EUROPEAN UNION AGENCY
FOR CYBERSECURITY

PRIPRAVA DOKUMENTIRANEGA SISTEMA ZA ODZIVANJE NA INCIDENTE

11 02 2026

VSEBINA IN CILJI

Cilj je spoznati:

1. Komponente učinkovitega načrta za odzivanje na incidente
2. Zahteve glede obveščanja, povezovalne točke
3. Praktični primer odziva na simuliran incident

NAČRT ODZIVANJA NA INCIDENTE

SPLOŠNO

Načrt odzivanja na incidente določa, kako organizacija zazna, obvladuje in odpravi kibernetske incidente ter kako obnovi delovanje.

- Postopki za odkrivanje, prijavo, analizo, omejevanje, dokumentiranje, odzivanje, obveščanje in poročanje o incidentih.
- Usklajen z zakonskimi zahtevami in Nacionalnim načrtom odzivanja na kibernetske incidente.

Namen: zagotoviti usklajen, hiter in nadzorovan odziv v času incidenta.

Kaj vključuje: sistemi za zaznavo in odziv, orodja, za koga velja (pogodbeniki, dobavitelji), postopki zaposlenih ob sumu na incident, lestvica za ocenjevanje incidentov, vloge in odgovornosti...

Zavezancem po ZInfV-1 je lahko v pomoč vzorčna varnostna dokumentacija, ki jo je pripravil URSIV in je dostopna na njihovih spletnih mestih.

ELEMENTI NAČRTA ODZIVANJA NA INCIDENTE

1. PODROČJE UPORABE

Organizacija opredeli:

- **zakaj** ta načrt obstaja (kaj določa),
- **kaj vsebuje** dokument (npr. opis sistema za zaznavo in odziv, spremljanje in vodenje dnevniških zapisov…),
- **za koga** dokument velja (npr. zaposlene, pogodbenike, dobavitelje…),
- kako se **preizkušajo, pregledujejo in posodabljajo** vloge, odgovornosti in postopki iz načrta.

2. OPREDELITEV POJMOV

Organizacija opredeli, kaj je varnostni dogodek, incident in pomembni incident.

VARNOSTNI DOGODEK	Poskus ali sum na aktivnost, ki bi lahko vplivala na razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov.
INCIDENT	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	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. SISTEM ZA ZAZNAVO IN ODZIV NA INCIDENTE, POSTOPKI

Organizacija navede, katere sisteme in postopke uporablja za zaznavo in odziv na incidente.

Primer:

- Sistem za zaznavo ali preprečevanje vdorov (**IDS/IPS/NDR/FW**),
- Sistem za upravljanje informacij in dogodkov varnosti (**SIEM**),
- Sistem za centralizirano zbiranje dnevnikov (če ni vzpostavljenega SIEM),
- Sistem za upravljanje ranljivosti,
- Sistem za zaznavo in odziv na končnih točkah (**EDR/XDR**),
- Sistem za vodenje zahtevkov (ticketing system)
- Sistem za obveščanje uporabnikov.

3. SISTEM ZA ZAZNAVO IN ODZIV NA INCIDENTE, POSTOPKI - PRIMERI

SISTEM	NAMEN	POSTOPKI OB INCIDENTU
IDS/IPS/FW	Neprekinjeno spremljanje prometa, odkrivanje in preprečevanje sumljivih aktivnosti	Opozorila korelira SIEM. Ob potrditvi incidenta se izvozi log s surovimi podatki in trenutna konfiguracija oz. pravila varnostnih sistemov. Po potrebi se začasno prilagodijo pravila oz. politika.
SIEM	Centralno zbiranje in analiza varnostnih dogodkov iz različnih virov. Korelacija in časovnice za hitro odkrivanje incidentov.	Sprožijo se postopki za ohranjanje forenzičnih dokazil (npr. dvig retencije, označevanje virov, zavarovanje dokazov). Zaklene se primer in izvozi časovnica in korelacijsko poročilo. Primer se poveže z zahtevo v ticketing sistemu.
EDR	Spremljanje in analiza dejavnosti na končnih točkah za odkrivanje groženj in odzivanje nanje.	Izvede se izolacija naprav po odobritvi. Zajame se triažni paket (procesi, povezave, dnevniški zapisi) in po potrebi RAM/disk.
Ticketing sistem	Centralizirano orodje za evidentiranje, razvrščanje, dodeljevanje in sledenje incidentom ter povezanim nalogam, z revizijsko sledjo.	Odpre se zadeva, določi se odzivni čas. V zadevo se poveže vse artefakte in odobritve.

