv in povzročanje škode na omrežjih, sistemih in aplikacijah zavezancev. Uvedeni ukrepi so odvisni od vrste kibernetskega incidenta in bo za njihovo izvedbo morda potrebno tudi sodelovanje drugih deležnikov (na primer v primeru napada DDoS bo potrebna podpora ponudnika internetne storitve in podobno). V tej fazi je treba izvesti vse aktivnosti, ki pripomorejo k blaženju posledic incidenta, odkrivanju storilca in v nadaljevanju k preprečevanju novih incidentov.

Sprejeti ukrepi v fazi ublažitve so odvisni od vrste incidenta in nevarnosti, ki jo pomeni. Določanje ukrepov v fazi ublažitve temelji na naslednjih točkah:

- določanje vzrokov in znakov kibernetskega incidenta za določitev najučinkovitejših ukrepov,
- prepoznavanje, omejevanje ali odstranjevanje programske opreme, ki jo napadalci uporabljajo ali so jo uporabili za izvedbo kibernetskega incidenta (pri tem je ključno, da se ohrani čim več morebitnih dokazov o kibernetskem incidentu, ki bi koristili v predkazenskem postopku),
- priprava za obnovitev z zadnjo čisto varnostno kopijo podatkov (angl. *backup*),
- določitev storitev, ki so bile uporabljene med kibernetskim incidentom, saj napadalci včasih uporabijo zakonite storitve napadenega sistema.

PREDVIDENE OSNOVNE NALOGE:

- ZAVEZANCI – prek svojih zmogljivosti informacijske varnosti ali pogodbenih izvajalcev spremljajo svoja omrežja, sisteme in aplikacije, nadaljnje upravljanje incidenta, stalno ocenjevanje nevarnosti in vpliva ter stopnjevanja incidenta, vmesno poročanje odzivnemu centru, zavarovanje in hranjenje zapisov in dokazov o incidentu ter druge naloge, ki pripomorejo k ublažitvi kibernetskih incidentov.

- ODZIVNI CENTRI – s svojimi zmogljivostmi spremljajo referenčna omrežja, za katera so pristojni, in zaznavajo morebitne nepravilnosti ter o njih obveščajo zavezance, nudijo strokovno tehnično pomoč zavezancem pri upravljanju kibernetskih incidentov, o

kibernetskih incidentih v okviru časovnih norm za posamezno stopnjo kibernetskega incidenta obveščajo URSIV, po potrebi obveščanje javnosti.

- URSIV – spremljanje poročil o kibernetskem incidentu, glede na stopnjo incidenta usklajuje njegovo upravljanje, po potrebi obveščanje ustreznih deležnikov in javnosti.

Faza ublažitve je nadaljevanje faze omejevanja, torej se nadaljuje preprečevanje širjenje incidenta in njegovega stopnjevanja ter blažijo njegove posledice in morebitna povzročena škoda. Uspešnejše je blaženje kibernetskega incidenta in njegovega vpliva, manjše bodo posledice in škoda, ki jo povzroči kibernetski incident, uspešnejša pa bo tudi faza obnovitve oziroma okrevanja, ki sledi.

5.5 Faza obnovitve/okrevanja

Faza okrevanja je namenjena **vrnitvi stanja omrežij, sistemov, aplikacij ali storitev v stanje pred kibernetskim incidentom**. Ključno je, da se storitve zavezancev začnejo izvajati običajno in nemoteno za uporabnike.

Faza okrevanja se lahko izvede v različnih delih upravljanja kibernetskega incidenta, odvisno od sestava omrežij in sistemov ter njihove povezanosti z opravljanjem storitve zavezanca. Če zavezanec lahko storitev opravlja na rezervnem omrežju in izloči napadene dele, potem lahko delno okrevanje storitev izvede takoj, ko je to mogoče, in se z napadenimi sistemi ukvarja v nadaljevanju. V nasprotnem primeru je treba najprej obnoviti omrežje, sistem ali aplikacijo, ki je bila napadena, in šele nato začeti obnavljati storitve na teh sistemih.

Pomembno je, da se z obnovitvijo sistemov, ki so bili vpleteni v kibernetske incidente, ne hiti. Ključno je, da se vse faze in ukrepi izvedejo temeljito, postopno in dokončno, saj je treba zagotoviti, da so omrežja, sistemi ali aplikacije, preden so dani nazaj v uporabo, zares čisti in varni.

Omrežjem, sistemom ali aplikacijam, ki so vrnjene v uporabo, je treba nameniti posebno pozornost, prav tako kakršnim koli znakom sumljivih kibernetskih aktivnosti, ki jim je treba določiti časovno obdobje z dodatnimi ukrepi za spremljanje.

PREDVIDENE OSNOVNE NALOGE:

- ZAVEZANCI – prek svojih zmogljivosti informacijske varnosti ali pogodbenih izvajalcev spremljajo obnovljena omrežja, sisteme in aplikacije, ocenijo končni vpliv in posledice incidenta, obnovitev sistemov in vrnitev storitev zavezanca v običajno stanje ter druge naloge, ki pripomorejo k okrevanju po kibernetskih incidentih.

- ODZIVNI CENTRI – s svojimi zmogljivostmi spremljajo referenčna omrežja, za katera so pristojni, in zaznavajo morebitne nepravilnosti ter o njih obveščajo zavezance, nudijo strokovno tehnično pomoč zavezancem pri obnovitvi omrežij in sistemov.

