EUROPEAN UNION AGENCY
FOR CYBERSECURITY

DELAVNICA „SKLADNOST Z ZINFV-1

Delavnica 1: Temeljne politike & Upravljanje tveganj (povzetek)

Dr. Denis ČALETA, ICS-Ljubljana
Božidar Dajčman, ICS-Ljubljana

11 | 02 | 2026

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

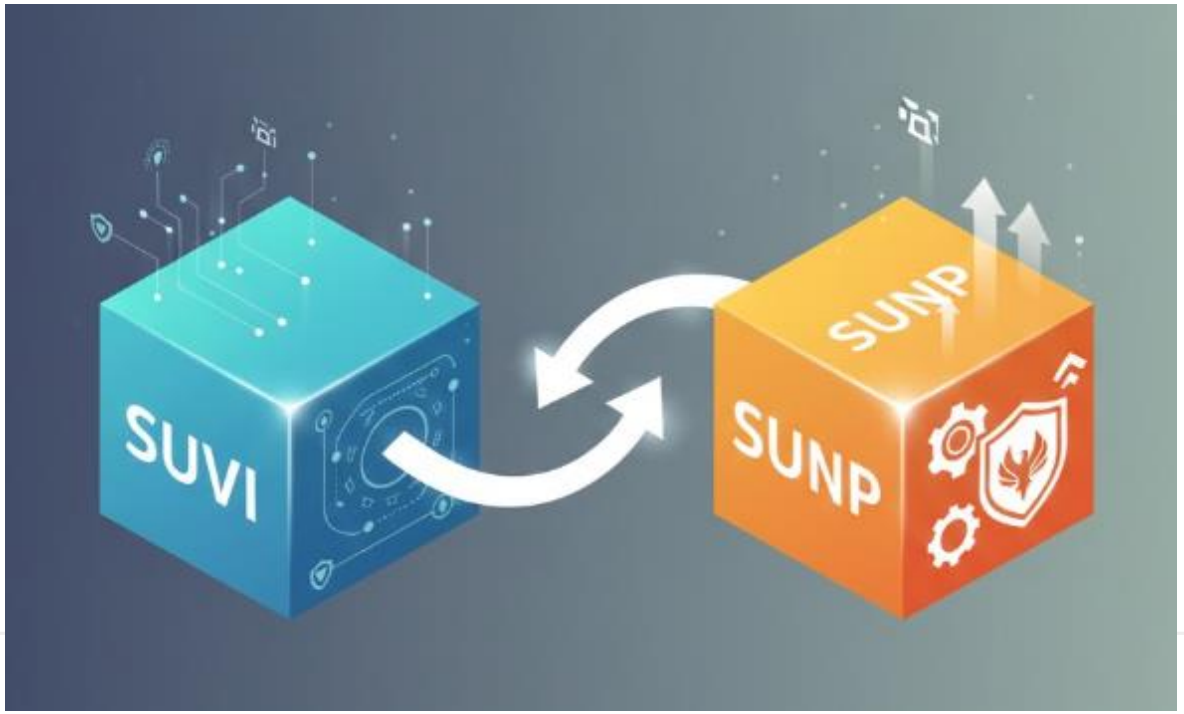
DELAVNICA 3/2
Varnostni ukrepi & ocenjevanje učinkovitosti
11. MAR 2026

VSEBINA MODULA 1 (PREJŠNJA DELAVNICA)

Čas	Aktivnost	Izvajalec	Opombe
09:00-09:10	Predstavitev cilji in namen delavnice	Denis Čaleta (ICS)	
09:10-09:30	Uvod z opredelitvijo ključnih obveznosti zavezancev s poudarkom na pripravi varnostne dokumentacije	Božidar Dajčman (ICS)	
09:30-10:00	Priprava krovne varnostne politike	Denis Čaleta (ICS)	
10:00-11:00	Upravljanje in popis informacijskih sredstev	Denis Čaleta (ICS)	
11:00-11:15	Odmor za kavo		
11:15-12:45	Analiza in upravljanje tveganj	Božidar Dajčman (ICS)	
12:45-13:00	Vprašanja in diskusija	Vsi udeleženi	
13:00	Zaključek	Denis Čaleta (ICS)	

