EUROPEAN UNION AGENCY
FOR CYBERSECURITY

NEPREKINJENOST POSLOVANJA IN OKREVANJE PO NESREČI

Živa Drobnič Kvartuč, Telekom Slovenije
Božidar Dajčman, ICS

11 02 2026

VSEBINA IN CILJI

Cilj je spoznati:

1. Postopek analize vplivov na poslovanje (BIA)
2. Komponente Načrta neprekinjenega poslovanja (BCP), načrta okrevanja po nesreči
3. Ciljni čas obnovitve in ciljna točka obnove podatkov
4. Uporaba rezultatov BIA za razvoj BCP, upravljanje varnostnih kopij in okrevanje po nesreči
5. Predstavitev kratkih primerov izdelave dokumentacije

POLITIKA NEPREKINJENEGA POSLOVANJA

Politika neprekinjenega poslovanja je osrednji dokument, ki določa zavezo organizacije, da ob motnjah, izrednih dogodkih ali krizah ohranja kontinuirano izvajanje ključnih procesov/storitev.

Namen: vzpostaviti okvir za vzpostavitev, vzdrževanje in nenehno izboljševanje SUNP. Pregleduje se najmanj enkrat letno in ob večjih spremembah v organizaciji.

Ključne zaveze: izvedba analize vplivov na poslovanje (BIA), priprava načrta neprekinjenega poslovanja (BCP), določitev minimalne ravni poslovanja, varnostnega kopiranja in redundance, redno testiranje, usposabljanje, nenehno izboljševanje.

- cilji in načela, vloge in odgovornosti, popis poslovnih funkcij/procesov, analiza vplivov na poslovanje in načrt neprekinjenega poslovanja, minimalna raven poslovanja in minimalne operativne zahteve, upravljanje varnostnih kopij in redundantnih zmogljivosti

ANALIZA VPLIVOV NA POSLOVANJE

SPLOŠNO

Analiza vplivov na poslovanje (BIA) je osnova za vzpostavitev in vzdrževanje sistema upravljanja neprekinjenega poslovanja (SUNP). Določa okvir in metodologijo za ocenjevanje posledic motenj na ključne poslovne funkcije, procese, vire in storitve.

NAMEN BIA:

- prepoznati kritične poslovne procese in storitve v organizaciji, katerih motnja ali izpad bi imela najhujše posledice za njeno delovanje,
- določiti potrebne korake in prioritete za preprečevanje tovrstnih vplivov, odzivanje in obnovo procesov.

BIA se uporablja za vse organizacijske enote, funkcije in procese, ki so vključeni v opredeljen obseg SUNP.

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

KAJ VKLJUČUJE BIA?

- Navedba poslovnih procesov in lastnikov poslovnih procesov,
- Ocena posledic prekinitve poslovanja (finančne, pravne, ugled, časovne…),
- Določitev ciljne časovne točke za obnovo procesa in ciljne točke obnove podatkov,
- Identifikacija odvisnosti in potrebnih virov (osebje, zunanji dobavitelji, infrastruktura…),
- Navedba informacijskih sistemov (HW in SW) in komunikacijskih povezav za delovanje procesov,
- Razvrstitev ključnih procesov glede na njihovo kritičnost in vrstni red obnove glede na skupno oceno kritičnosti (višja ocena kritičnosti -> prednost pri obnovi).

OCENA KRITIČNOSTI PROCESOV

*Proces mora z vidika kritičnosti oceniti **lastnik procesa**.*

- *Kako bi izpad procesa vplival na poslovanje in zagotavljanje storitev?*

KAJ SE UPOŠTEVA PRI OCENI?

FINANČNI VPLIV	izguba dohodkov, povečani stroški, pogodbene kazni
UGLED	izguba zaupanja strank, negativna medijska izpostavljenost
VARNOST IN ZDRAVJE	neposreden vpliv na varnost zaposlenih, strank, okolja…
OPERATIVNE ODVISNOSTI	odvisnost drugih procesov od delovanja ocenjevanega procesa *Ali kakšen drug proces ne more delovati brez tega procesa?*
PRAVNI/REGULATORNI VPLIV	zakonske zahteve za delovanje procesa – izvajanje zakonskih nalog, javnega pooblastila, poročanje finančni upravi, izplačevanje plač zaposlenim…

KRITIČNOST PROCESOV – ČASOVNI OKVIRI

Proces ocenimo z vidika, ***koliko časa lahko organizacija deluje brez njega*** *oz.* ***ne da bi nastale škodljive posledice*** *za poslovanje.*

RTO: ciljna časovna točka obnove procesa *(Recovery Time Objective)*	Čas, v katerem moramo obnoviti proces, da preprečimo nesprejemljiv vpliv na poslovanje.
RPO: ciljna točka obnovitve (podatkov) *(Recovery Point Objective)*	Maksimalen čas sprejemljive izgube podatkov.

krajša RTO in RPO = bolj kritičen proces

METODA OCENJEVANJA KRITIČNOSTI PROCESOV

Organizacija opredeli metodo za ocenjevanje kritičnosti procesov in kriterije oz. matriko ocenjevanja.

PRIMER:

Procesi se razvrstijo v tri kategorije:

- *kritični procesi (obnova v nekaj minutah/urah),*
- *pomembni procesi (obnova v nekaj dneh),*
- *podporni procesi (obnova v 2 tednih).*

Primer opisne matrike ocenjevanja:

Vpliv izpada	Opis	Primer
Visok (kritičen proces)	Izpad lahko povzroči zelo veliko finančno škodo. Izpad ima velik negativni vpliv na ugled. Izpad ima težke pravne (zakonske) posledice ali za dlje časa ali popolnoma onemogoči nadaljevanje poslovanja.	Glavni proizvodni procesi, obdelava naročil, izvajanje plačil, opravljane pomembnih zakonskih nalog.
Srednji (pomemben proces)	Izpad lahko povzroči veliko finančno škodo. Izpad ima pravne (zakonske) posledice. Izpad za krajši čas onemogoči nadaljevanje poslovanja.	Upravljanje s kadri, priprava analiz in poročil.
Nizek (podporni proces)	Izpad lahko povzroči manjši vpliv, ki ga je mogoče prenesti dalj časa.	Interne raziskave, poročila, podporne naloge.

Vir: URSIV

Organizacija opredeli način ocenjevanja kritičnosti procesov:

- kateri kriteriji se upoštevajo (finančni, operativni in pravni/regulatorni vpliv, vpliv na ugled, varnost in zdravje, časovna občutljivost…),
- kako se ocenjuje posamezen kriterij (točke),
- matrika ocenjevanja vpliva,
- način določanja skupne ocene kritičnosti.