5.6 Faza zaključka incidenta

Zadnja faza pri upravljanju kibernetskega incidenta se izvede, potem ko je kibernetski incident pod nadzorom, ko so sistemi obnovljeni in storitve povrnjene v normalno stanje. Ta faza se ne sme zanemariti, saj je ključna za učenje iz pridobljenih izkušenj iz upravljanja kibernetskih incidentov.

V tej fazi je treba **analizirati**, kaj se je zgodilo, vzroke kibernetskega incidenta, kako se je kibernetski incident razvijal med upravljanjem ter vse težave, ki so se pojavile med njegovim upravljanjem. Namen te analize upravljanja kibernetskega incidenta je učenje iz preteklih dogodkov in sprejemanje ustreznih ukrepov za preprečevanje podobnih položajev ter izboljševanje postopkov in ukrepov samega upravljanja incidenta. V tem delu se zaključna faza začne prekrivati s fazo priprav, saj se naučene izkušnje lahko vključijo v varnostno dokumentacijo, ozaveščanje, usposabljanja in vaje.

V zaključni fazi se pripravi tudi podrobno **končno poročilo o kibernetskem incidentu** (v skladu s preglednico 8), ki zajema tudi oceno škode in stroškov zaradi kibernetskega incidenta ter lahko zajema tudi priporočila ukrepov, ki jih mora zavezanec sprejeti za preprečevanje prihodnjih kibernetskih incidentov.

PREDVIDENE OSNOVNE NALOGE:

- ZAVEZANCI – izvedba podrobne analize kibernetskega incidenta in njegovega upravljanja, priprava in pošiljanje zaključnega poročila, priprava predloga ukrepov za prenovo ali nadgradnjo strojne in programske opreme, priprava predlogov prenove varnostne dokumentacije, izmenjava izkušenj o kibernetskem incidentu z odzivnim centrom in URSIV, druge naloge, ki so lahko v pomoč v fazi priprav v prihodnje.

- ODZIVNI CENTRI – nudijo strokovno tehnično pomoč zavezancem pri izvedbi analiz kibernetskega incidenta in njegovega upravljanja, sodelovanje pri pripravi končnega poročila o kibernetskem incidentu, pošiljanje zaključnega poročila pristojnemu nacionalnemu organu v skladu s časovnimi okviri, izmenjava podatkov o kibernetskem incidentu z zavezanci, po potrebi obveščanje javnosti.

- URSIV – analiza zaključnega poročila o kibernetskem incidentu, po potrebi obveščanje vlade in SNAV o zaključku in ključnih informacijah o kibernetskem incidentu, vključitev pridobljenih izkušenj v usposabljanja in vaje, mednarodna izmenjava podatkov o kibernetskem incidentu, po potrebi obveščanje javnosti.

6 ODZIVANJE NA KRITIČNE KIBERNETSKE INCIDENTE NA DRŽAVNI RAVNI

V primeru kibernetskega incidenta ali kibernetskega napada, ki ogroža varnost države ali državne sisteme, ki zagotavljajo normalno delovanje družbe in prebivalcev, je potrebno sprejemanje odločitev na najvišji strateški ravni. Zaradi tega se koordinacija upravljanja kibernetskega incidenta, ki je ocenjen kot kritični (C1 ali C2, za katerega obstaja dejanska nevarnost, da preide v C1), prenese na URSIV.

6.1 Državna raven

Za usklajevanje kibernetske varnosti na državni ravni skrbi **Koordinacijska skupina za kibernetsko varnost** (v nadaljevanju: skupina). Skupino vodi direktor URISV. Izvaja redna srečanja po potrebi, a vsaj dvakrat mesečno. V primeru izrednega dogodka je skupina sklicana na predlog direktorja URSIV. Skupino sestavljajo stalni člani in njihovi namestniki. Delo poteka na rednih in izrednih sestankih. Redni sestanki so praviloma namenjeni izmenjavi podatkov in informacij o kibernetski varnosti, usklajevanju predlogov predpisov in normativnih aktov, ki urejajo področje kibernetske varnosti v Republiki Sloveniji, usklajevanju nacionalnih letnih poročil in odgovorov na vprašalnike mednarodnih organizacij ter drugim nalogam s področja kibernetske varnosti, ki potrebujejo medresorsko usklajevanje. Izredni sestanki pa so praviloma namenjeni koordinaciji upravljanja kibernetskega incidenta.

Koordinacijska skupina lahko zaradi potreb predlaga sklic različnih ravni (tehnični, operativni, strateški člani skupine, ki obravnavajo določene zadeve v njihovi pristojnosti).

Člani in nadomestni člani koordinacijske skupine so direktor URSIV in predstavniki URSIV, SI-CERT, SIGOV-CERT, SOVE, Policije ter MO. URSIV vodi seznam članov in nadomestnih članov skupine ter ji nudi administrativno-tehnično podporo.

Direktor URSIV lahko na predlog članov skupine zaradi širšega usklajevanja določene tematike ali strateških vprašanj na sestanke povabi tudi predstavnike drugih državnih organov in služb. URSIV v skladu z drugim odstavkom 22. člena ZInfV[6] sodeluje z vsemi potrebnimi deležniki, s katerimi ocenjuje stanje ogroženosti in sprejema odločitve v zvezi z upravljanjem kibernetskega incidenta, zato v primerih kritičnega kibernetskega incidenta, ki vpliva na varnost države ali ustvarja kritične motnje na več bistvenih storitvah v državi, ali incidenta, ki ima velik medresorski vpliv, lahko direktor URSIV ob sodelovanju članov skupine poleg predstavnikov drugih državnih organov na sestanke povabi tudi predstavnike gospodarskih subjektov in raziskovalno-akademskega področja. Vabljeni subjekti v skupini predvsem pripomorejo k omejevanju posrednih vplivov kibernetskega incidenta, čim hitrejšemu nadomeščanju in ponovnemu vzpostavljanju sistema za varnost države ali motenih bistvenih storitev ter k celovitemu okrevanju po kritičnem kibernetskem incidentu ali kompleksnem kibernetskem napadu.

