REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE
ZA INFORMACIJSKO VARNOST

URSIV

NAČRT ZA OKREVANJE IN ODPORNOST

Financira Evropska unija
NextGenerationEU

NAČRT ODZIVANJA NA INCIDENTE S PROTOKOLOM OBVEŠČANJA PRISTOJNE CSIRT SKUPINE – vzorčna dokumentacija

Različica:	1.0
Datum veljavnosti:	
Avtor:	
Odobril:	

November 2025

Uvodna pojasnila

Ta dokument predstavlja vzorčno predlogo za pripravo dokumenta »Načrt odzivanja na incidente s protokolom obveščanja pristojne skupine CSIRT« iz 6. točke prvega odstavka 21. člena Zakona o informacijski varnosti (Uradni list RS, št. 40/25; v nadaljevanju: ZInfV-1). Dokument je generičen in je namenjen izključno kot pomoč pri doseganju skladnosti predvsem malim in srednje velikim organizacijam v Republiki Sloveniji (do približno 200 uporabnikov oziroma naprav), ki morajo izpolnjevati zahteve iz ZInfV-1[1].

Dokument ni univerzalna rešitev, temveč izhodiščni okvir, ki ga mora vsaka organizacija obvezno prilagoditi svojemu dejanskemu stanju informacijsko-komunikacijske infrastrukture, posebnostim sektorja (npr. zdravstvo, finance, energetika, javna uprava), obsegu poslovanja ter morebitnim dodatnim zahtevam ali priporočilom pristojne CSIRT skupine. Ta dokument je zato treba razumeti kot osnovo oziroma ogrodje, ki ga je treba dopolniti s konkretnimi podatki organizacije (kontakti, notranjimi sistemi, dejanskimi postopki), da bo v primeru incidenta omogočal hitro, usklajeno in uspešno ukrepanje.

Pri pripravi tega dokumenta organizacija preveri in ustrezno upošteva najmanj: seznam dejansko uporabljenih varnostnih orodij (npr. SIEM, EDR, IDS/IPS, centralni logi idr.); kontaktne podatke pristojne CSIRT skupine in način priglasitve incidentov; sektorsko specifične vrste incidentov in grožnje; pogodbeno dogovorjene obveznosti z dobavitelji in (poslovnimi) partnerji ter uporabo storitev SOC operacije (ang. *Security Operations Center* oz. *MSSP/SOC-as-a-Service*) oziroma stalnega varnostnega monitoringa omrežnega prometa, dejavnosti končnih naprav, dnevniških zapisov, identitet in ranljivosti.

Po ustrezni prilagoditvi dokument podpiše oziroma potrdi vodstvo organizacije, pregleda in preizkusi pa ga vsaj enkrat letno ali po vsakem pomembnem incidentu, pomembnih spremembah v informacijsko-komunikacijski infrastrukturi, pomembnih spremembah organiziranosti ali procesov ali spremembi zakonodaje. Le tako organizacija zagotavlja uspešen in pravno skladen odziv na kibernetske incidente.

Zelo priporočena je vzpostavitev lastnih ali pogodbenih SOC zmogljivosti. Za manjše ali srednje velike organizacije je to najučinkovitejši način za zagotovitev neprekinjenega spremljanja, pravočasnega zaznavanja in hitrega odziva, ki ga ZInfV-1 oziroma Izvedbena uredba Komisije (EU) št. št. 2024/2690 izrecno zahtevata.

Uporabljeni viri:

- *Zakon o informacijski varnosti (Uradni list RS, št. 40/25);*
- *Izvedbena uredba Komisije (EU) 2024/2690, z dne 17. oktobra 2024, o določitvi pravil za uporabo Direktive (EU) 2022/2555 v zvezi s tehničnimi in metodološkimi zahtevami ukrepov za obvladovanje tveganj za kibernetsko varnost ter podrobnejšo opredelitvijo primerov, v katerih se incident šteje za pomembnega, kar zadeva ponudnike storitev DNS, registre TLD imen, ponudnike storitev računalništva v oblaku, ponudnike storitev podatkovnega centra, ponudnike omrežij za dostavo vsebin, ponudnike upravljanih storitev, ponudnike upravljanih varnostnih storitev, ponudnike spletnih tržnic, spletnih iskalnikov in platform za storitve družbenega mreženja ter ponudnike storitev zaupanja (Uradni list EU, L 2024/2690);*
- *Standard ISO/IEC 27001:2022;*
- *Strokovni okvir NIST Cybersecurity Framework (CSF);*
- *Technical Implementation Guidance on Cybersecurity Risk Management Measures, ENISA, junij 2025.*[2]