Primer opisne matrike ocenjevanja vpliva:

Kriterij/Vpliv	1 – Nizek (1 točka)	3 – Srednji (2 točki)	5 – Visok (3 točk)
Finančni vpliv	Izguba manj kot 1.000 EUR.	Izguba od 1.000 do 20.000 EUR.	Izguba več kot 20.000 EUR.
Pravni/regulatorni vpliv	Brez pravnih posledic.	Možna opozorila, opomini ali manjše globe do največ 20.000 EUR.	Visoke globe, izguba licence ali koncesije.
Ugled	Interni vpliv, stranke ali javnost ne opazi.	Negativne pritožbe posameznih strank, omejen negativni odmev na socialnih omrežjih.	Velika škoda ugledu, odmevna negativna medijska izpostavljenost.
Časovna občutljivost	Izpad sprejemljiv več kot en teden.	Izpad sprejemljiv do treh dni.	Izpad nesprejemljiv že več kot 24 ur.

SKUPNA OCENA KRITIČNOSTI *= npr. seštevek točk vseh kriterijev:*

- *10-12: kritični proces*
- *7-9: pomembni proces*
- *4-6: podporni proces*

Vir: URSIV

Primer izračuna kritičnosti procesov (izmišljena organizacija)

Proces	Finančni vpliv	Pravni vpliv	Ugled	Časovna občutljivost	Skupaj	Kritičnost
Prodaja/naročila	3	2	3	3	11	Kritični
Računovodstvo	2	3	2	2	9	Pomembni
Kadrovske evidence	1	2	2	1	6	Podporni
Elektronska pošta	3	2	3	3	11	Kritični
Izdaja osebnih dokumentov	1	3	3	3	10	Kritični

Vir: URSIV

ANALIZA TVEGANJ IN RANLJIVOSTI PROCESOV

1. prepoznava možnih **tveganj** za vsak **poslovni proces**,
2. ocena **verjetnosti nastanka** identificiranih tveganj,
3. ocena **vpliva** identificiranih tveganj na poslovanje,
4. opredelitev in določitev **ravni tveganja** (npr. nizka, srednja, visoka).

IZVEDBA ANALIZE TVEGANJ IN RANLJIVOSTI

Matriko verjetnosti in vpliva za ocenjevanje tveganj opredeli organizacija.
V nadaljevanju primer modela 5x5:

Primer:

Lestvica verjetnosti	Opis
Zelo nizka verjetnost (1 točka)	Dogodek je malo verjeten (1× v 10 letih).
Nizka verjetnost (2 točki)	Redko, vendar možno (1× v 5 letih).
Srednja verjetnost (3 točke)	Občasno (1× na 2 do 3 leta).
Visoka verjetnost (4 točke)	Pogosto (vsaj 1× na leto).
Zelo visoka verjetnost (5 točk)	Pričakovano večkrat letno.

Vir: URSIV

Lestvica vpliva	Opis
Zanemarljiv vpliv (1 točka)	Dogodek ne povzroči opaznega vpliva na poslovanje.
Majhen vpliv (2 točki)	Dogodek lahko povzroči manjše motnje, obvladljivo brez večjih posledic ali zelo omejen vpliv.
Srednji vpliv (3 točke)	Dogodek lahko povzroči opazne kratkotrajne motnje (finančne izgube in krajše prekinitve,) z manjšim vplivom na posamezno organizacijsko enoto.
Visok vpliv (4 točke)	Dogodek lahko povzroči motnje ključnih procesov, večji finančni vpliv ali izgubo podatkov v manjšem obsegu.
Kritičen vpliv (5 točk)	Dogodek lahko povzroči hude posledice - dolgoročne prekinitve ključnih procesov, velik negativni finančni vpliv, prekinitev poslovanja, izgubo podatkov ali izgubo ugleda.

Vir: URSIV

KAKO IZRAČUNAMO TVEGANJE?

TVEGANJE = verjetnost x vpliv

- vsakemu tveganju določimo oceno verjetnosti (npr. 1-5) in oceno vpliva (npr. 1-5),
- zmnožek teh ocen predstavlja skupno raven tveganja (npr. 1-25).

Tveganja organizacija razvrsti v vnaprej določene kategorije. **Primer:**

- visoko tveganje (16-25 točk)
- srednje tveganje (9-15 točk)
- nizko tveganje (1-8 točk)

Primer izračuna:

Zmnožek (Verjetnost × Vpliv)	Raven tveganja	Opis
1–8 točk	**Nizko tveganje**	Dogodek lahko povzroči manjše posledice, obvladljivo z rednimi ukrepi. Operativno delo je mogoče nadomestiti ali prestaviti.
9–15 točk	**Srednje tveganje**	Dogodek lahko povzroči opazne posledice, potrebni so ukrepi za obvladovanje tveganj. Možne so zamude, povečani stroški ali zmanjšana kakovost storitev.
16–25 točk	**Visoko tveganje**	Dogodek lahko ima resne negativne posledice, zahteva proaktivne ukrepe in ukrepe za pripravljenost. Možno je prenehanje delovanja ali bistveno omejevanje ključnih storitev.

Vir: URSIV

KAKO IZRAČUNAMO TVEGANJE?

Primer tipičnih tveganj z določeno verjetnostjo, vplivom in oceno ravni tveganja:

Tveganje	Verjetnost	Točk	Vpliv	Točk	Raven tveganja	Točk
Kibernetski napad (npr. izsiljevalska programska oprema)	Visoka	4	Visok	4	Visoko	16
Izpad infrastrukture (npr. električni izpad)	Nizka	2	Kritičen	5	Srednje	10
Človeška napaka (npr. napačna konfiguracija)	Srednja	3	Srednji	3	Srednje	9
Tveganje dobavne verige (npr. izpad Microsoft oblaka)	Srednja	3	Visok	4	Srednje	12

