EUROPEAN UNION AGENCY
FOR CYBERSECURITY

NAČRTI ODZIVANJA IN PRIPRAVLJENOST

VSEBINA

Splošno o načrtih odzivanja.

Elementi izvedbenega načrta odzivanja.

Pripravljenost in koordiniran odziv.

Primer načrta odzivanja.

SPLOŠNO O NAČRTIH ODZIVANJA

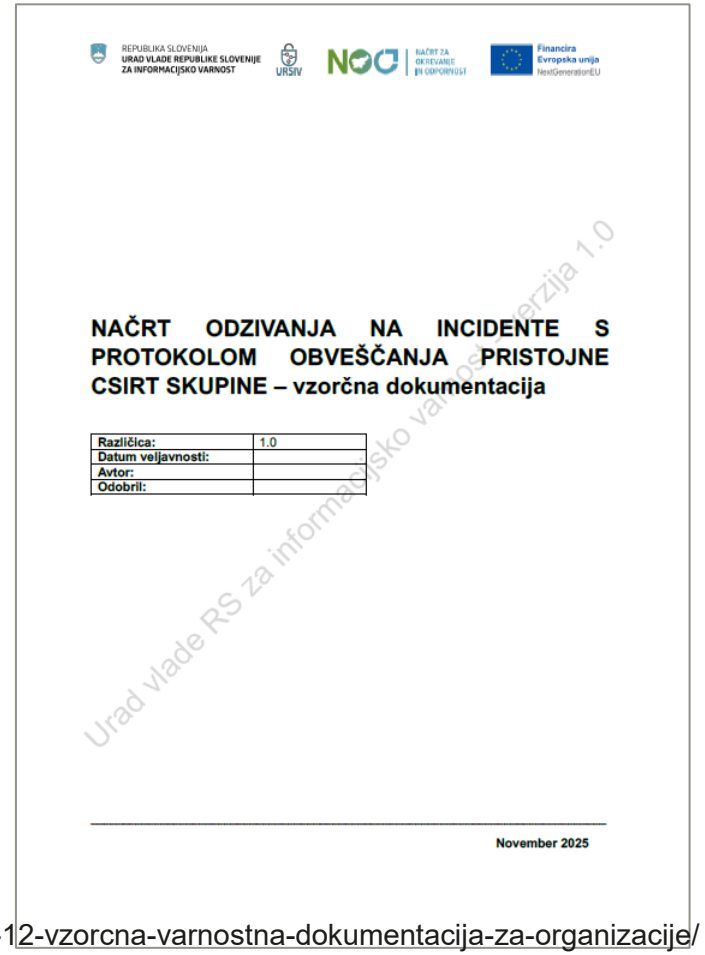
ZAKONSKE OBVEZNOSTI

ZInfV-1 zahteva formalni krovni Načrt odzivanja na incidente.

Ta mora vključevati:

- opredelitev sistemov za zaznavo in odziv na incidente,
- opis postopkov za zaznavo in odziv na incidente,
- opredelitev vlog in odgovornosti pri odzivu na incidente,
- opredelitev skupine za odziv na incidente,
- postopek odzivanja na incidente po korakih (zaznava, prijava, ocena, klasifikacija, obvladovanje, obveščanje in poročanje),
- protokol komuniciranja znotraj in izven organizacije,
- opredelitev analize in poročanja o incidentu,
- navodila glede pregledovanja in posodabljanja načrta

*V pomoč pri pripravi je lahko **vzorčna varnostna dokumentacija, ki jo je pripravil URSIV** (dostopna na njihovih spletnih straneh)*


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

https://www.gov.si/novice/2025-12-12-vzorcna-varnostna-dokumentacija-za-organizacije/

IZVEDBENI NAČRTI ODZIVANJA NA INCIDENTE (PLAYBOOKS)

Izvedbeni načrti odzivanja (angl. *playbooks*) predstavljajo **celovite dokumentirane postopke** in **protokole**, ki narekujejo **odziv** skupin za odzivanje **na specifične incidente ali grožnje:**

- navodila za odzivanje po korakih in odločitvena drevesa,
- vloge, odgovornosti in
- standardizirani postopki dela

pri odzivanju na incidente.

npr. napadi spletnega ribarjenja (phishing), napadi onemogočanja (DDoS), okužbe z zlonamerno programsko opremo, napadi z izsiljevalskim virusom (ransomware)...