[1] Zavezanci iz ZInfV-1, ki so ponudniki storitev DNS, registri TLD imen, ponudniki storitev računalništva v oblaku, ponudniki storitev podatkovnega centra, ponudniki omrežij za dostavo vsebin, ponudniki upravljanih storitev, ponudniki upravljanih varnostnih storitev, ponudniki spletnih tržnic, spletnih iskalnikov in platform za storitve družbenega mreženja ter ponudniki storitev zaupanja, morajo pri pripravi tega dokumenta upoštevati določbe Izvedbene uredbe Komisije (EU) št. 2024/2690, z dne 17. oktobra 2024.

2 (https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf

KAZALO

1. Namen in področje uporabe

Ta dokument določa vloge, odgovornosti in postopke za pravočasno odkrivanje, analiziranje, omejevanje in dokumentiranje kibernetskih incidentov, odzivanje nanje ter obveščanje poročanje o njih.

Dokument vsebuje tudi opis sistema za zaznavo in odziv na incidente, ki vključuje orodja za spremljanje in vodenje dnevniških zapisov v svojih omrežnih in informacijskih sistemih za odkrivanje varnostnih dogodkov, ki bi se lahko šteli za incidente.

Velja za vse zaposlene, pogodbenike in dobavitelje, ki upravljajo, obdelujejo ali dostopajo do informacijskih sredstev organizacije.

Vloge, odgovornosti in postopki, določeni v tem dokumentu, se preskusijo in pregledajo ter posodobijo v načrtovanih časovnih presledkih in po pomembnih incidentih ali v primeru nastalih pomembnih sprememb v omrežnih in informacijskih sistemih ali ob pomembnih spremembah tveganj.

2. Opredelitev varnostnega dogodka, incidenta in pomembnega incidenta

Varnostni dogodek je zaznan poskus ali sum na aktivnost, ki bi lahko vplivala na razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov.

Incident je dogodek, ki je ogrozil razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali storitev, ki jih omrežni in informacijski sistemi zagotavljajo ali so prek njih dostopni.

Pomemben incident je incident, ki je organizaciji povzročil ali bi lahko povzročil resne operativne motnje pri opravljanju storitev ali finančne izgube ali je vplival ali bi lahko vplival na druge fizične ali pravne osebe s povzročitvijo precejšnje premoženjske ali nepremoženjske škode.[3]

3. Sistem za zaznavo in odziv na incidente ter postopki[4]

Organizacija uporablja naslednje sisteme in postopke za zaznavo in odziv na incidente:

- **Sistem za zaznavo / preprečevanje vdorov (IDS[5] /IPS[6] / NDR[7] / FW[8]):** Neprekinjeno spremljanje omrežnega prometa in odkrivanje / preprečevanje sumljivih dejavnosti.

[3] Ko gre za zavezanca, za katerega velja Izvedbena uredba Komisije (EU) 2024/2690, z dne 17. oktobra 2024 je potrebno upoštevati in navesti definicije pomembnega incidenta iz izvedbene uredbe, glede na vrsto zavezanca.
Prag za določitev pomembnega incidenta za zavezance, za katere ne velja izvedbena uredba Komisije izhaja iz analize vplivov na poslovanje in analize obvladovanja tveganj.
[4] Organizacija navede, katere sisteme za zaznavo in odziv na incidente uporablja.
[5] IDS – Intrusion Detection System - sistem za zaznavanje vdorov (prepoznava sumljive ali zlonamerne aktivnosti v omrežju ali sistemih).
[6] IPS – Intrusion Prevention System - sistem za preprečevanje vdorov (poleg zaznavanja lahko avtomatsko blokira napade).
[7] NDR – Network Detection Response - Rešitev za napredno zaznavanje in odziv na grožnje v omrežju, pogosto z analitiko in avtomatizacijo.
[8] FW – Firewall - varnostna pregrada, ki nadzoruje in filtrira omrežni promet glede na pravila.