Vir: URSIV

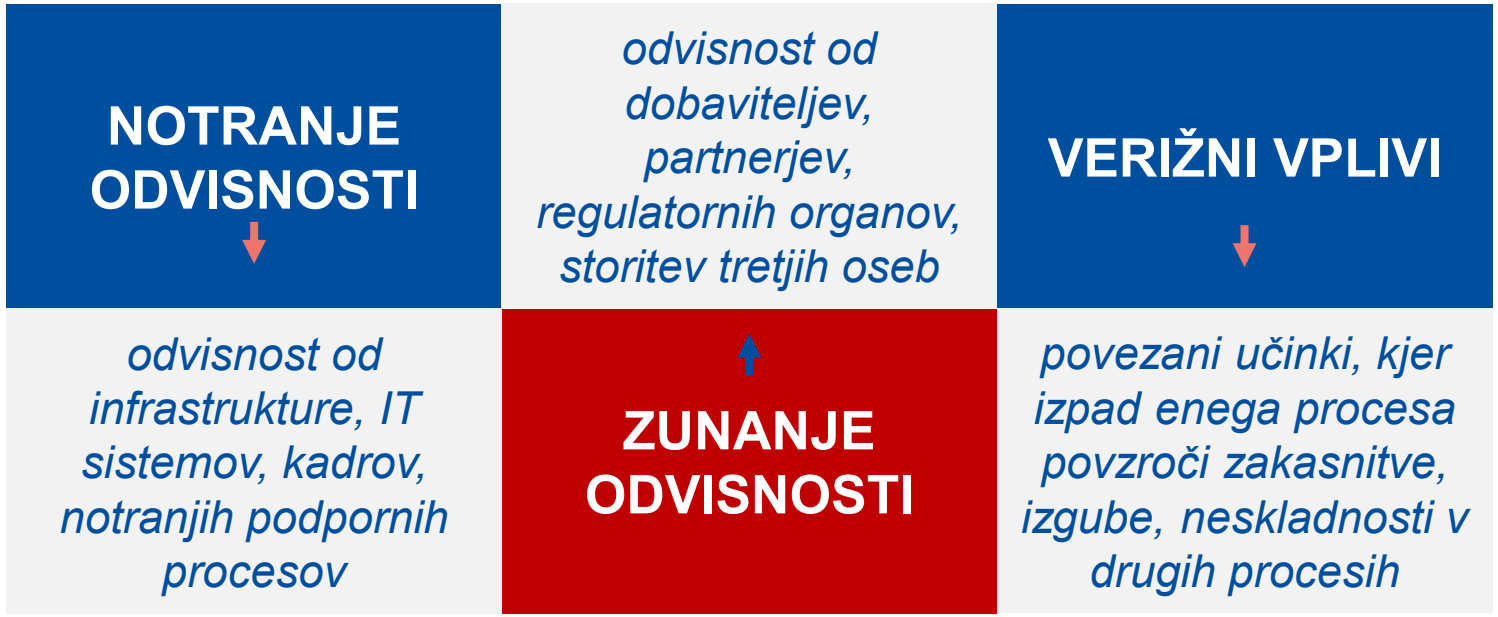
Verjetnost uresničitve tveganj se med organizacijami razlikuje.

Verjetnost lahko povečajo naslednje ranljivosti:

- *zastarela in neposodobljena programska oprema,*
- *šibka avtentikacija,*
- *pomanjkanje nadzora ključnih dobaviteljev,*
- *pomanjkanje redundance (podvojenih zmogljivosti),*
- *…*

ANALIZA ODVISNOSTI IN VERIŽNIH VPLIVOV

- opisna določitev **notranjih in zunanjih odvisnosti** vsakemu poslovnemu procesu (odvisnosti, ki omogočajo delovanje procesa),
- opredelitev možnih **verižnih vplivov** (izpad procesa vpliva na druge procese in poslovanje).



VZDRŽEVANJE IN IZBOLJŠEVANJE

Analiza vplivov na poslovanje je **živ dokument**, ki ga je treba **redno pregledovati in posodabljati**, na primer:

- vsaj enkrat letno,
- ob nastanku večjih sprememb v organizaciji ali poslovnih procesih,
- ob pojavu pomembnih incidentov z vplivom na neprekinjenost poslovanja.

Organizacija ob opredelitvi pregledovanja in posodabljanja dokumenta **določi tudi odgovornosti** za pregledovanje in posodabljanje. Primer:

- **splošni del** Analize vplivov na poslovanje: vodja SUNP
- **posamezni procesi**: lastniki procesov

UPORABNOST ZA NAČRT NEPREKINJENEGA POSLOVANJA

Rezultati analize vplivov na poslovanje organizaciji pomagajo pri pripravi načrta neprekinjenega poslovanja.

- **prioritizacija poslovnih procesov** glede na oceno njihove **kritičnosti**
- določanje **prioritet za zagotavljanje neprekinjenega poslovanja**
- pragovi **sprejemljivih motenj, izpadov** (prekinitve delovanja)
- opredelitev **dejanskih potreb organizacije** in omogočanje razvoja učinkovitih **strategij za neprekinjeno poslovanje in obnovitev/ponovno vzpostavitev** delovanja

PRIMER

Opredelitev kritičnega poslovnega procesa:

Št. procesa	***IT-001***
Naziv procesa	*Zagotavljanje elektronske pošte (Microsoft Exchange, hibridni model, 200 uporabnikov)*
Lastnik procesa	*Vodja IT oddelka/CISO*
Ključna informacijska sredstva	*- E-poštni strežniki (MS Exchange)* *- strežniki DNS* *- Omrežna oprema (usmerjevalniki, požarne pregrade, stikala)* *- E-poštne baze podatkov* *- Uporabniški računi* *- IT administratorji (3 osebe)* *- 200 uporabnikov*
Kritičnost procesa	***Kritičen*** *(visok vpliv na finance, ugled, pravne obveznosti in operativne procese)*
RTO	*2 uri*
RPO	*15 minut*
Minimalno poslovanje	***DA***

Vir: URSIV

Točkovna ocena kritičnosti procesa

Kriterij	Točke
Finančni vpliv	4
Pravni/regulatorni vpliv	3
Ugled	4
Časovna občutljivost	5

Minimalne operativne zahteve

Nujno potrebno osebje	IT administratorji (2 za vzdrževanje sistema), podporno osebje (1) za komunikacijo ob izpadu
Osnovne informacijske in komunikacijske storitve	Omrežna povezava, mobilna komunikacija (rezervni kanal), strežniška in oblačna infrastruktura za e-pošto
Nujni dobavitelji, partnerji in dobavne poti	Microsoft (licence, oblačne storitve), internetni ponudnik, pogodbeni vzdrževalci IT sistemov
Zakonski in varnostni pogoji	Skladnost z GDPR, licence za programsko opremo, izvajanje varnostnih ukrepov (avtentikacija, varnostne kopije, požarne pregrade)

Analiza tveganj in ranljivosti

Tveganje	Verjetnost	TOČK	Vpliv	TOČK	Raven tveganja	TOČK
Kibernetski napad	Visoka	4	Visok	4	**Visoko**	**16**
Izpad infrastrukture	Nizka	2	Kritičen	5	**Srednje**	**10**
Človeška napaka	Srednja	3	Srednji	3	**Srednje**	**9**
Dobaviteljsko tveganje	Srednja	3	Visok	4	**Srednje**	**12**

Analiza odvisnosti

Vrsta odvisnosti	Opis
Notranje	Omrežje, požarne pregrade, končne uporabniške naprave...
Zunanje	Internetni ponudnik, Microsoft, AV dobavitelj, dobavitelj električne energije...