4. VLOGE IN ODGOVORNOSTI

Organizacija opredeli vloge in odgovornosti v okviru odzivanja na incidente.

Primer:

VODJA INFORMACIJSKE VARNOSTI	VODSTVO ORGANIZACIJE	VARNOSTNA EKIPA	IT ODDELEK	UPORABNIKI
Skrb za celoten proces odzivanja na incidente in komunikacijo s pristojnim CSIRT, vodstvom organizacije in ostalimi deležniki.	Določanje notranje komunikacije, komunikacije s CSIRT in javnostjo.	Izvedba tehničnih ukrepov za obvladovanje incidentov.	Podpora obnove sistemov in implementacije varnostnih popravkov.	Prijava sumljivih aktivnosti in sodelovanje pri preprečevanju incidentov.

5. SKUPINA ZA ODZIV NA INCIDENTE

Organizacija opredeli skupino za odziv na incidente informacijske varnosti.

- člani skupine morajo imeti ustrezna znanja in kompetence,
- lahko so vključeni zaposleni in po potrebi pogodbeni izvajalci,
- opredeli se, kdo imenuje skupino za odziv na incidente, če so kakšni stalni člani (npr. vodja informacijske varnosti)…

6. POSTOPEK ODZIVANJA NA INCIDENTE

- **Zaznava in prijava** (opredelimo, kam in kako se incidenti prijavljajo, katere informacije je treba vključiti)
- **Ocena in klasifikacija** resnosti (opredelimo, kdo oceni resnost in ocenjevane vidike)
- **Obvladovanje** (opredelimo ukrepe za obvladovanje glede na predhodno razvrstitev):
  - odprava vzroka
  - obnovitev
- **Naučene lekcije.**

Smiselno je, da ima organizacija za učinkovit odziv na incidente tudi posamezne operativne scenarije oz. t.i. playbooke.

Zaznava in prijava

- *sistem/zaposleni/pogodbeni izvajalec*
- *način prijave incidenta (telefon, e-pošta...)*
- ***Prijava vsebuje vsaj:***
  - *podatke o prijavitelju,*
  - *datum in čas zaznave,*
  - *vpletene sisteme in/ali uporabnike,*
  - *opis incidenta, nastale posledice,*
  - *sprejete ukrepe.*

Ocena in klasifikacija resnosti

- *varnostna ekipa/vodja informacijske varnosti*
- ***Vidiki ocenjevanja (primer):***
  - *obseg in vpliv na storitve,*
  - *vrsta grožnje,*
  - *možnost širjenja.*

  (pomen prizadetih sistemov za zagotavljanje storitev, vpliv na uporabnike, stabilnost organizacije, pretekle izkušnje...)
- ***Razvrstitev v kategorije (primer):***
  - *Nizko – Srednje – Visoko – Kritično*
  - *Dvom? -> Višja stopnja.*

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

Vir: URSIV

Obvladovanje

Ukrepi se izvedejo glede na razvrstitev incidenta.

Primer:

- **izolacija** prizadetih sistemov in omejitev širjenja,
- **zbiranje dokazov** za podrobnejšo analizo
  - artefakti, dnevniki v zvezi z nenavadnimi/neželenimi trendi),
- **odprava vzroka** (glede na ugotovljen vektor napada) in odprava posledic incidenta
  - odprava ranljivosti in varnostnih vrzeli,
- **obnovitev** sistemov in storitev
  - odprava in sanacija vseh posledic za nadaljevanje normalnega delovanja omrežij, informacijskih sistemov, storitev organizacije.

V okviru obvladovanja incidenta je pomembno, da se izvedene aktivnosti dokumentirajo (dnevnik dejavnosti odzivanja na incident).