Postopki ob incidentu: SIEM korelira opozorila; ob potrditvi incidenta se izvozi »*alert log*« s surovimi podatki[9] in trenutna konfiguracija / pravila varnostnih sistemov; po potrebi se začasno prilagodi politika oziroma pravila.

- **Sistem za upravljanje informacij in dogodkov varnosti (SIEM):** Centralno zbiranje in analiza varnostnih dogodkov iz različnih virov; korelacija in časovnice za hitro odkrivanje incidentov.

  Postopki ob incidentu: sprožijo se postopki za ohranjanje forenzičnih dokazil (po potrebi dvig retencije, označitev virov »*do not purge«, zavarovanje dokazov*), zaklene se »case« in izvozi časovnica ter korelacijsko poročilo; primer se poveže z ID zadeve v »ticketing sistemu« oziroma sistemu za upravljanje zahtevkov. Uporabi se nastavitve za zagotovitev integritete dokazil.

- **Sistem za centralizirano zbiranje dnevnikov (če ni vzpostavljenega SIEM):** Centralno sprejemanje in hramba dnevniških zapisov iz strežnikov, omrežnih naprav in aplikacij. Omogoča iskanje, osnovno korelacijo in pripravo časovnic za potrebe preiskave in poročanja CSIRT.

  Postopki ob incidentu: vklopi se »*log freeze/retention bump*« na prizadetih virih; izvozi se zadnje in rotirane[10] datoteke dnevniških zapisov ter ustvari »*immutable*« kopija (*WORM / append-only*); preveri se integriteta (SHA-256/512) in časovno žigosanje; izvede se ročno / skriptno združevanje za predvideno časovnico; arhivira se konfiguracija dnevniškega strežnika in seznam aktivnih virov (aktivnih procesov strežnika); preveri se TLS protokol za pošiljanje dnevniških zapisov in veljavnost certifikatov, da se oceni možnost morebitnega poseganja v celovitost in avtentičnost dnevniških zapisov.

- **Sistem za upravljanje ranljivosti:** Redno skeniranje in odpravljanje ranljivosti v informacijskih sredstvih kot kontekst za oceno možnosti izkoriščanja ranljivosti.

  Postopki ob incidentu: izvozi se zadnje in predzadnje poročilo skeniranj prizadetih sredstev; označi se »*legal hold*« nad relevantnimi poročili; pripravi se »*CVE/CWE«* preslikava in načrt odprave.

- **Sistem za zaznavo in odziv na končnih točkah (EDR):** Spremljanje in analiza dejavnosti na končnih točkah za odkrivanje groženj in odzivanje nanje.

  Postopki ob incidentu: izvede se izolacija naprav (končnih točk) (»*network containment«*) po odobritvi vodje informacijske varnosti; zajame se triažni paket (procesi, povezave, avto-prilagoditve, izvlečki dnevniških zapisov) in po potrebi RAM/disk (forenzično slikanje) z uporabo t. i. »*write-blockerjev«,* ki preprečijo spremembe RAM/disk zapisa med zajemanjem triažnega paketa, da se ohrani celovitost.

- **Sistem za vodenje zahtevkov** (angl. *ticketing system*): Centralizirano orodje za evidentiranje, razvrščanje, dodeljevanje in sledenje incidentom ter povezanim nalogam, z revizijsko sledjo (skrb za enolični ID incidenta).

[9] Če je možno se izvede še usmerjeni PCAP zajem na prizadetih segmentih.
[10] Rotirane datoteke (ang. *rotated log files*) so starejše kopije dnevniških zapisov, ki jih je sistem samodejno preimenoval, stisnil ali premaknil, ko je glavna aktivna »*log*« datoteka dosegla določeno velikost ali starost.

Postopki ob incidentu: odpre se zadeva, določi odzivne čase; v zadevo se poveže »*Evidence Manifest*« in vse artefakte in odobritve (npr. izolacija, izklop storitev, delitev dokazov) se vodijo prek »*workflow-a*«.)