VARNOSTNA DOKUMENTACIJA (21. ČLEN)

Bistveni in pomembni subjekti za zagotavljanje visoke ravni informacijske in kibernetske varnosti ter odpornosti svojih omrežnih in informacijskih sistemov vzpostavijo in vzdržujejo dokumentirani **sistem upravljanja varovanja informacij** in **sistem upravljanja neprekinjenega poslovanja.**



VARNOSTNA DOKUMENTACIJA – OBVEZNE SESTAVINE

1. Politika ali področne politike o varnosti omrežnih in informacijskih sistemov
2. Popis informacijskih sredstev in podatkov
3. Analiza obvladovanja tveganj
4. Politika in načrt neprekinjenega poslovanja
5. Načrt obnovitve in ponovne vzpostavitve delovanja
6. Načrt odzivanja na incidente s protokolom obveščanja CSIRT
7. Načrt varnostnih ukrepov
8. Politika s postopki za presojo učinkovitosti varnostnih ukrepov

TIPIČNA STRUKTURA POLITIKE

Namen in področje uporabe – kaj in koga politika zavezuje

- ✓ **Pravna in normativna skladnost** – ZInfV-1, GDPR, ISO/IEC 27001 itd.
- ✓ **Varnostni cilji** – celovitost, avtentičnost, zaupnost in razpoložljivost informacij
- ✓ **Upravljavski okvir** – struktura odgovornosti in poročanja
- ✓ **Načela upravljanja tveganj** (ISO 31000 ali NIST)
- ✓ **Načela zaščite informacijskih sistemov**
- ✓ **Ukrepi za odzivanje na incidente**
- ✓ **Varnost dobavne verige**
- ✓ **Izobraževanje in ozaveščanje zaposlenih**
- ✓ **Vzdrževanje in pregled politike**

SEKTORSKE – PODROČNE POLITIKE

Politika informacijske varnosti je lahko razdeljena na več **področnih varnostnih politik**, ki urejajo posamezna področja varnosti:

- Politika ozaveščanja in usposabljanja
- Politika varnosti dobavne verige
- Politika nadzora dostopa
- Politika ravnanja s sredstvi
- Politika varnosti človeških virov
- Politika fizične in okoljske varnost
- Politika upravljanja z ranljivostmi in posodobitvami
- Politika varnostnega kopiranja
- Politika kriptografije
- Politika zaščite pred zlonamerno programsko opremo
- Politika neprekinjenega poslovanja in obvladovanja nesreč
- Politika spremljanja in evidentiranja revizijskih sledi
- Politika uporabe ITK sredstev
- Politika uporabe oblačnih storitev
- Politika uporabe brezžičnih omrežij
- Politika dela od doma in na oddaljenih lokacijah
- Politika čiste mize in zaklepanja zaslona

KAJ OBSEGA POPIS SREDSTEV

Dejavnost/storitev: kaj organizacija izvaja (opis, lastnik, kritičnost, SLA).

- **Informacijska sredstva**: podatkovni nizi (opis, ZCRA, pravna podlaga/retencija, lokacija).
- **Informacijski sistem (IS)**: aplikacije in sistemi, ki obravnavajo IP (skrbnik, upravljavec, ključne komponente).
- **Infrastruktura**: strežniki/VM, baze, omrežje, varnostne naprave, oblak (računi/viri).
- **Identitete/računi**: skrbniški, storitveni, aplikativni računi (pravice/MFA).
- **Dobavitelji/partnerji**: pogodbe (SLA), integracije, odgovorne osebe.