Analiza verižnih vplivov

Dogodek	Posledice
Izpad e-pošte	Zamuda v prodajnih pogodbah (finance)
	Prekinjena podpora strankam (ugled)
	Neobdelani osebni podatki (skladnost)

NAČRT NEPREKINJENEGA POSLOVANJA

SPLOŠNO

Načrt neprekinjenega poslovanja je osnovni izvedbeni dokument, ki izhaja iz politike neprekinjenega poslovanja, rezultatov analize vpliva na poslovanje ter ocene tveganj. Vključuje kritične procese v skladu z rezultati analize vplivov na poslovanje, informacijsko-komunikacijske sisteme in pogodbene zunanje izvajalce.

Namen je organizaciji omogočiti, da:

- kljub resnim motnjam ali izrednim dogodkom lahko izvaja svoje kritične procese in poslovanje (vsaj na najmanjši še sprejemljivi ravni),
- hitreje povrne svoje normalno delovanje,
- zmanjša potencialne finančne, operativne in ugledne posledice.

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

2. OMEJITVE PRI IZVAJANJU

Organizacija opredeli potencialne omejitve oz. navede okoliščine, ki bi onemogočile izvajanje načrta neprekinjenega poslovanja.

Primeri:

- razpad kritične komunikacijske infrastrukture v državi,
- izredno ali vojno stanje,
- epidemija ali pandemija, ki povzroči večje pomanjkanje kadra,
- kibernetski napad, ki popolnoma onesposobi ali uniči IKT infrastrukturo,
- …

4. VLOGE IN ODGOVORNOSTI

Organizacija opredeli, kdo je odgovoren za:

PREDSTOJNIK ORGANIZACIJE/ DIREKTOR	KOORDINATOR/ VODJA NEPREKINJENEGA POSLOVANJA	KRIZNA EKIPA	IT ODDELEK/ POGODBENI IZVAJALCI
• potrditev načrta neprekinjenega poslovanja, • imenovanje vodje/koordinatorja neprekinjenega poslovanja, • imenovanje članov krizne ekipe, • dodeljevanje virov, • zagotavljanje skladnosti s predpisi.	• razvoj, posodabljanje in izvajanje načrta neprekinjenega poslovanja, • koordinacijo dela krizne ekipe, • koordinacijo testiranja načrta, • poročanje vodstvu.	• aktivacijo načrta neprekinjenega poslovanja in načrta obnovitve, • koordinacijo odzivnih aktivnosti, • notranjo komunikacijo, • komunikacijo z javnostjo, mediji in pristojnimi organi, • sodelovanje pri testiranju načrta.	• upravljanje varnostnih kopij, • IT podporo, • obnovitev sistemov, • zagotavljanje redundantnih virov, • …

Vsi zaposleni morajo poznati in upoštevati načrt neprekinjenega poslovanja in predpisane protokole, poročati o incidentih in sodelovati v usposabljanjih s tega področja.

5. KOMUNIKACIJSKI NAČRT

Organizacija opredeli načrt komuniciranja v primeru izrednih dogodkov za komunikacijo znotraj in izven organizacije.

- **določitev odgovornosti:**
  - *priprava izjav za medije, priprava predlog sporočil, govorec v kriznih razmerah, potrjevanje izjav,*
- priprava **predlog sporočil** za e-pošto, SMS, spletno stran…
- **protokol internega** obveščanja in poročanja:
  - *kdo, komu, kaj, nadaljnje aktivnosti,*
- protokol obveščanja **izven** organizacije,
- navodila za uporabo **alternativnih komunikacijskih kanalov**, če primarni niso dosegljivi,
- vnaprej pripravljeni **kontaktni seznami**:
  - *krizna ekipa, vodstvo, zaposleni, dobavitelji, mediji, pristojni organi.*

6. INTERNO POROČANJE IN AKTIVACIJA KRIZNE EKIPE

Organizacija opredeli kriterije in postopek za interno obveščanje o incidentih in aktivacijo krizne ekipe.

- **kako poteka obveščanje** o incidentih (kdo obvešča, kako, komu, kdaj),
- protokol za **aktivacijo krizne ekipe in načrta neprekinjenega poslovanja** (kdo, kako, katere informacije posredovati, potrditev, nadaljnje delo),
- **seznam članov** krizne ekipe, s **kontaktnimi podatki in namestniki**,
- **protokol po aktivaciji** načrta neprekinjenega poslovanja in krizne ekipe
  - *npr. ocena situacije, sklic sestanka z relevantnimi, določanje prioritet, obveščanje…*

PROTOKOL INTERNEGA POROČANJA IN AKTIVACIJE KRIZNE EKIPE - PRIMER

1. Zaznavanje in prijava incidenta

- Zazna se incident s strani odgovorne osebe za proces, zaposlenega ali pogodbenega izvajalca.
- Oseba, ki incident zazna, nemudoma obvesti vodjo neprekinjenega poslovanja po ustaljenih kanalih (e-pošta, SMS, telefonski klic, MS Teams).
- Če je incident povezan z informacijsko tehnologijo, se obvesti IT oddelek ali pogodbenega izvajalca. Ta potrdi obseg in vrsto težave.
- Če je ogrožena varnost ljudi ali premoženja, se najprej aktivirajo nujne varnostne službe, nato se poroča vodji neprekinjenega poslovanja.

PROTOKOL INTERNEGA POROČANJA IN AKTIVACIJE KRIZNE EKIPE - PRIMER

2. Aktivacija krizne ekipe

- Vodja neprekinjenega poslovanja po prejemu obvestila oceni resnost dogodka glede na vpliv na ključne procese.
- Če dogodek presega zmogljivosti rednega delovanja ali zahteva koordiniran odziv več enot, se aktivira krizna ekipa.
- Aktivacija se izvede z uradnim sporočilom prek ustaljenih internih kanalov. V sporočilo se navede opis, čas in kraj, stopnjo nujnosti, čas in način prvega sestanka krizne ekipe.
- Aktivacijo potrdi direktor organizacije ali njegov namestnik.
- Krizna ekipa se zbere v najkrajšem možnem času in potrdi aktivacijo Načrta obnovitve in ponovne vzpostavitve delovanja.
- Ob aktivaciji se zabeleži datum, ura, oseba, ki je izvedla aktivacijo in razlog.

PROTOKOL INTERNEGA POROČANJA IN AKTIVACIJE KRIZNE EKIPE - PRIMER

3. Koordinacija po aktivaciji

- Krizna ekipa opravi začetno oceno stanja, določi obseg motnje, prizadete procese, potencialne posledice in prioritetne ukrepe.
- Vodja neprekinjenega poslovanja delegira naloge posameznim članom ekipe in vzpostavi komunikacijo z drugimi deležniki za tehnične ukrepe.
- Član, pristojen za komunikacijo z javnostjo, pripravi osnutek obvestila za zaposlene in zunanje deležnike.
- Direktor organizacije potrdi javna obvestila in odločitve o obsegu aktivacije načrtov neprekinjenega poslovanja ali obnovitve.
- Obveščanje in ukrepanje se izvaja skladno s komunikacijskim načrtom.