IZVEDBENI NAČRT ODZIVANJA ≠ SPLOŠEN DOKUMENT

Gre za navodila in smernice, prilagojene kontekstu organizacije – specifični infrastrukturi organizacije, varnostnim orodjem, politikam in sprejemljivim ravnem posameznih tveganj.

IZVEDBENI NAČRTI ODZIVANJA NA INCIDENTE (PLAYBOOKS)

ZAKAJ?

- Sodobne grožnje zahtevajo standardizirane, jasne in preizkušene postopke odzivanja.
- Izvedbeni načrti operacionalizirajo zahteve po upravljanju tveganj v organizaciji.
- Izvedbeni načrti zmanjšajo nejasnosti glede postopkov odzivanja in s tem povezanih odgovornosti
- Z uporabo izvedbenih načrtov je odziv na incidente lahko hitrejši in bolj učinkovit.

ELEMENTI IZVEDBENEGA NAČRTA ODZIVANJA

ELEMENTI IZVEDBENEGA NAČRTA ODZIVANJA

DOBER IZVEDBENI NAČRT:

- Jasno določa **postopke** za **zaznavo, triažo, analizo, zajem dokazov, komunikacijo** znotraj in izven organizacije, **obveščanje pristojnih organov** ter **analizo po** incidentu.
- Jasno določa **vloge in odgovornosti** za posamezna dejanja in posledice v okviru reševanja incidenta.
- Se **redno pregleduje**, verzijam dokumenta in potrditvam pa se ustrezno **sledi**.

STRUKTURA IZVEDBENEGA NAČRTA

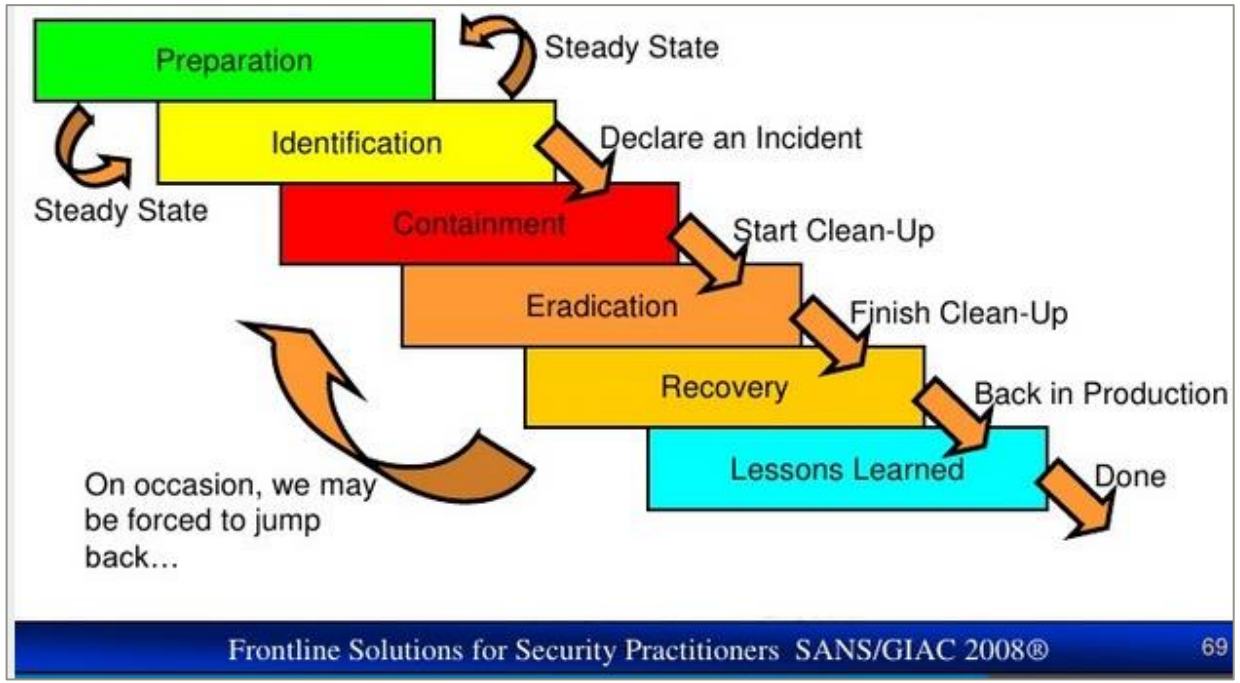
- Namen, obseg, predpogoji za uporabo,
- kontrola verzij, odobritev sprememb,
- vloge in odgovornosti (RACI matrika),
- uporabljena orodja (SIEM, EDR/XDR, SOAR...),
- postopki odzivanja po 6 fazah (v nadaljevanju),
- odločitvena drevesa (npr. Izolacija, izklop, aktivacija načrta okrevanja, vključitev pravne službe, obveščanje pristojnih organov...),
- protokol komuniciranja znotraj in izven organizacije,
- seznam kontaktnih podatkov (znotraj organizacije, pristojni organi, drugi deležniki izven organizacije),
- zahteve glede testiranja, pregledovanja in posodabljanja.