V času upravljanja kibernetskega incidenta ima skupina naloge predvsem v fazah ublažitve ter okrevanja in obnove, vendar ne s tehničnega vidika v omrežjih, sistemih in aplikacijah, ampak z vidika opravljanja storitev zavezancev. Tehnični vidik v fazah ublažitve in obnove omrežij, sistemov in aplikacij še vedno ostaja v rokah napadenega zavezanca, lahko pa mu skupina pri tem svetuje in pomaga.

Skupina opravlja koordinacijo upravljanja kibernetskega incidenta do povrnitve stanja v stanje pred kibernetskim incidentom oziroma do vzpostavitve in delovanja vseh ključnih bistvenih storitev v državi.

[6] 22. člen ZInfV (stanje povečane ogroženosti in ukrepanje)
(2) Pristojni nacionalni organ glede na podatke in informacije, s katerimi razpolaga, in v sodelovanju s preostalimi pristojnimi organi oceni, ali gre za stanje povečane ogroženosti iz prejšnjega odstavka.

6.2 Mednarodno sodelovanje pri odzivanju na kibernetske incidente

Pri kritičnih kibernetskih incidentih ali kibernetskih napadih večjih razsežnosti ali z vidika kibernetskih incidentov s čezmejnimi učinki ima Republika Slovenija po potrebi na voljo tudi mehanizme odzivanja in pomoči na mednarodni ravni, še posebej v okviru EU in Nata. Vladi aktivacijo mednarodne pomoči pri posamezni državi partnerici ali mednarodni organizaciji predlaga direktor URSIV. Republika Slovenija aktivacijo mednarodne pomoči izvede v skladu s predpisi in določili posamezne organizacije ali meddržavnega sporazuma.

Na strateški politični ravni ima Republika Slovenija kot država članica EU na voljo **instrumente političnega odzivanja na krize (IPCR)**, ki jih sproži z uveljavljanjem solidarnostne klavzule in **orodja kibernetske diplomacije**. To lahko vključuje tudi zaprosilo za uveljavitev usklajenega procesa pripisovanja odgovornosti za kibernetski incident ali napad, vendar to ni nujno. Odločitev za pripisovanje odgovornosti je v notranji pristojnosti držav članic EU.[7]

Mednarodna izmenjava operativnih informacij vključuje:

- EU-instrument Cyber Crisis Liaison Organisation – **CyCLOne** – odzivanje poteka s standardnimi operativnimi postopki, ki so določeni za delovanje te skupine, v kateri s svojimi predstavniki sodeluje URSIV.

- **Mreža CSIRT** – na tehnični ravni potekata mednarodno sodelovanje in izmenjava informacij pri odzivanju na kibernetske incidente ali napade po mreži CSIRT, kjer Republiko Slovenijo zastopa SI-CERT. Odzivanje poteka v skladu s standardnimi operativnimi postopki mreže.

- **Nato** – Republika Slovenija ima kot članica v okviru zavezništva na voljo različne mehanizme odzivanja na kibernetske incidente in napade. Nato prepoznava kibernetsko obrambo kot del kolektivne obrambe. Za pomoč pri odzivanju na ravni države se Republika Slovenija lahko obrne tako na zaveznice kot zavezništvo na različnih ravneh, od strateško-politične, operativne do tehnične. Mehanizmi pomoči, vključno z aktivacijo Natovih kibernetskih skupin za hitro odzivanje, so opredeljeni v memorandumu o razumevanju, ki ga ima Republika Slovenija sklenjenega z Natom in ureja sodelovanje na področju kibernetske obrambe.

[7] Na operativni ravni se v okviru EU razvija in krepi usklajeni odziv na kibernetske incidente in krize velikih razsežnosti na skupni ravni (t. i. Blueprint), ki bo omogočal pravočasno delitev informacij in situacijsko zavedanje med pristojnimi nacionalnimi organi.

7 ZAKLJUČEK

Zagotavljanje kibernetske varnosti je zapleten proces, ki zahteva veliko mero vedenja in zavedanja nevarnosti. Reševanje in odpravljanje zapletenih kibernetskih incidentov zahteva hitre in učinkovite ukrepe ter nemalokrat so v procese vključeni različni deležniki iz različnih resorjev in več ravni. Zaradi kompleksnosti procesov zaznavanja, omejevanja, blaženja ter obnovitve in ponovne vzpostavitve sistema po kibernetskem incidentu je zelo pomembno, da so ukrepi, poročanje in komuniciranje jasno opredeljeni, kar pa lahko dosežemo samo z dogovorjenimi in usklajenimi ter poenotenimi postopki.

Posamezni deležniki morajo imeti izdelane in usklajene podrobne interne načrte, ki so v skladu z Nacionalnim načrtom odzivanja na kibernetske incidente, ki predpisuje ukrepe na višjih ravneh, predvsem pa komunikacijo med deležniki. Ključno pri načrtih odzivanja je njihovo neprestano in temeljito preizkušanje prek vaj in usposabljanj, saj le tako lahko zagotovimo, da so učinkoviti in primerni za potrebe posameznih deležnikov ter državnih sestavov.