PROTOKOL INTERNEGA POROČANJA IN AKTIVACIJE KRIZNE EKIPE - PRIMER

4. Deaktivacija krizne ekipe

- Po stabilizaciji razmer in ponovni vzpostavitvi ključnih procesov, **vodja neprekinjenega poslovanja oceni, ali se lahko zaključi** krizno delovanje.
- Zaključek aktivacije **potrdi direktor** organizacije. Zaposlene in ključne deležnike **obvesti** o povrnitvi v normalno poslovanje.
- Krizna ekipa pripravi **poročilo** o incidentu, ki vsebuje:
  - opis dogodka,
  - vzrok,
  - potek aktivacije in ukrepov,
  - doseženi časi RTO/RPO,
  - pomanjkljivosti in predlogi izboljšav.
- Poročilo se **predstavi poslovodstvu**, se **arhivira** in **uporabi pri naslednjem preverjanju** načrta.

7. KONTAKTNI SEZNAMI

Načrt neprekinjenega poslovanja mora vsebovati kontaktni seznam relevantnih deležnikov (odgovornih oseb in dobaviteljev).

- ključni zaposleni s kontaktnimi podatki (telefonske številke, e-pošta), funkcijami, zadolžitvami,
- ključni dobavitelji z njihovimi storitvami in kontakti.

- **DODATNO:** ponudniki internetnih storitev, vzdrževalci opreme, varnostne službe, zunanji izvajalci.

Kontaktne sezname je treba redno preverjati in posodabljati:

- ob vsaki spremembi glede odgovornih oseb in dobaviteljev,
- ob testiranju načrta neprekinjenega poslovanja (vsaj enkrat letno),
- ob dejanski aktivaciji načrta neprekinjenega poslovanja.

8. POSTOPKI ZA ODZIV NA TIPIČNE INCIDENTE

Del načrta neprekinjenega poslovanja so tudi možni scenariji incidentov, motenj in odzivov, ki služijo:

- določitvi protokolov zaznavanja, razvrščanja in eskalacije incidentov,
- pripravi taktičnih odzivnih načrtov za posamezno vrsto dogodka,
- določitvi nujnih ukrepov za takojšnjo omejitev škode.

Scenarij incidenta/motenj	Opis incidenta/ dogodka	Možni učinki	Odzivni ukrepi
Požar	Požar v poslovnih prostorih ali podatkovnem centru, ki lahko prizadene fizično infrastrukturo (npr. strežnike, pisarne).	Prekinitev dostopa do prostorov, izguba opreme, nevarnost za osebje, okoljski vplivi.	1. Evakuacija in obveščanje gasilcev/intervencijskih služb (takojšnje, v minutah). 2. Aktivacija načrta neprekinjenega poslovanja in preklop na rezervne lokacije. 3. Ocena škode in obnova. 4. Poročanje CSIRT skupini – zgodnje obvestilo. 4. Testiranje in vaje letno; dokumentiranje za izboljšave.
Odpoved ključne strojne opreme	Okvara kritične naprave, npr. strežnika ali omrežne naprave zaradi mehanske napake ali preobremenitve.	Začasna nedelovanje sistemov, izguba produktivnosti, morebitna izguba podatkov.	1. Zaznavanje prek monitoringa in obveščanje IT oddelka/pogodbenega izvajalca (v minutah). 2. Aktivacija načrta neprekinjenega poslovanja in preklop na rezervno opremo (zagotovljena redundanca). 3. Analiza vzroka in popravilo/okrevanje. 4. Poročanje CSIRT skupini – zgodnje obvestilo. 5. Redno vzdrževanje in rezervni deli; post-incidentni pregled za preprečevanje ponovitev.