FAZE ODZIVANJA NA INCIDENTE

Izvedbeni načrt odzivanja vsebuje **natančne smernice** in **navodila** za **specifične tipe incidentov**, po **fazah**:

1. Priprava
2. Zaznavanje in analiza
3. Zajezitev
4. Odprava
5. Obnovitev
6. Aktivnosti po incidentu

Faze so načeloma enake pri vseh incidentih, posamezne specifične aktivnosti in ekipe, ki so odgovorne za njihovo izvedbo, pa se določijo glede na tip incidenta.



PRIPRAVLJENOST IN KOORDINIRAN ODZIV

PRIPRAVLJENOST IN KOORDINIRAN ODZIV

VLOGA IZVEDBENIH NAČRTOV ODZIVANJA

- Zagotavljanje konsistentnega učinkovitega odziva, ne glede na to kdo je vključen v odziv na incident ter kdaj do incidenta pride.
- Hitrejše odzivanje na incidente, saj ni potrebno razvijati posameznih strategij od začetka.
- Bolj učinkovito sprejemanje odločitev v času večjega pritiska med odzivanjem na incidente.
- Boljša koordinacija in komunikacija zaradi jasno določenih vlog, odgovornosti in komunikacijskih kanalov.

UČINKOVITOST ODZIVANJA

Z jasno postavljeni cilji odzivanja postavimo pragove učinkovitosti, utrjujemo skladnost ter dvigujemo zrelost upravljanja incidentov v organizaciji. Učinkovitost odzivanja na incidente lahko merimo z **različnimi metrikami:**

KPI	Ključni kazalniki uspešnosti (angl. *key performance indicators)*	Ocena dejanske učinkovitosti procesa – pripravljenost za zaznavanje, odzivanje, reševanje incidentov.
MTTD	Čas zaznave (angl. *Mean Time to Detect*)	Koliko časa organizacija potrebuje za zaznavo incidenta (kako hitro sistemi zaznajo, da je šlo nekaj narobe).
MTTA	Čas prepoznave (angl. *Mean Time to Acknowledge)*	Koliko časa traja, da sistemi ali relevantni deležniki prepoznajo alarm, po tem ko se je prožil. Ta časovna točka je ključna za pričetek dejanskega odziva na incident.
MTTR	Čas razrešitve (angl. *Mean Time to Resolve)*	Koliko časa je potrebno za dokončno razrešitev incidenta (od zaznave do obnovitve).