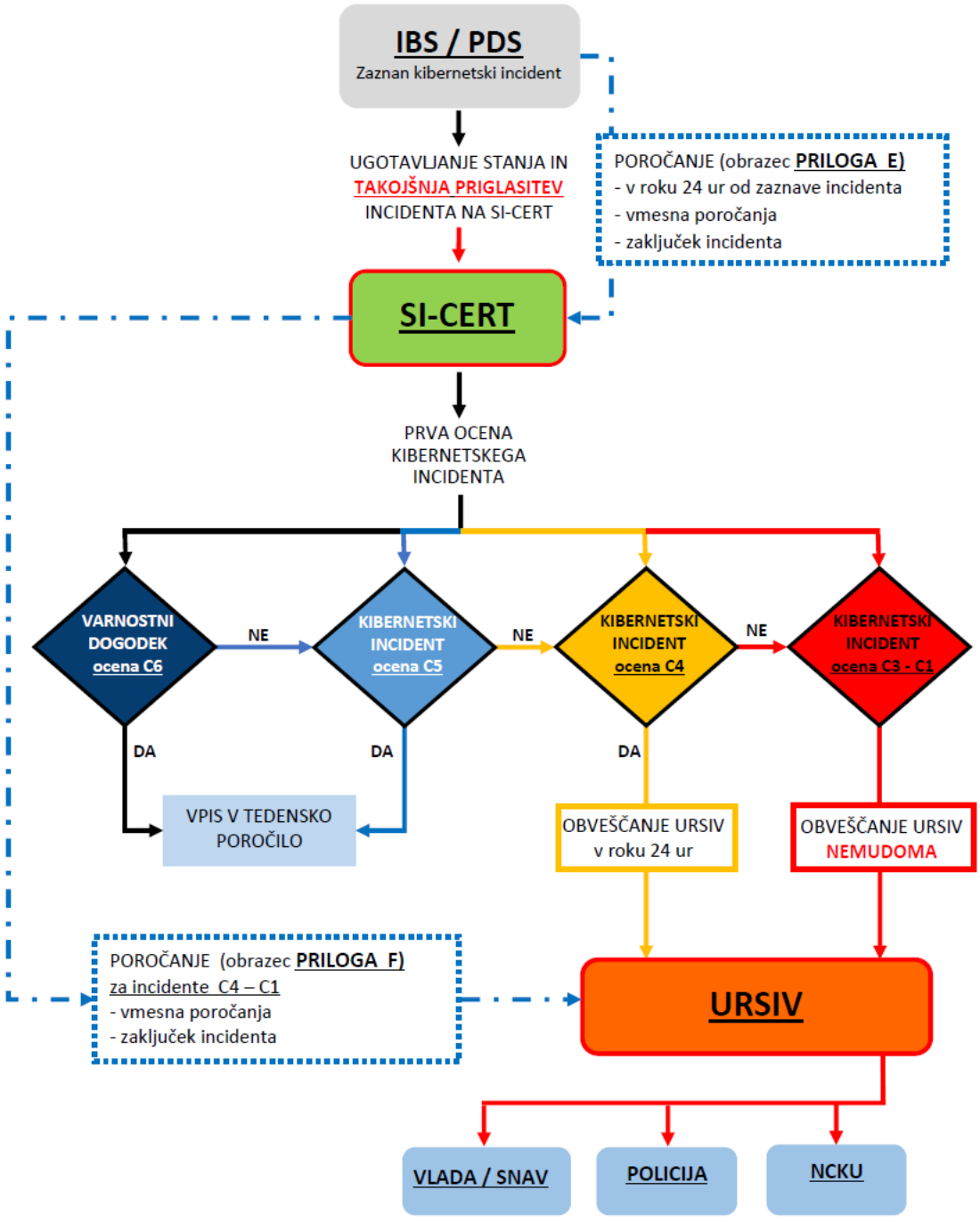
Nacionalni načrt odzivanja na kibernetske incidente je sprejet s sklepom vlade. Vlada s sklepom določi URSIV za skrbnika dokumenta in jo hkrati pooblasti, da priloge Nacionalnega načrta odzivanja na kibernetske incidente po potrebi posodablja. Obrazca za poročanje o kibernetskem incidentu (prilogi E in F) sta vzorčna obrazca, ki ju zavezanci in odzivni centri lahko uporabijo pri pošiljanju podatkov o kibernetskem incidentu. Zaradi enotnega poročanja in primerljivosti podatkov je poročanje na navedenih prilogah zaželeno in priporočljivo.

Nacionalni načrt odzivanja na kibernetske incidente je treba prilagajati novim trendom in izkušnjam, pridobljenim na podlagi upravljanja kibernetskih incidentov na državni in mednarodni ravni, spremembam mednarodnih normativnih aktov, spremembam slovenske zakonodaje ter ob upoštevanju drugih dejavnikov, ki bi lahko kakor koli vplivali na procese in postopke upravljanja kibernetskih incidentov. Revizija Nacionalnega načrta odzivanja na kibernetske incidente mora biti izvedena vsaj enkrat na tri leta.