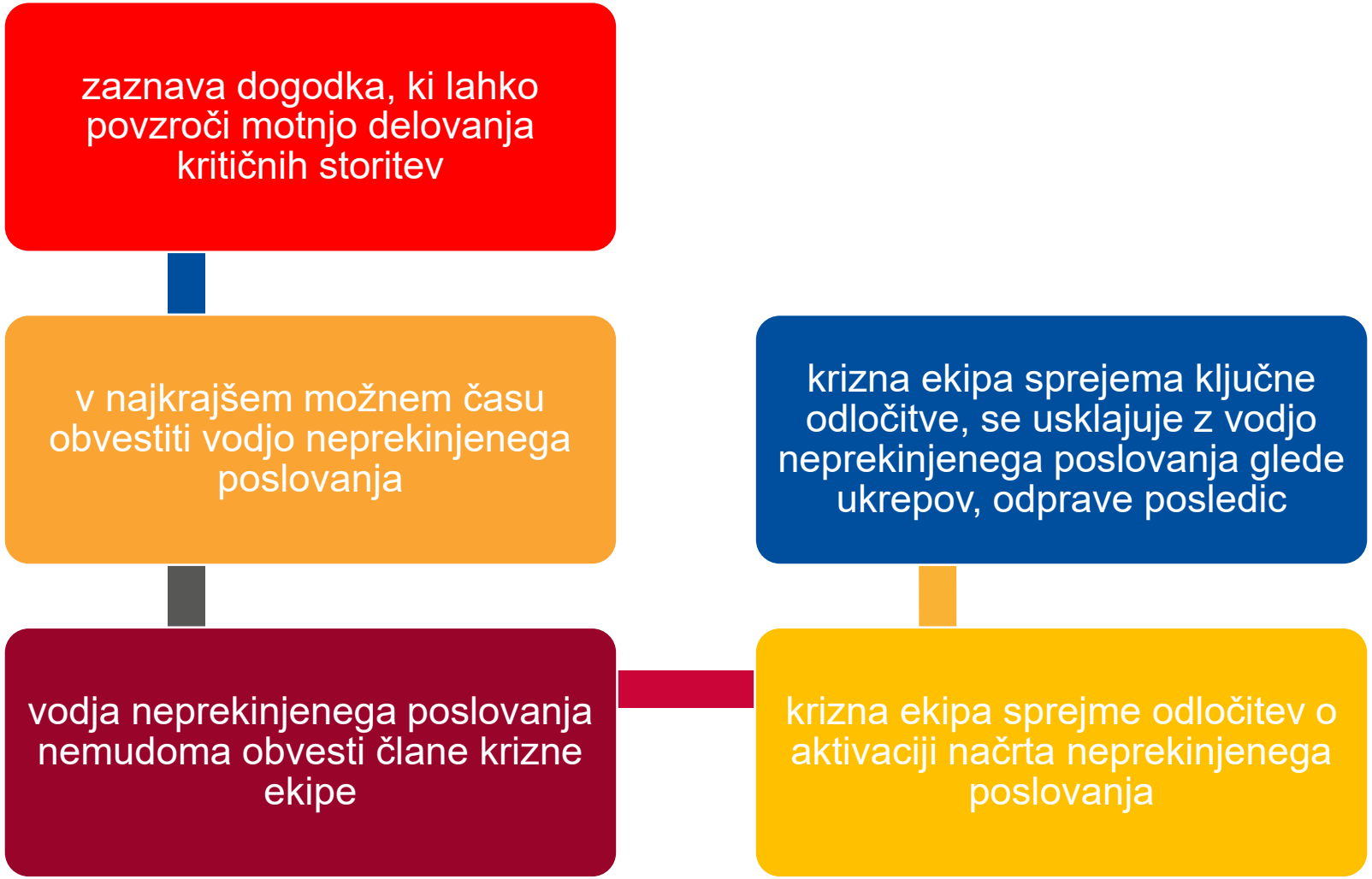
Vir: URSIV

9. NADOMESTNE LOKACIJE IN POSTOPKI ZA PRESELITEV KLJUČNIH PROCESOV

Organizacija z načrtom neprekinjenega poslovanja vnaprej:

- določi sekundarne lokacije za preselitev ključnih procesov ali možnost izvedbe dela na daljavo,
- namesti sisteme, dostope in varnostne politike na nadomestnih lokacijah ali vzpostavi pogoje za delo na domu,
- pripravi načrt logistike za selitev osebja in opreme,
- …

10. AKTIVACIJA NAČRTA NEPREKINJENEGA POSLOVANJA



11. MINIMALNA RAVEN POSLOVANJA IN MINIMALNE OPERATIVNE ZAHTEVE

Minimalna raven poslovanja obsega nujno potrebne poslovne procese, ki omogočajo poslovanje organizacije v izrednih in kriznih razmerah.

- na podlagi popisa in BIA organizacija pripravi seznam teh procesov

Za **vsak kritičen proces** določimo tudi **minimalne operativne zahteve**:

- nujno potrebno osebje,
- osnovne informacijska sredstva in komunikacijske storitve,
- nujni dobavitelji, partnerji, dobavne poti,
- zakonski in varnostni pogoji za delovanje.

12. UPRAVLJANJE VARNOSTNIH KOPIJ IN REDUNDANTNIH ZMOGLJIVOSTI

Upravljanje varnostnih kopij *(glede na dejansko stanje in specifike)*

- redno, vključno s konfiguracijskimi podatki in podatki v oblaku,
- varno shranjevanje, ločeno od glavnega sistema, z ustreznim nadzorom dostopa,
- določitev intervalov/obdobij hrambe (poslovne, regulativne zahteve, rezultati analize obvladovanja tveganj)

Lahko referiramo na drug akt, npr. krovno politiko ali politiko neprekinjenega poslovanja (če je tam opredeljeno).

Primer dobre prakse:

***3** (kopije podatkov) - **2** (vrsti shranjevanja) - **1** (oddaljena lokacija)*

Ni dovolj, da imamo varnostno kopiranje vzpostavljeno - moramo vedeti, kako upravljati z varnostnimi kopijami:

- *zaščita pred zlonamerno programsko opremo,*
- *evidentiranje,*
- *preverjanje celovitosti varnostnih kopij (npr. 1x mesečno),*
- *načrt in testiranje obnovitve iz varnostnih kopij.*

Pomembno: obnovitev podatkov iz varnostne kopije **obvezno iz zadnje čiste** varnostne kopije (prej testirati).

Upravljanje redundantnih zmogljivosti *(glede na dejansko stanje in specifike)*

- zadostni viri (omrežni in informacijski sistemi, opreme, zaloge, usposobljeno osebje)

PRIMERI: *rezervno napajanje, redundatni strežniki, geografsko ločeni podatkovni centri, avtomatski preklop strežnikov, redundanca omrežnih prehodov, neodvisni komunikacijski kanali…*

Ni dovolj, da so redundantne zmogljivosti vzpostavljene, potrebno je z njimi ustrezno upravljati:

- testiranje (preverjanje ustreznosti in zanesljivosti, dokumentiranje rezultatov)
  - ***PRIMERI:*** *načrtovan izklop primarnega napajanja, simulacija izpada primarnega podatkovnega centra, preklop (preverjanje časa preklopa, odziva)…*
- posodabljanje redundantnih sistemov

VZDRŽEVANJE, IZBOLJŠEVANJE IN TESTIRANJE

OBVEZNO PREGLEDOVANJE:

- vsaj enkrat letno,
- ob večjih spremembah,
- ob pojavu izrednih dogodkov, zaradi katerih je bil načrt aktiviran.

KAKO?

- simulacije odziva,
- table-top vaje,
- testiranje polnega preklopa za kritične sisteme,
- analiza uspešnosti po dejanskem incidentu.

CILJ = neprestano izboljševanje

KRIZNO UPRAVLJANJE IN OKREVANJE PO NESREČI

SPLOŠNO

Krizno upravljanje in priprava načrtov obnovitve sta ključna za pravočasno in usklajeno odzivanje na krizne situacije ter zmanjšanje vpliva na poslovanje organizacije.

Načrti obnovitve in ponovne vzpostavitve dopolnjujejo Politiko neprekinjenega poslovanja in Načrt neprekinjenega poslovanja.

Integracija standardov ISO 22301 in ISO 27031 omogoča vzpostavitev strukturiranega okvira, ki združuje poslovne potrebe in tehnične zahteve, kar povečuje odpornost organizacije proti različnim vrstam groženj, od naravnih nesreč do kibernetskih napadov.

NAČRTOVANJE OBNOVITVE V PROCESIH UPRAVLJANJA NEPREKINJENEGA POSLOVANJA

Načrtovanje obnove je ključna sestavina upravljanja neprekinjenega poslovanja (BCM).

- zagotavlja, da organizacija lahko nadaljuje s poslovanjem med in po motnji,
- zmanjšan vpliv na izvajanje storitev organizacije, ugled in deležnike
  - **zmanjšanje izpadov** (hitra obnova poslovnih procesov)
  - **zaščita prihodkov** (ohranjanje ključnih procesov in storitev = manjše finančne izgube)
  - **varovanje ugleda** (ohranitev zaupanja strank in deležnikov z dokazovanjem odpornosti)
  - **skladnost** (zakonske, regulativne in pogodbene obveznosti)

KAKO NAČRTOVATI OBNOVO?

- **Analiza vplivov na poslovanje:**
  - Identifikacija kritičnih procesov,
  - Vrednotenje vplivov motenj na te procese,
  - RTO, RPO.