- **Sistem za obveščanje uporabnikov:** Mehanizmi za prijavo sumljivih dejavnosti s strani uporabnikov (npr. *phishing* gumb, portal, e-pošta) in za obveščanje uporabnikov o ukrepih / incidentih.

  Postopki ob incidentu: prijave se pretvorijo v »*ticket*« (*tier-1*); originalne e-pošte se hranijo kot .eml/.msg z vsemi zaglavji; kopije poslanih obvestil, potrditve o pošiljanju in vsebine statusnih strani se arhivirajo s časovnimi žigi.

4. Vloge in odgovornosti

- **Vodja informacijske varnosti:** Skrbi za celoten proces odzivanja na incidente in komunikacijo s CSIRT, vodstvom organizacije in ostalimi deležniki.
- **Vodstvo organizacije:** Določa notranjo komunikacijo, komunikacijo s CSIRT skupino in komunikacijo z javnostjo.
- **Varnostna ekipa**[11]**:** Izvaja tehnične ukrepe za obvladovanje incidentov.
- **IT oddelek:** Podpira obnovo sistemov in implementacijo varnostnih popravkov.
- **Uporabniki:** Prijavljajo sumljive dejavnosti in sodelujejo pri preprečevanju incidentov.

5. Skupina za odziv na incidente

Organizacija ima določeno skupino za odziv na incidente informacijske varnosti s potrebnimi znanji in kompetencami. Člane skupine imenuje vodstvo organizacije s sklepom. V skupino so lahko vključeni zaposleni in (po potrebi) pogodbeni izvajalci. Stalni član skupine za odziv na incidente je vodja informacijske varnosti.

6. Postopek odzivanja na incidente

6.1 Zaznava in prijava incidenta

Ob zaznavi varnostnega dogodka ali incidenta mora sistem (samodejno) ali zaposleni ali pogodbeni izvajalec, ki za organizacijo opravlja storitve informacijske podpore, storitve povezane z informacijsko varnostjo ali storitve upravljanja s strojno opremo, prijaviti dogodek oziroma incident na elektronski naslov: *info@organizacija.si*. Prijava mora vsebovati najmanj naslednje podatke:

- podatke o prijavitelju;
- datum in čas zaznave;
- vpletene sisteme (aplikacija, sistem, omrežje) ali uporabnike;

[11] Varnostno ekipo sestavljajo vnaprej določeni lastni strokovnjaki ali pogodbeni izvajalci ali je ekipa mešana (lastni strokovnjaki in pogodbeni izvajalci).

- opis incidenta in nastale posledice in
- prve ukrepe, ki so bili sprejeti.

6.2 Ocena in klasifikacija resnosti incidenta

Varnostna ekipa oziroma vodja informacijske varnosti oceni resnost incidenta glede na:

- obseg in vpliv na storitve;
- vrsto grožnje in
- možnost širjenja.

Incidenti se razvrstijo v štiri kategorije oziroma stopnje glede na resnost incidenta in sicer: S1 (kritično), S2 (visoko), S3 (srednje) in S4 (nizko). Pri tem se **stopnja S1 in S2 štejeta in obravnavata kot pomemben incident**. Na podlagi razvrstitve se določijo in izvedejo nadaljnji ukrepi, obveščanja in poročanja.

Tabela razvrstitve glede na resnost in odzivni časi (dogodek, incident in pomemben incident)