UČINKOVITOST ODZIVANJA

Poleg prej navedenih metrik se lahko pri ocenjevanju učinkovitosti odzivanja upošteva tudi:

- Dogovor o izvajanju storitve (angl. *Service Level Agreement* oz. *SLA*) za zajezitev incidentov (npr. zajezitev v <30min)
- stopnja uspešne obnovitve iz čistih varnostnih kopij
- čas do obnovitve kritičnih storitev ali procesov
- delež avtomatiziranih postopkov brez človeškega posredovanja (orkestracija in avtomatizacija)

INTEGRACIJA ORODIJ

SIEM	Rešitev za upravljanje varnostnih informacij in dogodkov (angl. *Security Information and Event Management*)	Zbiranje, združevanje, analiza velike količine podatkov iz različnih virov, ki jih določi organizacija (aplikacij, naprav, strežnikov, uporabnikov) v realnem času.Pregled nad stanjem varnosti organizacije, zaznavanje, analiza in odziv na varnostne dogodke.
EDR	Rešitev za spremljanje in zaščito končnih točk (angl. *Endpoint Protection and Response*)	Nenehno spremljanje končnih točk (24/7), zbiranje podatkov iz končnih točk in analiza za razkrivanje sumljivih aktivnosti. Zaznava in odprava groženj, preden se razširijo po omrežju. Samodejna zamejitev groženj in opozarjanje varnostnih ekip.

INTEGRACIJA ORODIJ

XDR	Rešitev za razširjeno zaznavanje in odziv (angl. *Extended Detectiond and Response*)	Za širše področje kot EDR (končne točke, identitete, aplikacije, oblak, e-pošta...). Omogočanje vidljivosti verige kibernetskega napada ter obsežno obveščanje o grožnjah. Samodejno onemogočanje naprednih napadov v teku ter okrevanje prizadetih sredstev v varno stanje (prekinitev procesov, odstranjevanje zlonamernih pravil, izolacija naprav, onemogočanje računov).
SOAR	Rešitev za orkestracijo, avtomatizacijo in odziv na varnostne dogodke (angl. *Security Orchestration, Automation and Response*)	Avtomatizacija preprečevanja kibernetskih napadov in odzivanja nanje. Poenotenje integracij, določitev načina izvajanja posameznih opravil, priprava načrta odzivanja na dogodke glede na potrebe organizacije). Razbremenitev varnostnih ekip od ponavljajočih se in dolgotrajnih opravil.

ORKESTRACIJA IN AVTOMATIZACIJA ODZIVA

SOAR – Security Orchestration, Automation and Response

- **ORKESTRACIJA** = koordinirano sprejemanje odločitev ob izpolnjenih pogojih
  - *IP je prepoznan kot zlonameren na javnih listah – SOAR ga pošlje v blokado na požarni pregradi*

- **AVTOMATIZACIJA** = avtomatizirano izvajanje posameznih aktivnosti na varnostnih orodjih in informacijskih sistemih v okviru odzivanja na incident
  - *SOAR skenira zlonamerno datoteko in jo primerja s podatki na javnih listah npr. VirusTotal za podajo ocene varnosti datoteke*

- **ODZIV** = zbiranje podatkov iz različnih virov, povezovanje podatkov, določanje prioritete in kritičnosti ter avtomatska zabeležka informacij o incidentu v ustrezen sistem.