- **Ocena tveganja:**
  - Prepoznavanje potencialnih groženj,
  - Vrednotenje ranljivosti organizacije na te grožnje,
  - Razvoj strategij za zmanjšanje verjetnosti in vpliva teh groženj.

- **Razvoj obnovitvenih strategij:**
  - Prilagojene potrebam in kritičnim funkcijam organizacije,
  - Preventivni ukrepi, strategije ublažitve, podrobni obnovitveni postopki.

- **Učinkovit komunikacijski načrt** za obveščanje in usklajenost deležnikov med motnjo.

FAZE KRIZNEGA UPRAVLJANJA

- analiza tveganj,
- načrtovanje,
- usposabljanje in ozaveščanje.

PRIPRAVA

1. Identificirajte grožnje in ranljivosti, ocenite tveganja.
2. Vzpostavite politike in načrte obnovitve s postopki odzivanja na različne vrste incidentov, določite vloge in odgovornosti in komunikacijske strategije.
3. Redno usposabljajte osebje o postopkih in potencialnih grožnjah.

- aktivacija kriznega načrta,
- vzpostavitev krizne skupine,
- komunikacija,
- operativni ukrepi.

ODZIVANJE

1. V primeru krize takoj aktivirajte načrt obnovitve in obvestite ključne deležnike.
2. Sestavite ekipo za odzivanje, ki koordinira odziv, ter določite posamezne vloge.
3. Zagotovite jasno in pravočasno komunikacijo z notranjimi in zunanjimi deležniki.
4. Izvedite potrebne ukrepe za zaščito ljudi, premoženja, informacijskih virov.

FAZE KRIZNEGA UPRAVLJANJA

- ocena škode,
- obnovitveni ukrepi,
- analiza po krizi

OBNOVA

1. Ocenite obseg škode,
2. Določite prednostne naloge za obnovo,
3. Izvedite ukrepe za obnovo kritičnih procesov, storitev in sistemov
4. Opravite analizo odziva in identificirajte potencialne izboljšave.

- pregled načrtov,
- stalno usposabljanje,
- izboljšave procesov.

IZBOLJŠAVE

1. Na podlagi pridobljenih izkušenj preglejte in posodobite načrte obnovitve.
2. Nadaljujte z usposabljanjem osebja in organiziranjem vaj.
3. Implementirajte ugotovitve iz analiz in vaj v obstoječe postopke in načrte.

ELEMENTI NAČRTA OBNOVITVE IN PONOVNE VZPOSTAVITVE

Namen načrta je obnovitev in ponovna vzpostavitev delovanja, hitra in uspešna obnova po prekinitvah zaradi nepredvidenih dogodkov ali motenj.

- strukturiran pristop k ohranjanju in ponovni vzpostavitvi ključnih omrežnih in informacijskih sistemov v primeru nepredvidljivih dogodkov, ki povzročajo motnje ali prekinitev delovanja ključnih/kritičnih poslovnih procesov/funkcij.
- osredotočen na tehnično-informacijske vidike obnove.

Načrt mora biti **usklajen** s Politiko neprekinjenega poslovanja, Načrtom neprekinjenega poslovanja in rezultati analize vpliva na poslovanje.

OMEJITVE PRI IZVAJANJU

Organizacija opredeli potencialne omejitve, zaradi katerih ne bi bilo mogoče izvajati načrta obnovitve in ponovne vzpostavitve.

Primer: Če delno ali v celoti ne bi bilo možno izvajati Načrta neprekinjenega poslovanja (tam opredeljeno, kdaj ga ne moremo izvajati).

OBSEG NAČRTA

Organizacija opredeli obseg načrta obnovitve in ponovne vzpostavitve.

Primer:

- Vloge in odgovornosti,
- komunikacijski postopki,
- protokol aktivacije ekipe za obnovo,
- kontaktni seznami,
- postopki za obnovo ključnih sistemov (+redundanca in nadomestne lokacije),
- protokoli odzivanja na tipične incidente (izpad strežnikov, požar, kibernetski napad),
- obnova varnostnih kopij in testiranje obnove.

Vključeni prej identificirani **omrežni in informacijski sistemi** (fokus na kritičnih).

Upravljanje s postopkovniki za vzpostavitev normalnega delovanja za posamezen omrežni in informacijski sistem – *Primer: za vsak posamezni sistem varno shranjen postopkovnik z določenimi koraki za vzpostavitev normalnega delovanja.*

VLOGE IN ODGOVORNOSTI

Funkcija	Odgovornosti
Direktor/predstojnik organizacije	Potrdi načrt obnovitve in ponovne vzpostavitve delovanja omrežnih in informacijskih sistemov; s sklepom določi vodjo obnove IT sistemov; s sklepom imenuje ekipo za obnovo IT sistemov; dodeli potrebne vire; zagotovi skladnost z zakonodajo.
Vodja obnove IT sistemov	Skrbi za razvoj, posodabljanje in izvajanje načrta obnovitve in ponovne vzpostavitve delovanja omrežnih in informacijskih sistemov; aktivira in koordinira ekipo za obnovo IT sistemov; organizira testiranje načrta; poroča vodstvu.
Krizna ekipa	Aktivira Načrt obnovitve in ponovne vzpostavitve delovanja omrežnih in informacijskih sistemov; sodeluje z vodjo obnove IT sistemov; izvaja notranjo komunikacijo.
Ekipa za obnovo IT sistemov	Izvaja aktivnosti za obnovo in ponovno vzpostavitev delovanja IT sistemov; vključuje pogodbene izvajalce; sodeluje pri testiranju načrta.
IT oddelek/pogodbeni izvajalci	Ekipi za obnovo nudi vso potrebno podporo pri izvajanju aktivnosti za obnovitev sistemov.

Vir: URSIV

Dodatno:

- kdo je vodja obnove v primeru aktivacije načrta,
- jasno določiti odgovornosti za odločanje in usmerjanje med krizo.
- kdo sestavlja ekipo za obnovo,
- jasne naloge operativnega osebja za odzivanje in obnovo.

KONTAKTNI SEZNAMI

Organizacija glede na področne posebnosti oz. dejansko stanje pripravi kontaktne sezname, ki se jih uporabi v primeru aktivacije načrta.

Primer:

- Ključni zaposleni s kontaktnimi podatki (telefonske številke s stalno dosegljivostjo, e-pošta), funkcijami, zadolžitvami.
- Ključni dobavitelji s storitvami in kontaktnimi podatki.
- Ponudniki internetnih storitev, vzdrževalci opreme, zunanji izvajalci.

Podatke je treba redno pregledovati in posodabljati.

KOMUNIKACIJSKI NAČRT

Organizacija mora imeti jasne protokole komunikacije znotraj in izven organizacije.