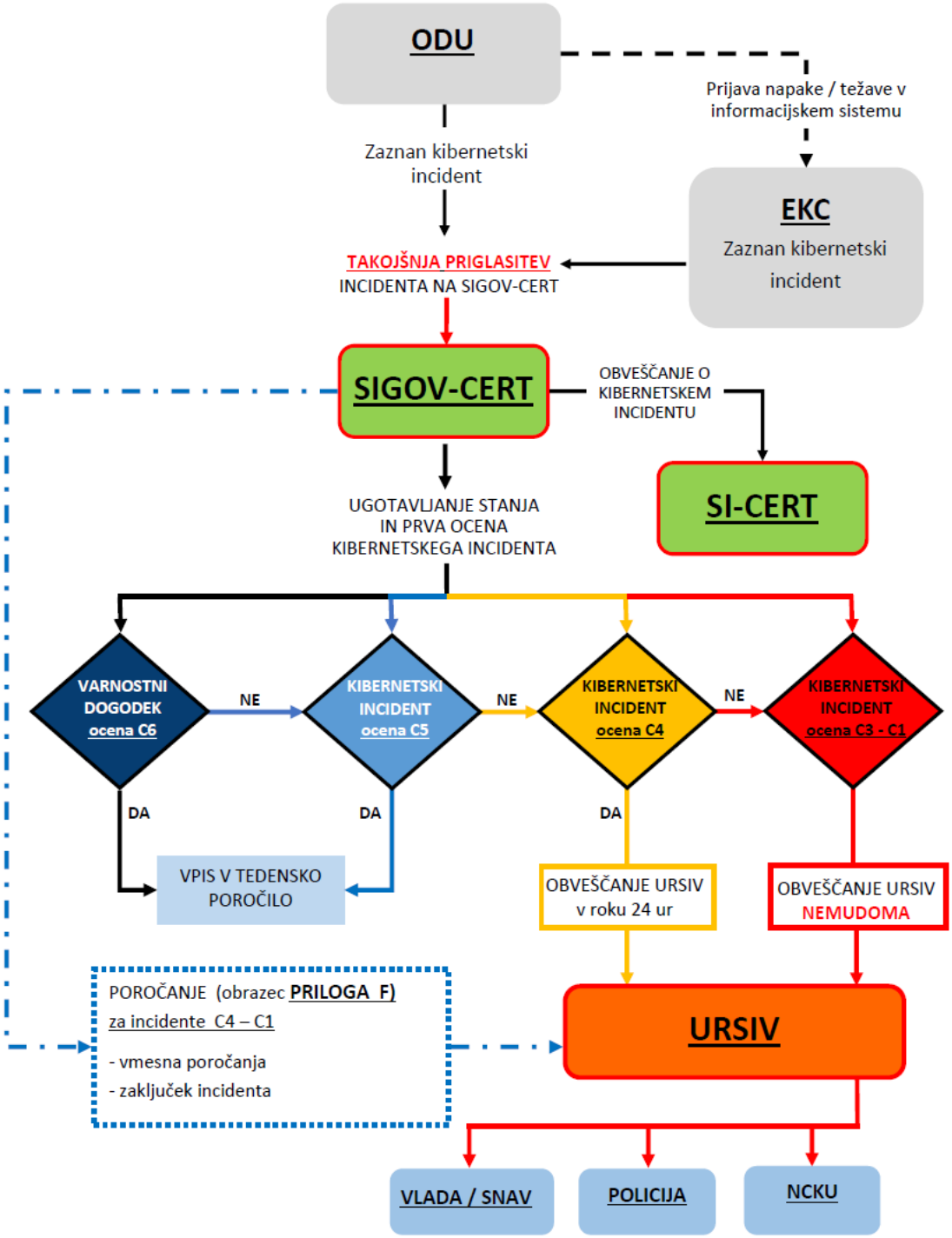
8 PRILOGE

- Priloga A – Diagram poteka poročanja IBS_PDS
- Priloga B – Diagram poteka poročanja ODU
- Priloga C – Diagram poteka poročanja SOC
- Priloga D – Diagram poteka poročanja AKOS
- Priloga E – Poročilo zavezanca o kibernetskem incidentu
- Priloga F – Prve informacije odzivnega centra o kibernetskem incidentu
- Priloga G – *Traffic Light Protocol*