Stopnja	Opis/merila	Primeri/posledice	Začetni odzivni čas
S1 – Kritično	Velik neposreden negativni vpliv na delovanje kritičnih storitev; velika verjetnost velike poslovne škode, ki lahko ogrozi preživetje organizacije; veliko tveganje za upad ugleda organizacije; velik čezmejni vpliv	Izsiljevalska programska koda na ključnih sistemih z izpadom storitev; kompromitacija privilegiranega AD / IdP; kompromitacija osebnih podatkov velikega obsega ali poslovnih skrivnosti; delna ali popolna degradacija storitev - dlje časa prekinjeno napajanje, daljši čas prekinjene povezave.	15 min
S2 – Visoko	Motnje ali pomembna degradacija storitev; možno širjenje; nastanek večje poslovne škode z še obvladljivimi posledicami za poslovanje organizacije; odtujeni pomembni podatki	Privilegiran dostop napadalca; aktivna eksfiltracija (odtekanje) podatkov; DDoS napad na ključno aplikacijo s pomembno degradacijo storitev; kritična ranljivost na sistemu z znaki izrabe; motnje v delovanju storitev - prekinjeno napajanje, prekinjene povezave).	30 min
S3 – Srednje	Omejen vpliv, nadzorovano širjenje, poslovna škoda je kratkoročna in sprejemljiva	Posamezna okužba končne točke brez vpliva na storitev; posamezen kompromitiran račun brez eksfiltracije; uspešen *phishing* posameznika brez posledic; napaka konfiguracije z nizkim tveganjem; minimalne motnje v delovanju storitev.	4 h
S4 – Nizko	Dogodki z minimalnim tveganjem, ki nimajo pomembnega vpliva na poslovanje organizacije	Lažno pozitivno SIEM opozorilo; poskusi napada brez uspeha; pravočasno izvedene aktivnosti za zamejevanje; brez motenj v delovanju storitev.	1 delovni dan

Pri razvrščanju oziroma vrednotenju pomembnosti incidenta se upošteva še dejanska prizadetost omrežnih in informacijskih sistemov, zlasti njihov pomen pri zagotavljanju (ključnih) storitev subjekta, resnost in tehnične značilnosti kibernetske grožnje in njenega vpliva na uporabnike in poslovno stabilnost organizacije, ranljivosti, ki se izkoriščajo, in pretekle izkušnje subjekta s podobnimi incidenti. Kadar je razvrščanje oziroma vrednotenje pomembnosti incidenta na mejnih vrednostih meril, se za vrednotenje upošteva višja stopnja.

6.3 Obvladovanje incidenta

Glede na razvrstitev incidenta se izvedejo naslednji ukrepi:

- izolacija prizadetih sistemov;

- zbiranje dokazov za analizo;
- odprava vzroka incidenta in
- obnovitev sistemov in storitev.

V postopkih obvladovanja in odzivanja na incidente, se najprej izvede odstranitev / izolacija prizadetih naprav iz omrežja oziroma se izolira omrežni segment informacijskega sistema ali storitve, ki je pri incidentu prizadeta in se takoj pristopi k omejitvi širjenja posledic.

V postopkih odziva na incidente se dokumentirajo vse izvedene aktivnosti v dnevnik dejavnosti odzivanja na incidente, zbirajo in dokumentirajo se artefakti ter zbirajo in pregledujejo dnevniki v zvezi z vsemi nenavadnimi ali neželenimi trendi (varne kopije in zgoščene vrednosti). V aktivnosti se vključi posameznike, pogodbene izvajalce ali ustrezne zunanje institucije, ki lahko s svojim znanjem in veščinami pripomorejo k vzpostavitvi nemotenega poslovanja.

Pri odpravi vzrokov za incident se ugotavlja vektor napada in odpravljajo vzroki za njegov nastanek ter odpravijo vse posledice, ki jih je povzročil incident. Odpraviti je potrebno vse varnostne vrzeli in ranljivosti, ki so bile izkoriščene za njegovo širitev.

V postopkih obnovitve sistemov in storitev se zagotovi odpravo in sanacijo vseh posledic incidenta za nadaljevanje normalnega delovanja omrežij in informacijskih sistemov oziroma storitev organizacije.

7. Obveščanje in poročanje o incidentih

7.1 Postopek obveščanja in poročanja o pomembnem incidentu

V primeru pojava **pomembnega incidenta** se nemudoma, najkasneje pa **v roku 24** ur obvesti vodstvo organizacije in pristojna CSIRT skupina (zgodnje sporočilo). Obvestilo mora vsebovati najmanj:

- opis incidenta;
- datum in čas zaznave;
- ukrepe, ki so bili sprejeti;
- oceno vpliva na storitve;
- kontaktne podatke odgovorne osebe;
- ali je potrebna pomoč CSIRT skupine in
- morebitne druga pomembna dejstva in okoliščine povezane z incidentom.