OBVEŠČANJE IN POVEZOVALNE TOČKE

7. OBVEŠČANJE IN POROČANJE O INCIDENTIH

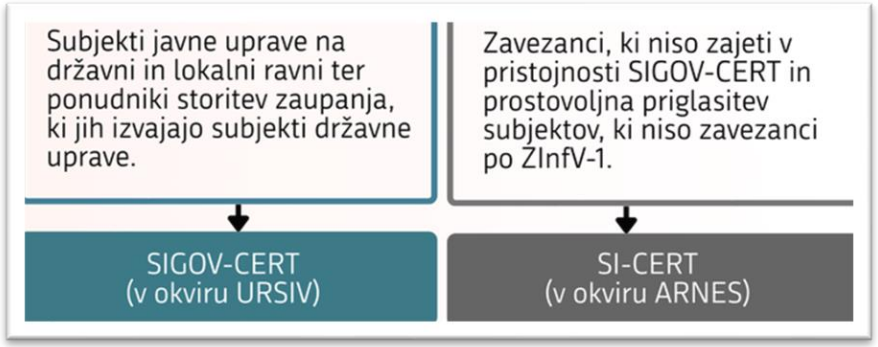
OBVEŠČANJE IN POROČANJE O POMEMBNEM INCIDENTU

*Organizacija opredeli postopke obveščanja in poročanja o incidentih. Posebej pomembni so postopki za **pomembne incidente**. Postopki morajo biti usklajeni z zakonskimi zahtevami.*

Bistveni in pomembni subjekti obvezno priglasijo **vse incidente, ki imajo pomemben vpliv na zagotavljanje storitev:**

- je ali bi lahko povzročil resne operativne motnje pri opravljanju storitev ali finančne izgube,
- vpliva ali bi lahko vplival na druge fizične ali pravne osebe s povzročitvijo precejšnje premoženjske ali nepremoženjske škode.

OBVEŠČANJE SKUPINE CSIRT



ZGODNJE SPOROČILO:

- *Je bil incident povzročen z nezakonitim ali zlonamernim dejanjem?*
- *Bi incident lahko imel čezmejni vpliv?*

do 24 ur po zaznavi

do 72 ur po zaznavi

PRIGLASITEV INCIDENTA:

- posodobitev stanja,
- začetna ocena (resnost, vpliv),
- kazalniki ogroženosti (če so),
- Priloga E (NOKI).

KONČNO POROČILO:

- podroben opis,
- Vrsta grožnje, temeljnega vzroka,
- Izvedeni blažilni in drugi ukrepi,
- čezmejni vpliv.

do 1 mesec po uradni priglasitvi

Pristojni CSIRT nemudoma oz. po možnosti v 24 urah odgovori – začetne povratne informacije, usmeritve, operativni nasveti. O priglasitvi seznani pristojni organ (URSIV)

PRIGLASITEV INCIDENTOV: POSEBNOSTI

- **UPRAVLJAVCI OSEBNIH PODATKOV:** priglasitev incidentov iz ZInfV-1, ki se nanašajo na bistvene subjekte, tudi če upravljavec sam ni zavezanec po ZInfV-1 (določa ZVOP-2).

- **FINANČNI SUBJEKTI:** poročanje o večjih incidentih, povezanih z IKT – pristojnim organom in skupini CSIRT; **krajši roki** za poročanje o **večjih incidentih** (določa **DORA**).

- **PONUDNIKI STORITEV ZAUPANJA:** obveznost uradne priglasitve najpozneje v **24 urah**.

Sum, da ima incident znake kaznivega dejanja -> nemudoma prijava policiji

Sum, da je prišlo do kršitve varstva osebnih podatkov -> nemudoma prijava Informacijskemu pooblaščencu

Katere informacije vključimo v zgodnje sporočilo?

- opis incidenta
- datum in čas zaznave,
- sprejeti ukrepi,
- ocena vpliva na storitve,
- kontaktni podatki odgovorne osebe,
- informacija o tem, ali potrebujemo pomoč CSIRT skupine,
  - **Če DA** – pošljemo vzorce škodljive kode, izvirnike e-sporočil, dnevniške zapise požarnih pregrad…
- druga pomembna dejstva, okoliščine (npr. medsektorski ali čezmejni vpliv).

OBVEŠČANJE POSLOVNIH PARTNERJEV IN KLJUČNIH STRANK

- incident vpliva ali bi lahko imel vpliv na podatke, storitve ali integracije poslovnih partnerjev/ključnih strank
- zahteva pogodbe s partnerji/ključnimi strankami
- zakonska zahteva (npr. kompromitacija API ključev, SSO, skupnih oblačnih okolij…)

Kaj vključiti?

