EUROPEAN UNION AGENCY
FOR CYBERSECURITY

DELAVNICA „SKLADNOST Z ZINFV-1

Delavnica 3: Načrt varnostnih ukrepov in presoja njihove učinkovitosti (prva ponovitev)

Andreja Markun, Telekom Slovenije
Božidar Dajčman, ICS

MODULARNI RAZPORED DELAVNIC

MODUL 1

DELAVNICA 1/1
Osnovne politike & upravljanje tveganj
28. JAN 2026

DELAVNICA 1/2
Osnovne politike & upravljanje tveganj
04. FEB 2026

MODUL 2

DELAVNICA 2/1
Odpornost & načrtovanje odziva na incidente
11. FEB 2026

DELAVNICA 2/2
Odpornost & načrtovanje odziva na incidente
24. FEB 2026

MODUL 3

DELAVNICA 3/1
Varnostni ukrepi & ocenjevanje učinkovitosti
03. MAR 2026

DELAVNICA 3/2
Varnostni ukrepi & ocenjevanje učinkovitosti
11. MAR 2026

MODUL 1: VSEBINA

VSEBINA

- Ključne obveznosti zavezancev s poudarkom na pripravi varnostne dokumentacije (8 obveznih sestavin)
- Priprava krovne varnostne politike
- Upravljanje in popis informacijskih sredstev
- Analiza in upravljanje tveganj

MODUL 1: OBRAZLOŽENI PRIMERI

Popis sredstev

IS_ID	Sredstvo	Vrsta sredstv	Osnovna storitev				
IT-DAT-001	SQL baza	Podatkovni	Hramba podatkov	5	5	5	5
IT-DAT-001	SQL baza	Podatkovni	Hramba podatkov	5	5	5	5
IT-DAT-001	SQL baza	Podatkovni	Hramba podatkov	5	5	5	5
IT-DAT-006	Telefonski	Podatkovni	Kontakti	1	1	2	1
SEC-002	EDR	Varnostni sistem	Zaščita endpointov	4	4	5	4
IT-APP-008	E-arhiv	Aplikacija	Hramba dokumentov	4	5	3	4
IT-APP-008	E-arhiv	Aplikacija	Hramba dokumentov	4	5	3	4
IT-APP-003	HRM	Aplikacija	Kadri	5	5	4	5
IT-INF-011	Mobilne	Infrastruktura	Mobilni dostop	3	3	4	4
IT-INF-011	Mobilne	Infrastruktura	Mobilni dostop	3	3	4	4
IT-INF-006	WiFi omrežje	Infrastruktura	Povezljivost	3	3	4	3
IT-INF-013	Testni strežnik	Infrastruktura	Testno okolje	2	2	2	2
OT-011	HVAC	OT sistem	Klimatizacija	3	3	5	3
OT-011	HVAC	OT sistem	Klimatizacija	3	3	5	3
OT-009	EMS	OT sistem	Energetski nadzor	4	4	4	4

Analiza tveganj

Ranljivost	Grožnja	Vpli	Verjetnost (INH)	Tveganje (INH)	Že uvedene kontrole	Verjetnost (REZ)	Tveganje (REZ)	Izbrana strategija
Dinamične poizvedbe	SQL Injection / neustrezna validacija	5	3	15	Patch management, hardening	2	10	Zmanjšanje tveganja
Ni HA	Izpad baze / okvara infrastrukture	5	2	10	Backup, monitoring	1	5	Sprejem tveganja
Šibek RBAC; manjkajoča MFA	Neavtoriziran dostop do baze	5	3	15	Osnovni RBAC (Role-Based Access Control), ločeni	2	10	Sprejem tveganja – izjema
Ni SLA	Izpad storitve	2	2	4	Osnovni nadzor	1	2	Sprejem tveganja
Agent out-of-date	Nepravočasne posodobitve	5	3	15	Centralno upravljanje	2	10	Zmanjšanje tveganja
Šibek nadzor vlog	Neavtoriziran dostop	5	3	15	RBAC, logging	2	10	Zmanjšanje tveganja
Neustrezen backup	Izguba podatkov	5	2	10	Backup	1	5	Sprejem tveganja
Premalo stroge vloge	Neavtoriziran dostop	5	3	15	RBAC,			
Neenotna MDM politika	Kompromitacija mobilne naprave	4	3	12	MDM, šifriranje			
Brez centralnega nadzora geolokacije	Izguba/kraja mobilne naprave	4	3	12	MDM remote			
Brez WIPS (Wireless Intrusion	DoS motnje na WiFi	4	2	8	RF (Radio Frequ			
Neredno patchanje	Zakasneli patchi v testnem okolju	2	3	6	Osnovni patchir			
Enojna klima; brez N+1	Izpad HVAC → pregrevanje strežnikov	5	3	15	Osnovni alarmi BMS			
Privzeta gesla	Neavtoriziran oddaljen dostop do HVAC	5	2	10	VPN; omeje			
Nepodpisani podatkovni tokovi	Manipulacija odčitkov energije	4	3	12	RBAC; osnov			