PRIMER POPISA SREDSTEV

IT IFRASTRUKTURA:

IS_ID	Informacijsko sredstvo	Lastnik	Skrbnik	Glavne funkcije	HW	SW	Z	C	R	A	Opombe
IT-INF-001	Fizični strežniki	Vodja IT	Sistem. admin	Gostovanje aplikacij	Strežniki	Linux/Windows	4	4	5	5	Kritično za poslovanje
IT-INF-002	Virtualizacijska platforma	Vodja IT	IT admin	Virtualizacija	VMware cluster	vSphere	4	4	5	4	Ključno jedro infrastrukture
IT-INF-003	SAN/NAS hramba	Vodja IT	Storage admin	Hramba podatkov	SAN/NAS	StorageOS	5	5	5	4	Vključeno v BC/DR
IT-INF-004	LAN omrežje	Vodja IT	Omrežni admin	Interna povezljivost	Switche	IOS	4	4	5	5	Osnovna komunikacijska infrastruktura
IT-INF-005	WAN/VPN	Vodja IT	Omrežni admin	Povezava lokacij	Routerji	Firmware	4	4	5	4	Ključno za oddaljeni dostop
IT-INF-006	WiFi omrežje	Vodja IT	Omrežni admin	Brezžična povezljivost	AP	Controller	3	3	4	3	Podporno sredstvo
IT-INF-007	DNS/DHCP storitve	Vodja IT	Sistem. admin	Omrežne storitve	VM	Bind/DHCP	4	4	5	5	Kritična omrežna storitev
IT-INF-008	E-poštni sistem	Vodja IT	Sistem. admin	Komunikacija	Cloud	Exchange	4	4	5	5	Zunanji izvajalec
IT-INF-009	VoIP telefonija	Vodja IT	IT tehnik	Telefonija	VoIP	CallManager	3	3	4	3	Podporno sredstvo
IT-INF-010	Backup sistem	Vodja IT	Backup admin	Backup/Restore	NAS	Veeam	5	5	5	4	Vključeno v BC/DR
IT-INF-011	Mobilne naprave	Vodja IT	IT admin	Mobilna komunikacija	Telefoni	MDM	3	3	4	4	Upravljano preko MDM
IT-INF-012	Gostujoče WiFi	Vodja IT	Omrežni admin	Gostujoči dostop	AP	Controller	1	1	2	1	Nizka kritičnost
IT-INF-013	Testni strežnik	Vodja IT	IT admin	Testiranje	VM	Various	2	2	2	2	Ni produkcijski
IT-INF-014	Dev strežnik	Vodja IT	DevOps	Razvoj	VM	Dev tools	2	2	2	2	Testno okolje
IT-INF-015	Tiskalniški sistem	Vodja IT	IT admin	Tiskanje	VM	Print server	1	1	2	1	Podporno sredstvo

IT APLIKACIJE

IS_ID	Aplikacija	Lastnik	Skrbnik	Glavne funkcije	HW	SW	Z	C	R	A	Opombe
IT-APP-001	ERP	Direktor financ	IT admin	Finance, nabava	Strežnik	ERP Suite	5	5	5	5	Kritično za poslovanje
IT-APP-002	CRM	Vodja prodaje	IT admin	Upravljanje strank	VM	CRM	4	4	4	4	Ključno za prodajo
IT-APP-003	HRM	Vodja kadrov	HR admin	Kadri	VM	HRM Pro	5	5	4	5	Vključuje osebne podatke (GDPR)
IT-APP-004	DMS	Vodja kakovosti	DMS admin	Dokumenti	VM	DMS	4	5	4	4	Poslovna dokumentacija
IT-APP-005	Helpdesk	Vodja IT	IT admin	Podpora	VM	Jira	3	3	4	3	Podporno sredstvo
IT-APP-006	BI/Analitika	Direktor	BI analitik	Analize	VM	BI Tools	3	4	4	4	Podporno sredstvo

OCENA TVEGANJ PO SREDSTVIH

Za vsako sredstvo ali skupino (enakih) sredstev se ugotavljajo:

- **grožnje in ranljivosti**;
- **vpliv** na izgubo zaupnosti, celovitosti, razpoložljivosti in avtentičnosti (ZCRA);
- **verjetnost** uresničenja grožnje ter posledice za poslovanje in
- **ocena (faktor) tveganja** in ustrezni ukrepi za njegovo zmanjšanje ali sprejem.