- povzetek incidenta, časovni okvir, prizadete komponente,
- kako so lahko prizadeti podatki ali sistemi poslovnega partnerja (obseg, vrsta podatkov),
- priporočeni takojšnji ukrepi za poslovnega partnerja (rotacija poverilnic, blokada IP, posodobitve…),
- zaupnost in navodila za ravnanje z obvestilom.

OBVEŠČANJE UPORABNIKOV

- **Bistveni in pomembni subjekti** uporabnike svojih storitev **nemudoma** obvestijo o **pomembnih** incidentih, ki bodo **verjetno negativno vplivali na zagotavljanje storitev**.
- uporabnikom svojih storitev nemudoma sporočijo vse **ukrepe in sredstva**, ki jih uporabniki lahko sprejmejo **v odziv na grožnjo**.

KDAJ SE UPORABNIKOV NE OBVEŠČA?

• podatki o grožnji predstavljajo **tajne podatke**, **poslovno skrivnost** ali **varovane podatke** (upoštevamo področno zakonodajo).

• podatki o grožnji predstavljajo **varovane podatke pristojnega nacionalnega organa** in je treba upoštevati **zaščito varnosti in poslovnega interesa** zadevnih subjektov.

• razkritje lahko **škodil preiskavi incidenta ali nacionalni varnosti**.

OBVEŠČANJE O POMEMBNEM INCIDENTU NA STRANI POGODBENIKA ALI DOBAVITELJA

Organizacija opredeli dolžnosti glede obveščanja o incidentih, do katerih pride pri pogodbenikih in dobaviteljih, ki upravljajo, obdelujejo ali dostopajo do informacijskih sredstev organizacije (to je treba urediti tudi pogodbeno).

- katere incidente so dolžni prijavljati organizaciji (npr. po stopnjah),
- v kolikšnem času,
- kam,
- katere informacije morajo vključiti v obvestilo (*npr. povzetek, časovni okvir, prizadeti sistemi, vpliv na organizacijo, priporočeni ukrepi*…).

KOMUNIKACIJA ZNOTRAJ ORGANIZACIJE IN Z JAVNOSTJO

Organizacija opredeli, kdo določa pravila komuniciranja znotraj organizacije, s pristojno skupino CSIRT in javnostjo (npr. vodstvo).

- kdo bo pristojen za komuniciranje z javnostjo in dajanje izjav,
- kakšen obseg podatkov se lahko posreduje širši javnosti,
- lahko se opredelijo pravila za posamezne primere.

POMEMBNI MEDSEKTORSKI IN ČEZMEJNI INCIDENTI

- se ob priglasitvi ugotovi, da ima medsektorski ali čezmejni vpliv
  - CSIRT nemudoma zagotovi pristojnemu nacionalnemu organu (URSIV) priglašene informacije o incident

- incident bi ob daljšem trajanju lahko poslabšal stabilnost nacionalne varnosti
  - pristojni nacionalni organ (URSIV) obvesti Nacionalni center za krizno upravljanje (NCKU), osrednji organ za odzivanje na hibridne grožnje in druge pristojne organe v skladu z 18. členom ZInfV-1.

- kadar pristojni nacionalni organ ali skupina CSIRT meni, da je potrebno (npr. pomemben incident zadeva 2 ali več držav članic EU), enotna kontaktna točka (URSIV) na zahtevo nemudoma obvesti enotne kontaktne točke drugih prizadetih držav članic in agencijo ENISA.

AKTIVNOSTI PO INCIDENTU

ANALIZA IN POROČANJE (NAUČENE LEKCIJE)

Analiza in poročanje se izvedeta po obvladovanju incidenta. Pripravi se poročilo, v katerem je:

- povzetek incidenta,
- analiza vzrokov,
- ocena uspešnosti in ustreznosti odziva,
- priporočila za preprečevanje podobnih incidentov,
- posodobitev internih aktov skladno z ugotovitvami, predlaganimi izboljšavami.

*Organizacija v načrtu odziva določi, **kdo pripravi in podpiše** poročilo (npr. vodja informacijske varnosti) in **komu** se poročilo **posreduje** (vodstvu).*

PREGLEDOVANJE IN POSODABLJANJE

Dober načrt odziva na incidente se redno pregleduje in posodablja.

najmanj enkrat letno,
ob pomembnih spremembah,
po vsakem pomembnem,
po potrebi za uskladitev z nacionalnimi in evropskimi predpisi, mednarodnimi standardi in dobrimi praksami.