Akcijski načrt

Zahtevani dodatni ukrepi	Nosilec	Rok izvedb	Možni KPI za spremljanje tveganja
WAF; pentest	Vodja DBA	2026-07-12	Brez kritičnih SQLi ranljivosti (CVSS ≥
			RTO ≤ 1 h; RPO ≤ 15 min; uspešen DR
Za možne ukrepe (MFA; strožji RBAC) ni na razpolago			0 nepooblaščenih dostopov v 6 mesecih
			MTTR ≤ 4 h; ≤1 izpad/kvartal
Avtomatizacija update; compliance report; SIEM	Vodja IT INFR	2026-07-12	>= 98% agentov posodobljenih < 7 dni
strožji RBAC; revizija pravic	Direktor Zalednih	2026-07-12	0 kršitev dostopa; uspešni revizijski
			Uspešen restore test; RPO ≤ 24 h
strožji RBAC; MFA;	Vodja HR	2026-07-12	0 PII incidentov; uspešni GDPR pregledi
			0 kompromitacij; 100% MDM compliance
			100% remote wipe izveden
			≤1 incident/kvartal
			100% patch compliance
Preventivno vzdrževanje; uvedba N+1 redundance;	Direktor REM	2026-07-12	MTTR ≤ 1 h; 0 kritičnih izpadov
			0 nepooblaščenih dostopov
			0 napak v odčitkih

PREGLED MODULA 2 (PREJŠNJA DELAVNICA)

KIBERNETSKA ODPORNOST IN NAČRTOVANJE ODZIVA NA INCIDENTE

NEPREKINJENOST POSLOVANJA IN OKREVANJE PO NESREČI

- Analiza vplivov na poslovanje
- Načrt neprekinjenega poslovanja
- Načrt okrevanja po nesreči
- Časovni okviri (RPO, RTO)
- Primeri izdelave dokumentacije

DOKUMENTIRAN SISTEM ZA ODZIVANJE NA INCIDENTE

- Načrt odzivanja na incidente
- Zahteve glede obveščanja
- Povezovalne točke pri odzivanju na incidente
- Praktični primer odziva (simuliran incident)

BIA

Analiza vplivov na poslovanje (BIA) je osnova za vzpostavitev in vzdrževanje sistema upravljanja neprekinjenega poslovanja (SUNP).

NAMEN BIA:

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

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

Dokument podpiše in potrdi vodstvo organizacije.

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

O NAČRTU

Načrt neprekinjenega poslovanja je osnovni izvedbeni dokument, ki izhaja iz politike neprekinjenega poslovanja, rezultatov analize vpliva na poslovanje ter ocene tveganj.

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.

Dokument podpiše oz. potrdi vodstvo organizacije.

ELEMENTI NAČRTA NEPREKINJENEGA POSLOVANJA

- opredelitev omejitev za izvajanje načrta
- določitev obsega (ključni poslovni procesi)
- določitev ključnih vlog in odgovornosti
- opredelitev postopkov za zagotavljanje neprekinjenega poslovanja
- opredelitev ciljev in kazalnikov uspešnosti
- opredelitev dokumentacije za podporo sistemu neprekinjenega poslovanja
- opredelitev postopkov za redno preverjanje, testiranje, izboljševanje, pregledovanje in posodabljanje