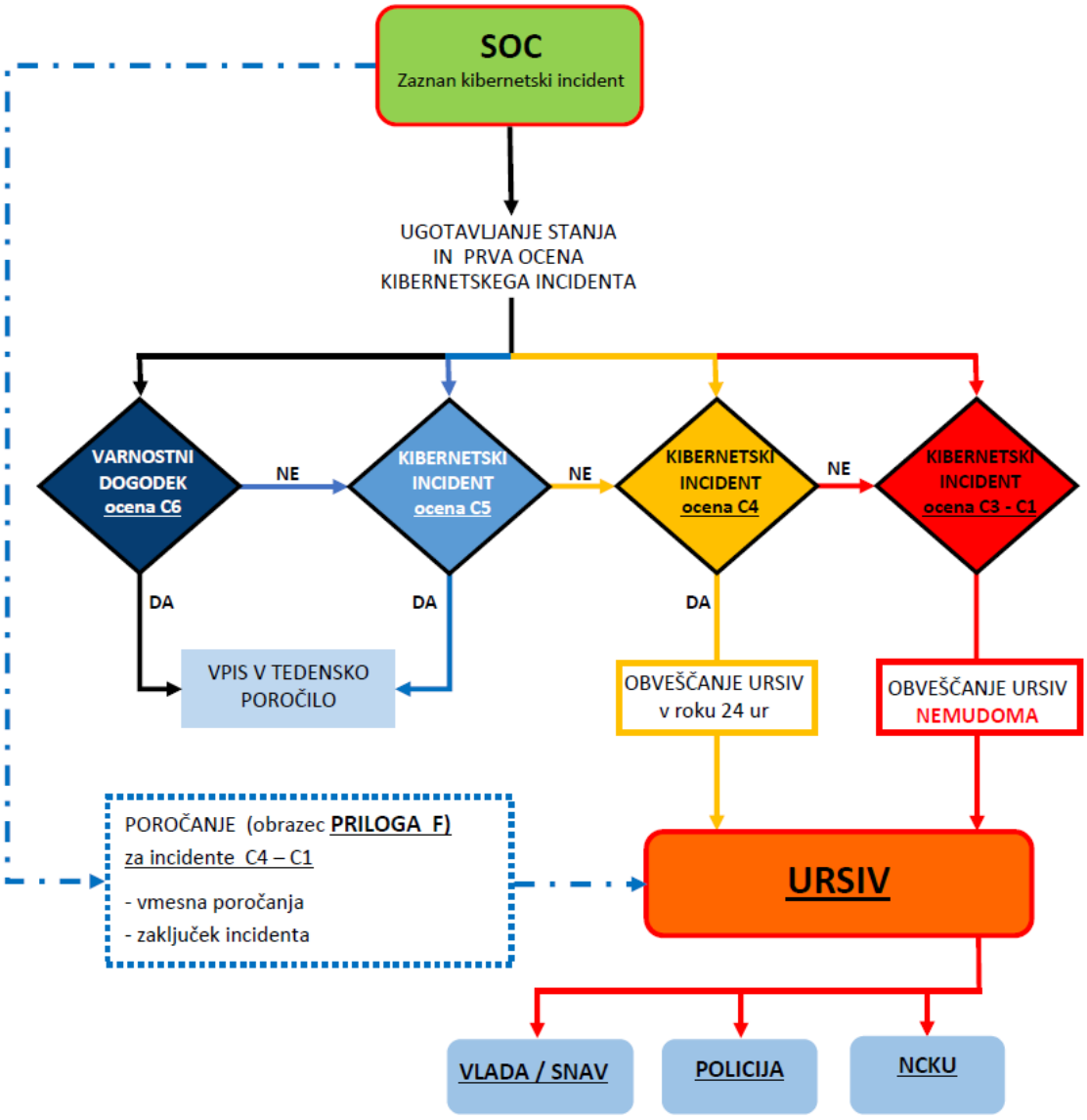
POTEK POROČANJA O KIBERNETSKEM INCIDENTU
IZVAJALCI BISTVENIH STORITEV IN PONUDNIKI DIGITALNIH STORITEV