KAJ OBSEGA POSODABLJANJE?

aktualnost kontaktnih podatkov,
testiranje in vaje (preverjanje zmogljivosti odziva),
ocena uspešnosti obstoječih mehanizmov za zaznavo in obvladovanje,
revizija vlog in odgovornosti (kadrovske in organizacijske spremembe).

KDO JE ODGOVOREN?

Določi organizacija v načrtu – *npr. vodja informacijske varnosti pripravi predlog, ki ga mora potrditi vodstvo.*

PRAKTIČNA VAJA

PRAKTIČNA VAJA / NAMIZNA VAJA (TABLETOP EXERCISE)

Simulirani incident: Ransomware v poslovnem omrežju

Cilj vaje

➢ Udeleženci vadijo usklajen odziv na kibernetski incident s poudarkom na:

- zaznavi in klasifikaciji incidenta
- odzivanju in odločanju v realnem času
- aktivaciji postopkov eskalacije
- preverjanju **obveznosti prijave incidenta po ZInfV-1** (URSIV/SI-CERT)

OZADJE SCENARIJA

- Vaša organizacija zagotavlja bistvene storitve. Med običajnim delovnim dnem se pojavijo naslednje težave:
  - Več uporabnikov poroča, da ne more dostopati do skupnih map.
  - Na delovnih postajah se pojavi odkupno sporočilo (ransom note):

    "Vaše datoteke so šifrirane. Če želite ključ, plačajte 2 BTC v 48 urah."
  - Antivirus zazna poskuse zlonamerne aktivnosti, ki jih ne uspe zaustaviti.
  - Na strežniku varnostnih kopij je zaznana nenavadna aktivnost.
  - Nekateri sistemi se nenadoma izklapljajo iz omrežja.

POTEK VAJE S ČASOVNIMI INJEKTI

Korak 1 – Zaznava (Triage)

Injekt 1: SOC zazna nenavaden promet med strežniki.

Vprašanja za skupino:

- *Ali gre za **varnostni dogodek** ali **incident**?*
- *Kaj so **prvi podatki**, ki jih potrebujemo?*
- *Katere dnevnike ali orodja morate preveriti?*

Korak 2 – Začetni odziv

Injekt 2: Potrjeno – gre za ransomware LockBit.

Odločitve:

- *Izolirati okužene naprave **takoj** ali počakati in opazovati?*
- *Aktivirati **ekipo za odzivanje na incidente (IRT)**?*
- ***Izklopiti datotečni strežnik** – da ali ne?*

Korak 3 – Ocena vpliva (Impact Assessment)

Injekt 3: Finančni oddelek poroča, da plače ne morejo biti izplačane.

Razprava:

- *Ali je prizadeta **kritična storitev**?*
- *Aktivirati **načrt neprekinjenega delovanja (BCP/DRP)**?*
- *Ali obstaja **tveganje izgube podatkov**?*

Korak 4 – Prijava incidenta (ZInfV-1)

Injekt 4: Varnostne kopije so morda kompromitirane. Obnovitev bo trajala več kot 24 ur.

Odločitev:

- *Ali je to **prijavljiv incident** po ZInfV-1?*
- *Ali je treba **URSIV obvestiti v 24 urah**?*
- *Ali vključimo **SI-CERT** za tehnično podporo?*

Injekt 5: Pojavi se novica na družbenih omrežjih: "Vašo organizacijo je napadel ransomware.„

Odločitve:

- *Kako komunicirati z javnostjo?*
- *Kdo daje izjave – IT, PR ali vodstvo?*
- *Ali priznati incident ali zadržati informacije?*

Korak 6 – Zajezitev in obnova

Skupina pripravi načrt:

- *Kako **zajeziti širjenje napada**?*
- *Kateri sistemi se **prioritetno obnavljajo**?*
- *Kako **zagotoviti forenzične dokaze**?*

PRIČAKOVANI REZULTATI

Udeleženci morajo:

- določiti resnost incidenta
- aktivirati eskalacijski postopek
- odločiti o **prijavi pristojnemu CSIRT**
- pripraviti **načrt odzivanja**
- zaščititi kritične storitve
- zagotoviti dokumentiranje za naknadno analizo

DISKUSIJA

HVALA ZA POZORNOST