OCENA KRITIČNOSTI POSLOVNIH PROCESOV

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

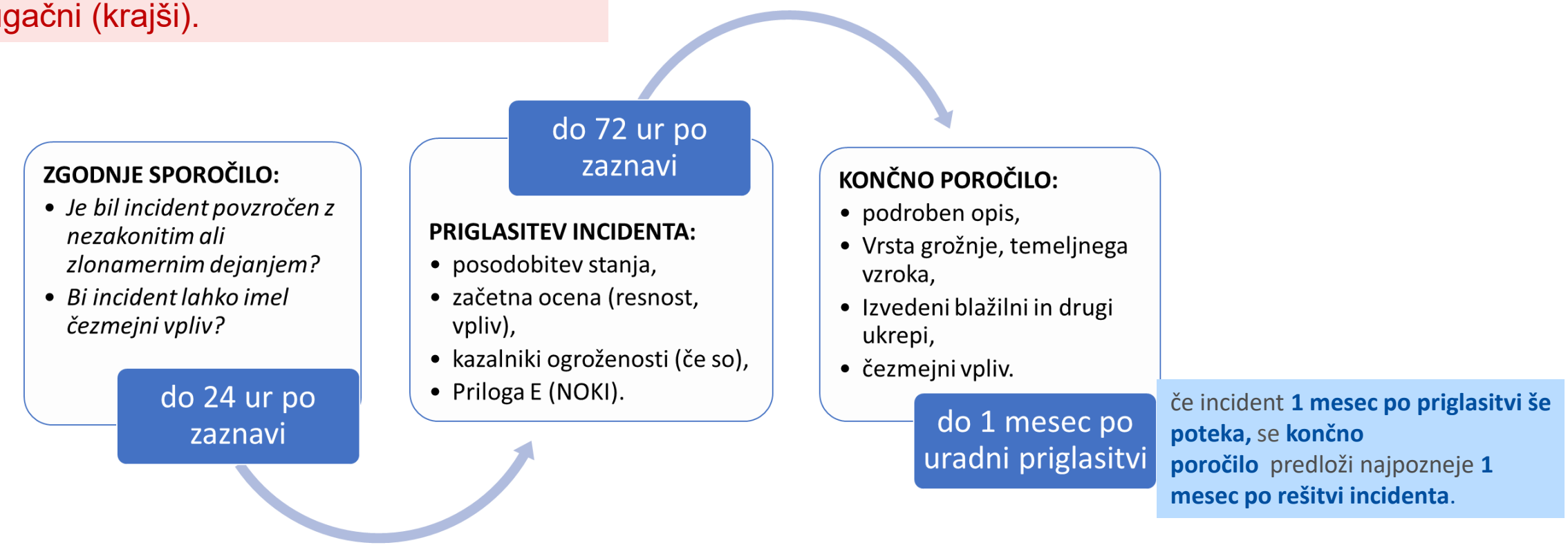
- *Kako bi izpad procesa vplival na poslovanje in zagotavljanje storitev?*

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…

OBVEŠČANJE SKUPINE CSIRT

POZOR: za določene subjekte so roki drugačni (krajši).



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

URNIK

Čas	Aktivnost	Izvajalec
9:00 – 9:10	Predstavitev in namen delavnice	Andreja Markun, Telekom Slovenije Božidar Dajčman, ICS
9:10 – 10:30	Načrt varnostnih ukrepov	Andreja Markun, Telekom Slovenije
10:30 – 11:00	Pregled primerov	Božidar Dajčman, ICS
11:00 – 11: 15	Odmor za kavo	
11:15 – 12:15	Postopki za presojo učinkovitosti varnostnih ukrepov	Andreja Markun, Telekom Slovenije
12:15 – 12: 45	Pregled primerov	Božidar Dajčman, ICS
12:45 – 13:00	Vprašanja in diskusija	
13:00	Zaključek	Andreja Markun, Telekom Slovenije

CILJI DELAVNICE 3: NAČRT VARNOSTNIH UKREPOV IN PRESOJA NJIHOVE UČINKOVITOSTI

Udeležencem omogočiti, da **razumejo in znajo v praksi povezati**:

- **načrt varnostnih ukrepov**,
- in **presojo učinkovitosti teh ukrepov**, v skladu z zahtevami **ZInfV-1**
- **praktični primeri**