ORKESTRACIJA IN AVTOMATIZACIJA ODZIVA

MOŽNA UPORABA:

- Integracija z obstoječimi orodji: SIEM, požarna pregrada, EDR/XDR, platforme z obveščevalnimi informacijami.
- Lov na grožnje z naprednimi poizvedbami (prepoznava trendov in anomalij, ki lahko kažejo na napredne grožnje - APT.
- Avtomatizacija ponavljajočih se opravil - zmanjšanje odzivnega časa in razbremenitev analitikov, da se lahko osredotočijo na kompleksnejšo analizo.
- Generiranje poročil o aktivnostih, izvedenih v okviru odziva na incident.

STALNO IZBOLJŠEVANJE

Izvedbene načrte odzivanja na incidente je potrebno **redno testirati, da potrdimo njihovo ustreznost in učinkovitost**. Na primer:

- v okviru testiranja načrtov neprekinjenega poslovanja oz. Načrta okrevanja posameznih storitev, procesov in virov,
- simulacija scenarijev, brez dejanskega izpada sistemov a z realnimi odzivi relevantnih deležnikov (t.i. *table-top* vaje),
- testiranje dejanskega vdora v informacijski sistem (t.i. *red team* testiranje).

Sledi pregled ugotovitev testiranja, iskanje potencialnih izboljšav in po potrebi prilagoditev posameznih načrtov.

Vsako **spremembo in njeno potrditev se ustrezno dokumentira** v pregledu verzij.

PRIMER NAČRTA ODZIVANJA

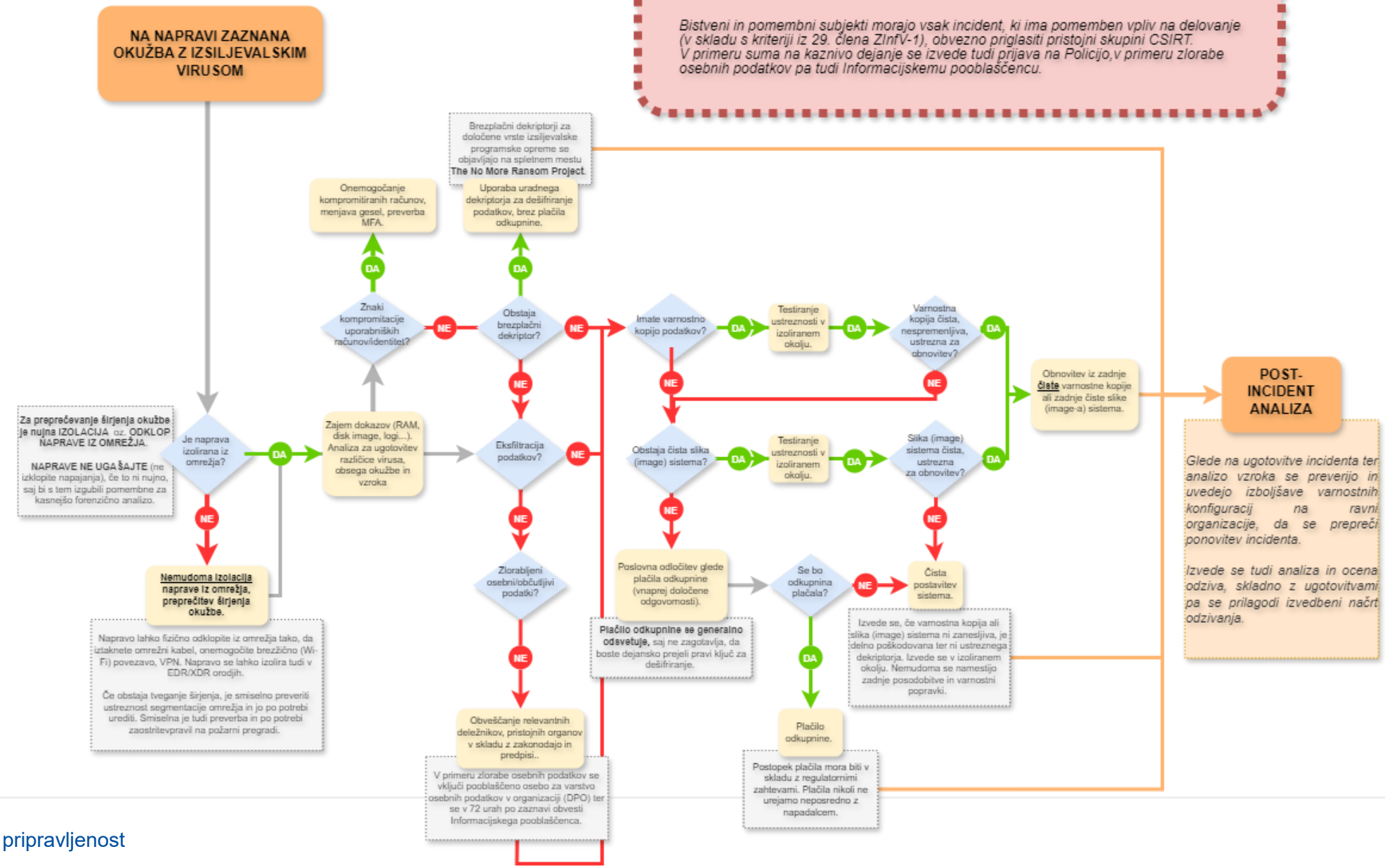
Primer (izvedbeni načrt - okvir):