- **Notranja komunikacija:** jasne komunikacijske linije znotraj organizacije.
- **Zunanja komunikacija:** strategije za obveščanje javnosti, strank, dobaviteljev in drugih deležnikov.
- **Medijska komunikacija:** pravila komuniciranja z mediji, priprava izjav za medije in določitev osebe, ki bo v kriznih situacijah komunicirala z mediji.

POSTOPKI ZA OBNOVO IN PONOVNO VZPOSTAVITEV

Organizacija pripravi tipične scenarije dogodkov, ki povzročijo aktivacijo načrta. Pripravijo se standardni postopki, ki jim je treba slediti v primeru aktivacije.

Primer:

- *Prioriteta:* obnova na primarni lokaciji, če je to časovno in operativno najbolj učinkovito.
- Če na primarni lokaciji ne bo uspešno ali bo trajalo predolgo, se prične z obnovo na nadomestni lokaciji.
  - **ODLOČITEV:** krizna ekipa v posvetovanju z vodjo obnove

- za posamezne informacijske sisteme ali sredstvo se izdela Navodilo za obnovo sistema po korakih – varno hranimo na vsaj dveh lokacijah, dostopno vodji obnove, članom krizne ekipe, članom ekipe za obnovo IT sistemov.

- za IT naprave, ki rabijo konfiguracijsko datoteko, hranimo aktualne produkcijske datoteke na dveh varnih in ustrezno oddaljenih mestih. Dostopno vodji obnove, članom krizne ekipe, članom ekipe za obnovo IT sistemov.

Primer: Izpad komunikacij

Upoštevamo najboljše prakse za alternativne kanale in hiter preklop.

1. Zaznava izpada	Uporabimo monitoring (npr. „ping“ teste) za potrditev. Ocenimo vpliv na IT storitve (npr. dostop do oblaka).
2. Preklop na alternativne poti	Aktiviramo redundančne povezave (npr. mobilni podatki, sekundarni ISP), konfiguriramo VPN preko drugega kanala.
3. Obnovitev primarne komunikacije	Kontaktiramo ponudnika za popravek. Testiramo obnovo – preverimo hitrost in varnost.
4. Validacija sistemov	Preverimo dostop do aplikacij in podatkov. Sinhroniziramo zamujene transakcije.
5. Optimizacija za prihodnost	Posodobimo redundanco (npr. dodamo več ponudnikov). Dokumentiramo incident.

VIRI IN OPREMA

Organizacija mora opredeliti, kateri viri in oprema so potrebni za obnovitev in ponovno vzpostavitev delovanja.

- **Zmogljivosti:** identifikacija potrebnih virov in opreme za odzivanje na krize.
- **Dostopnost:** zagotovitev, da so viri in oprema dostopni ter pripravljeni za uporabo v vsakem trenutku.

AKTIVACIJA NAČRTA

Organizacija navede, kakšni pogoji morajo biti izpolnjeni za aktivacijo načrta obnovitve in ponovne vzpostavitve.

Primer:

- po zaznavi dogodka, ki je povzročil motnje delovanja bistvenih oziroma kritičnih storitev.

- **ODLOČITEV O AKTIVACIJI:** krizna ekipa.
  - Sprejema vse ključne odločitve,
  - Se usklajuje z vodjo obnove IT sistemov.

VZDRŽEVANJE, IZBOLJŠEVANJE IN TESTIRANJE

Organizacija opredeli intervale in načine pregledovanja, testiranja in posodabljanja načrta.

PREGLED:

- Najmanj enkrat letno,
- ob večjih spremembah,
- ob pojavu izrednih dogodkov.

TESTIRANJE za izboljšanje pripravljenosti:

- Redne simulacije in testiranja (npr. dve testiranji letno),
- redno testiranje sistemov rezervnega napajanja (UPS, dizelski agregati).

Po vsakem pomembnem incidentu se izvede analiza uspešnosti in uvedejo izboljšave.

ŠTUDIJA PRIMERA

ŠTUDIJA PRIMERA: IZPAD PODATKOVNEGA CENTRA

Namen:

Testiranje odpornosti organizacije, odzivanja na krizne dogodke in zmožnosti zagotavljanja neprekinjenega delovanja (BCP/DRP) v skladu z zahtevami ZInfV-1/NIS2.

POTEK NAMIZNE VAJE – ČASOVNI INJEKCIJI

Čas (injiciranje)	Dogodek	Pričakovan odziv / odločitev
T+0 min	Popoln izpad primarnega podatkovnega centra (DC1)	Razglasitev večjega incidenta, aktivacija incidentne ekipe
T+15 min	Napaka UPS sistema – rezervno napajanje odpove	Aktivacija DRP, eskalacija vodstvu
T+30 min	Sum na ransomware v dnevnikih SIEM	Razglasitev kibernetskega incidenta + vključitev CERT/SOC
T+45 min	Vodstvo zahteva oceno vpliva	Upoštevaj rezultate BIA za prioritete
T+60 min	Nedelovanje e-pošte	Aktivacija alternativne komunikacije (SMS, Teams, telefon)
T+90 min	Dobavitelj backup rešitev zamuja s podporo	Aktivacija plana tveganj dobavne verige
T+120 min	Mediji zahtevajo odziv podjetja	Sprožitev kriznega komuniciranja
T+180 min	Negotovost glede integritete varnostnih kopij	Preverjanje RPO in varnosti podatkov
T+240 min	Prizadeti uporabniki zahtevajo RTO čas	Komuniciranje realnih časov obnovitve

KLJUČNE ODLOČITVENE TOČKE

Udeleženci morajo razpravljati o:

- Kdaj razglasiti **krizo** in aktivirati krizno vodenje?
- Kako **prioritizirati obnovo sistemov** glede na BIA?
- Kako vzpostaviti **komunikacijo ob izpadu IT sistemov**?
- Kako zagotoviti **koordinacijo IT + poslovanje + varnost**?
- Ali je treba dogodek **prijaviti** v skladu z **ZInfV-1 (24 ur / 72 ur)**?

POVEZAVA Z ZAHTEVAMI ZINFV-1/NIS2

Zahteva	Povezava z vajo
Upravljanje tveganj (21. člen NIS2)	Vaja temelji na rezultatih BIA in ocene tveganj
BCP/DRP – načrt neprekinjenega poslovanja (14. člen ZInfV-1)	Preverja zmožnost aktivacije postopkov
Odzivanje na incidente (Incident Response)	Testira aktivacijo IR procesa
Tveganja dobavne verige (NIS2)	Vaja vključuje odvisnost od dobaviteljev
Operativna odpornost	Preverja stabilnost ključnih storitev
Krizno komuniciranje	Aktivira notranje in zunanje komuniciranje
Prijava incidentov (24/72 ure)	Preverja, kdaj je treba incident uradno prijaviti

HVALA ZA POZORNOST