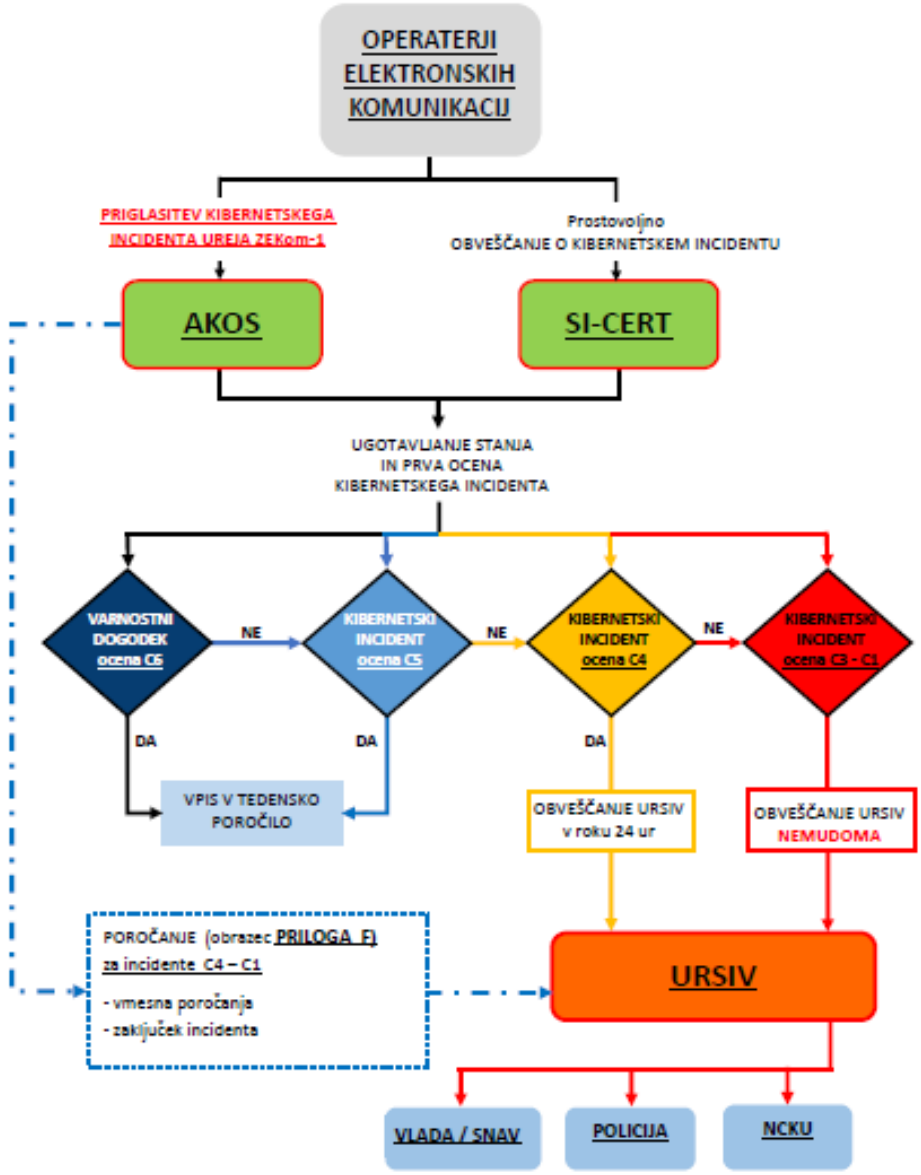
POTEK POROČANJA O KIBERNETSKEM INCIDENTU—ORGANI DRŽAVNE UPRAVE



POTEK POROČANJA O KIBERNETSKEM INCIDENTU—SOC MO, Policija, SOVA



POTEK POROČANJA O KIBERNETSKEM INCIDENTU—AKOS



OBRAZEC ZA POROČANJE O KIBERNETSKEM INCIDENTU

0. Osnovni podatki incidenta

0.1	Referenčna številka incidenta **(Določi odzivni center)**	Kliknite ali tapnite tukaj, če želite vnesti besedilo.	
0.2	Zadeva	Kliknite za zapis kratek opis incidenta.	
1.5	Poročilo	☐	Prostovoljna priglasitev incidenta
		☐	Prvo poročilo o incidentu zavezanca
		☐	Vmesno poročilo o incidentu zavezanca
		☐	Končno poročilo o incidentu zavezanca

1. Splošne informacije o poročevalcu

1.1	Naziv subjekta, ki poroča	Kliknite za vpis naziva zavezanca.	
1.2	Sektor zavezanca	Izberite sektor.	
1.3	Kontaktni podatki za tehnična vprašanja	Ime priimek, naziv.	
		Telefon.	
		E-naslov.	
1.4	Kontaktna oseba zavezanca	☐	Enaka kontaktni osebi za tehnična vprašanja.
		Ime priimek, naziv.	
		Telefon.	
		E-naslov.	

2. Začetne informacije o incidentu

2.1	Začetek / nastanek incidenta	Izberi datum.	Kliknite za vnos časa hh:mm.
	Čas zaznave incidenta v sistemu	Izberi datum.	Kliknite za vnos časa hh:mm.
2.2	Opis incidenta	Kliknite za kratek opis zaznave in trenutne situacije vezane na kibernetski incident.	
2.3	Taksonomija	Klasifikacija incidenta (prva ocena).	
2.5	Ocena stopnje nevarnosti	Primarna ocena stopnje nevarnosti.	Kliknite za dodaten opis kaj je potencialno ogroženo (sistem, informacije, storitev,…).
2.6	Ocena možnega vpliva	Primarna ocena možnega vpliva.	Kliknite za dodaten opis možnega vpliva incidenta (obseg in področje) ter potencialni mednarodni vpliv.
2.7	Ocena stopnje incident	Glede na kriterije predlagana ocena stopnje kibernetskega incidenta.	
2.8	Opombe	Zapis vseh ostalih podatkov, ki bi lahko koristili v nadaljnjem upravljanju s kibernetskim incidentom.	

3. Vmesno / končno poročanje

3.1	Poročilo		☐ Vmesno	☐ Končno
3.2	Čas zadnjega poročanja		izberite datum.	Kliknite za vnos časa hh:mm.
3.3	Trenutno stanje kibernetskega incidenta		☐ V reševanju	☐ Zaključen
3.4	Opis napake	Tehnični podatki o številu in vrsti sredstev, ki jih je prizadel kibernetski incident (naslovi IP, operacijski sistemi, aplikacije, strežniki in drugo).		
		☐ Okvara sistema	☐ Okvara strežnika	☐ Socialni inženiring
		☐ Zloraba sistema	☐ Zloraba strežnika	☐ Zloraba IP naslova
		☐ Nedelujoče aplikacije	☐ Kraja podatkov	☐ Izsiljevalski virus
		Drugo: Kliknite za vnos besedila.		
3.5	Izvor incidenta	Vzrok kibernetskega incidenta, če je znan (odpiranje sumljive datoteke, povezovanje USB naprave, dostop do zlonamernega spletnega mesta in drugo).		
		☐ USB ključ	☐ Spletno mesto	☐
		☐ Elektronsko sporočilo	☐ Zlonamerne datoteke	☐
		☐ Vdor v sistem	☐	☐
		Drugo: Kliknite za vnos besedila.		
3.6	Ogrožena storitev zavezanca	☐ Bistvena storitev ZInfV	☐ Ostale storitve	
		Katera bistvena storitev je ogrožena? Kliknite za vnos.	Katera storitev je ogrožena? Kliknite za vnos.	
3.7	Taksonomija	Klasifikacija incidenta		
3.8	Stopnja nevarnosti	Stopnja nevarnosti.	Kliknite za dodaten opis kaj je napadeno (sistem, informacije, storitev,…).	
3.9	Vpliv incidenta	Vpliv kibernetskega incidenta.	Kliknite za dodaten opis vpliva incidenta (obseg in področje) ter potencialni mednarodni vpliv.	
3.10	Stopnja incidenta	Glede na kriterije stopnje kibernetskega incidenta.	Stopnja po ZInfV Izberite element.	
3.11	Čezmejni vpliv incidenta	Ali ima kibernetski incident vpliv na katero drugo državo (katero, kakšen, kolikšen).		
		☐DA ☐NE	Kliknite za vnos – če DA, na katero državo, kako in v kolikšni meri?	
3.12	Akcijski načrt in protiukrepi	Kateri ukrepi so bili sprejeti za ustavitev širjenja in nadaljevanja kibernetskega incidenta ter kateri ukrepi za odpravo kibernetskega incidenta. Kateri protiukrepi in ukrepi so še načrtovani v nadaljevanju reševanja kibernetskega incidenta.		
		Že sprejeti ukrepi: Kliknite za vnos besedila.		
		Načrtovani ukrepi: Kliknite za vnos besedila		
3.13	Povzročena škoda	Kliknite za vnos ocene materialne škode ali škode povzročene imenu zavezanca.		
3.14	Potrebe za odpravo	Tehnično osebje in tehnična sredstva, ki so potrebna za odpravo		