Zaznana okužba naprave z izsiljevalskim virusom	
1-PRIPRAVA	Določitev vlog in odgovornosti, zagotovitev orodij, nespremenljivih varnostnih kopij in načrt komunikacije. Pripravite tudi kontaktne sezname in postopke za obveščanje.
2-ZAZNAVANJE IN ANALIZA	Prepoznava vdora (phishing, izraba ranljivosti, C&C komunikacija, eskalacija privilegijev). Zaznava okužbe (alarm, nenavadno šifriranje in obnašanje datotek, izsiljevalsko sporočilo). Sledi izolacija naprave iz omrežja. Obvestijo se relevantni deležniki. Zajamejo se dokazi (RAM, disk, logi, omrežne povezave). Preveri se potencialna kompromitacija uporabniških računov. Če je do kompromitacije prišlo, se te račune onemogoči in se jim zamenja gesla. Preveri se status glede MFA.
3-ZAJEZITEV	Preprečevanje širjenja okužbe - izolacija dodatnih naprav, onemogočanje računov, dostopov, zaostritev varnostnih politik (npr. tudi samo začasno MFA, omrežni dostop...)
4-ODPRAVA	Odstranitev zlonamerne programske opreme, preverba, da ni 'ostankov' (t.i. *backdoor*, skripte...). Onemogočanje nepotrebnih računov in preverba konfiguracij.
5-OBNOVITEV	Preverba varnostnih kopij/slik sistema in njihove ustreznosti za obnovitev. Če so ustrezne, obnovitev iz zadnje čiste kopije ali preverjene slike sistema v izoliranem okolju. Preverba integritete obnovljenih sistemov pred ponovnim priklopom.
6-AKTIVNOSTI PO INCIDENTU	Izvedba analize po incidentu. Ugotavljanje izvornega vzroka in glede na to izvedba izboljšav varnostnih nastavitev in postopkov. Posodobitev izvedbenega načrta odzivanja in drugih relevantnih dokumentov. Po potrebi obvestilo drugih deležnikov.

Primer (oris postopka - odločitveno drevo):

POMEMBNO: V vsakem primeru ocenite vpliv incidenta na delovanje.

Bistveni in pomembni subjekti morajo vsak incident, ki ima pomemben vpliv na delovanje (v skladu s kriteriji iz 29. člena ZInfV-1), obvezno priglasiti pristojni skupini CSIRT. V primeru suma na kaznivo dejanje se izvede tudi prijava na Policijo, v primeru zlorabe osebnih podatkov pa tudi Informacijskemu pooblaščencu.



HVALA