Če je potrebna pomoč CSIRT skupine se v zgodnjem sporočilu pošljejo še naslednji podatki, če so na voljo: vzorci škodljive kode, izvirniki e-sporočil, dnevniški zapisi požarnih pregrad, dnevniški zapisi prizadetih sistemov, ipd.

Če obstajajo razlogi za sum, da je bil incident povzročen s protipravnim ravnanjem posameznika je potrebno nemudoma, najkasneje pa v roku 24 ur obvestiti policijo.

Kadar incident vpliva ali lahko imel vpliv na podatke, storitve ali integracije poslovnih partnerjev ali ključnih strank ali ko tako zahteva pogodba ali je to zakonska zahteva (npr. kompromitacija

API ključev[12], SSO[13] / IdP[14] zaupanja, skupna oblačna okolja, izvoz podatkov, dobaviteljska veriga) je potrebno o incidentu obvestiti zadevne poslovne partnerje in ključne stranke. Obvestilo vsebuje najmanj naslednje podatke:

- povzetek incidenta/grožnje, časovni okvir in prizadete komponente;
- kako so lahko prizadeti podatki/sistemi poslovnega partnerja (obseg, vrste podatkov);
- priporočeni takojšnji ukrepi za poslovnega partnerja (npr. rotacija poverilnic / API ključev, blokada IP[15] naslova / IoC[16], preverbe dnevnikov, posodobitve) in
- zaupnost in navodila za ravnanje z obvestilom.

Čim prej, najpozneje pa v 72 urah po zaznavi pomembnega incidenta se izvede priglasitev incidenta pristojni CSIRT skupini, v kateri se po potrebi posodobijo informacije iz zgodnjega sporočila in se navede začetna ocena pomembnega incidenta, vključno z njegovo resnostjo in vplivom ter kazalniki ogroženosti / zlorabe (ang. *IoC - Indicators of Compromise*), kadar so ti znani.

V primeru incidentov, ki vplivajo na zaupnost, celovitost, razpoložljivost ali avtentičnost osebnih podatkov, je o incidentu potrebno takoj obvestiti pooblaščenca za varstvo podatkov (DPO) v organizaciji, ki skladno s svojimi pristojnostmi in veljavnimi predpisi izvede potrebne ukrepe in obveščanja pristojnih organov.

Na zahtevo CSIRT skupine se pošlje v najkrajšem možnem času vmesno poročilo o novih znanih dejstvih in okoliščinah pomembnega incidenta in trenutnemu stanju in izvedenih odzivnih aktivnostih.

Najkasneje v enem mesecu po zaznavi pomembnega incidenta se pristojni CSIRT skupini pošlje končno poročilo o pomembnem incidentu, ki vključuje najmanj naslednje podatke:

- podroben opis incidenta, vključno z njegovo resnostjo in vplivom;
- vrsto grožnje ali temeljnega vzroka, ki je na podlagi zbranih dokazov domnevno povzročil incident;
- izvedene blažilne ukrepe in ukrepe, ki se še izvajajo in
- podatke o čezmejnem vplivu incidenta, če so ti nastali.

V primeru pomembnega incidenta, ko po enem mesecu od njegove zaznave še vedno potekajo odzivne aktivnosti, je potrebno pristojni CSIRT skupini predložiti poročilo o napredku, končno poročilo pa poslati najpozneje en mesec po rešitvi incidenta.

Pristojni CSIRT skupini se v roku 72 ur po zaznavi incidenta priglasi tudi incident stopnje S3, ki se izvede kot prostovoljna priglasitev.

[12] API ključ - Application Programming Interface Key - unikaten identifikator, ki ga aplikacija ali uporabnik prejme za dostop do API.
[13] SSO – Single Sign-On - mehanizem avtentikacije, ki uporabniku omogoča, da se samo enkrat prijavi, nato pa lahko dostopa do več informacijskih sistemov ali aplikacij, ne da bi moral ponovno vnašati geslo.
[14] IdP – Identity Provider - sistem ali storitev, ki upravlja digitalne identitete uporabnikov in izdaja dokazila o njihovi avtentikaciji drugim sistemom.
[15] IP – Internet Protocol – internetni protokol (osnovni komunikacijski protokol, ki določa način naslavljanja in prenosa podatkov med napravami v omrežju).
[16] IoC – Inicators of Compromise - kazalnik kompromitiranja (ogroženosti ali zlorabe), dokaz ali sled, ki kaže, da je sistem lahko kompromitiran ali je bil tarča kibernetskega napada.