	posledic	incidenta in jih zavezanec neposredno nima na razpolago. Predvideno število dni za odpravo kibernetskega incidenta.
3.15	Časovni okvir odprave posledic	Ocena koliko časa po zaključenem incidentu bo zavezanec potreboval, da bo odpravil posledice incidenta ter stanje (sistemov, omrežij, storitev,…) povrnil nazaj v običajno, kot je bilo pred kibernetskim incidentom.
3.16	Opombe	Kliknite za zapis vseh ostalih podatkov, ki niso zajeti v zgornjih točkah.
3.17	Priloge	Seznam priloženih dokumentov, ki bodo pomagali poznati vzrok težave ali njeno razrešitev (posnetki zaslona, datoteke z informacijami, elektronska pošta, logbooki in drugo).
		Kliknite za vnos besedila.

OBRAZEC ODZIVNEGA CENTRA O PRVIH INFORMACIJAH KIBERNETSKEGA INCIDENTA

0. Osnovni podatki incidenta

0.1	Referenčna številka incidenta **(Določi odzivni center)**	Referenčna št. enaka kot v poročilu zavezanca - Kliknite za vnos besedila.
0.2	Zadeva	Zadeva enaka kot v poročilu zavezanca - Kliknite za zapis kratek opis incidenta.
o.3	Naziv zavezanca, pri katerem se incident obravnava	Kliknite za vpis naziva zavezanca.

1. Začetne informacije o incidentu

1.1	Začetek / nastanek incidenta	Izberi datum.	Kliknite za vnos časa hh:mm.	
	Čas zaznave incidenta v sistemu	Izberi datum.	Kliknite za vnos časa hh:mm.	
1.2	Opis incidenta	Kliknite za kratek opis zaznave in trenutne situacije vezane na kibernetski incident.		
1.3	Ocena stopnje incident	Glede na kriterije predlagana ocena stopnje kibernetskega incidenta.		
1.4	Potrebe po asistenci	Predlog potencialne potrebe po asistenci pristojnega nacionalnega organa pri upravljanju s kibernetskim incidentom (kakšna in v kolikšni meri). Ali je potrebna aktivacija kakšnih državnih struktur, služb in organov, ki bi lahko pomagali pri reševanju in odpravi posledic kibernetskega incidenta.		
1.5	Ocenjen vpliv	Število prizadetih uporabnikov.	Ocenjena povzročena škoda.	Trajanje motenj na storitvah zavezanca.
1.6	Opombe	Zapis vseh ostalih podatkov, ki bi lahko koristili v nadaljnjem upravljanju s kibernetskim incidentom.		

TRAFFIC LIGHT PROTOCOL -TLP		
BARVA	**KDAJ NAJ BO UPORABLJEN**	**KAKO LAHKO DELIMO INFORMACIJE**
TLP – RED Ni za razkritje, omejeno samo za udeležence	Vir informacije lahko uporabi TLP – RED, kadar na informacije ni mogoče učinkovito ukrepati in lahko, če se zlorabijo, vplivajo na zasebnost, ugled ali delovanje stranke.	Prejemniki ne smejo deliti informacij TLP – RED z udeleženci zunaj določene izmenjave, sestanka ali pogovora, v katerem so bile prvotno razkrite. Na primer v okviru sestanka so informacije TLP – RED omejene na tiste, ki so prisotni na sestanku. V večini okoliščin je treba TLP – RED izmenjati ustno ali osebno.
TLP – AMBER Omejeno razkritje, omejeno na organizacije udeležencev.	Vir informacije lahko uporabi TLP – AMBER, kadar informacije zahtevajo učinkovito ukrepanje, vendar to prinaša tveganja za zasebnost, ugled ali delovanje, če se informacije delijo izven vpletenih organizacij.	Prejemniki lahko podatke TLP – AMBER delijo samo s člani svoje organizacije in s strankami, ki morajo poznati informacije, da se lahko zaščitijo ali preprečijo nadaljnjo škodo. Viri lahko določijo dodatne predvidene omejitve skupne rabe informacij, ki jih je potrebno upoštevati.
TLP – GREEN Omejeno razkritje, omejeno na skupnost.	Vir informacij lahko uporabi TLP - GREEN, kadar so informacije koristne za ozaveščanje vseh sodelujočih organizacij, pa tudi z vrstniki v širši skupnosti ali sektorju.	Prejemniki lahko delijo informacije TLP – GREEN z vrstniki in partnerskimi organizacijami znotraj svojega sektorja ali skupnosti, vendar ne prek javno dostopnih kanalov. Informacije v tej kategoriji se lahko v določeni skupnosti široko širijo. TLP – GREEN informacije morda ne bodo objavljene zunaj skupnosti.
TLP – WHITE Razkritje ni omejeno.	Vir informacij lahko uporabi TLP – WHITE, kadar informacije predstavljajo minimalno ali nepredvidljivo tveganje zlorabe, v skladu z veljavnimi pravili in postopki za javno objavo.	V skladu s standardnimi pravili o avtorskih pravicah se lahko TLP – WHITE podatki distribuirajo brez omejitev.