Pristojni CSIRT skupini se obvestilo pošlje na način, ki ga določi pristojna CSIRT skupina (npr. obrazec, uporaba varnih povezav, platforma za priglasitev incidentov).

7.2 Obveščanje o pomembnem incidentu na strani pogodbenika ali dobavitelja

Pogodbeniki in dobavitelji, ki upravljajo, obdelujejo ali dostopajo do informacijskih sredstev organizacije, so dolžni incidente stopenj S1, S2 in S3 v svojih omrežjih in informacijskih sistemih nemudoma, najkasneje pa v roku 24 ur prijaviti organizaciji na elektronski naslov: *info@organizacija.si.* Obvestilo vsebuje najmanj naslednje podatke:

- povzetek incidenta / grožnje, časovni okvir in prizadete komponente;
- kako so lahko prizadeti podatki / sistemi organizacije (obseg, sredstva, vrste podatkov);
- priporočeni takojšnji ukrepi za organizacijo (npr. rotacija poverilnic / API ključev, blokada IP naslova / IoC, preverbe dnevnikov, posodobitve) in
- navodila za ravnanje z obvestilom.

Pogodbeniki in dobavitelji, ki upravljajo, obdelujejo ali dostopajo do informacijskih sredstev organizacije, so dolžni voditi dnevnik dejavnosti odzivanja na incidente.

7.3 Komunikacija znotraj organizacije in z javnostjo

Vodstvo organizacije za vsak posamezni primer določi pravila komuniciranja o incidentu znotraj organizacije in s CSIRT skupino ter določi osebo pristojno za komuniciranje z javnostjo in dajanje izjav za javnost. Odloča tudi o obsegu podatkov, ki se posredujejo širši javnosti.

7.4 Analiza in poročanje

Po obvladovanju incidenta se izvede analiza vzrokov in pripravi poročilo, ki vključuje:

- povzetek incidenta;
- analizo vzrokov;
- oceno uspešnosti in ustreznosti odziva in
- priporočila za preprečevanje podobnih incidentov.

Poročilo o analizi vzrokov incidenta pripravi in podpiše vodja informacijske varnosti in ga posreduje vodstvu organizacije.

Morebitno neupoštevanje priporočil s strani vodstva organizacije ali prekoračitve predvidenih rokov za implementacijo priporočil vodja informacijske varnosti upošteva kot vhodne informacije pri prvi oceni tveganj informacijske varnosti.

8. Pregled in posodabljanje načrta

Načrt odzivanja na incidente se:

- pregleduje in preizkuša najmanj enkrat letno;
- posodobi ob pomembnih spremembah v omrežjih in informacijskih sistemih, organizacijskih spremembah ali spremembah zakonodaje;

- revidira po vsakem pomembnem incidentu, kjer se ugotovitve iz »*post mortem*« analize uporabijo za izboljšave postopkov, orodij ali komunikacijskih poti in
- usklajuje z veljavnimi nacionalnimi in evropskimi predpisi ter mednarodnimi standardi in dobrimi praksami.

Posodabljanje vključuje:

- preverjanje aktualnosti kontaktnih podatkov (CSIRT, notranje ekipe, pogodbeni izvajalci);
- testiranje in vaje za preverjanje odzivnih zmogljivosti (npr. simulacije napadov, namizne vaje in simulacije);
- oceno uspešnosti obstoječih mehanizmov za zaznavo in obvladovanje incidentov in
- revizijo vlog in odgovornosti v primeru sprememb v kadrovski ali organizacijski strukturi organizacije.

Odgovornost za redni pregled in posodabljanje načrta nosi vodja informacijske varnosti, ki v sodelovanju z varnostno ekipo pripravi predlog sprememb ter ga predloži vodstvu v odobritev.