REZULTAT IZVEDENE ANALIZE TVEGANJ IN IZVAJANJE UKREPOV

Rezultat analize tveganj je **register tveganj**.

Vključuje:

- naziv sredstva (ali skupine sredstev) na katerega se tveganje nanaša,
- lastnika sredstva/tveganja,
- opis tveganja,
- vpliv v primeru kršitve zaupnosti, celovitosti, razpoložljivosti in avtentičnosti (ZCRA).
- oceno verjetnosti realizacije grožnje,
- faktor inherentnega tveganja,
- predlagane ukrepe za zmanjšanje tveganj, prenos ali sprejem tveganj,
- faktor rezidualnega tveganja,
- rok za realizacijo ukrepov.

REGISTER TVEGANJ - PRIMER

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	Popis sredstev								Analiza tveganj								
2	IS_ID	Sredstvo	Vrsta sredstva	Osnovna storitev	Z	C	I	A	Ranljivost	Grožnja	Vpli	Verjetnost (INH)	Tveganje (INH)	Že uvedene kontrole	Verjetnost (REZ)	Tveganje (REZ)	Izbrana strategija
3	IT-DAT-001	SQL baza	Podatkovni sistem	Hramba podatkov	5	5	5	5	Dinamične poizvedbe	SQL Injection / neustrezna validacija	5	3	15	Patch management, hardening	2	10	Zmanjšanje tveganja
4	IT-DAT-001	SQL baza	Podatkovni sistem	Hramba podatkov	5	5	5	5	Ni HA	Izpad baze / okvara infrastrukture	5	2	10	Backup, monitoring	1	5	Sprejem tveganja
5	IT-DAT-001	SQL baza	Podatkovni sistem	Hramba podatkov	5	5	5	5	Šibek RBAC; manjkajoča MFA	Neavtoriziran dostop do baze	5	3	15	Osnovni RBAC (Role-Based Access Control), ločeni	2	10	Sprejem tveganja – izjema
6	IT-DAT-006	Telefonski	Podatkovni sistem	Kontakti	1	1	2	1	Ni SLA	Izpad storitve	2	2	4	Osnovni nadzor	1	2	Sprejem tveganja
7	SEC-002	EDR	Varnostni sistem	Zaščita endpointov	4	4	5	4	Agent out-of-date	Nepravočasne posodobitve	5	3	15	Centralno upravljanje	2	10	Zmanjšanje tveganja
8	IT-APP-008	E-arhiv	Aplikacija	Hramba dokumentov	4	5	3	4	Šibek nadzor vlog	Neavtoriziran dostop	5	3	15	RBAC, logging	2	10	Zmanjšanje tveganja
9	IT-APP-008	E-arhiv	Aplikacija	Hramba dokumentov	4	5	3	4	Neustrezen backup	Izguba podatkov	5	2	10	Backup	1	5	Sprejem tveganja
10	IT-APP-003	HRM	Aplikacija	Kadri	5	5	4	5	Premalo stroge vloge	Neavtoriziran dostop	5	3	15	RBAC, logging	2	10	Zmanjšanje tveganja
11	IT-INF-011	Mobilne naprave	Infrastruktura	Mobilni dostop	3	3	4	4	Neenotna MDM politika	Kompromitacija mobilne naprave	4	3	12	MDM, šifriranje, PIN/biometrija	2	8	Sprejem tveganja
12	IT-INF-011	Mobilne naprave	Infrastruktura	Mobilni dostop	3	3	4	4	Brez centralnega nadzora geolokacije	Izguba/kraja mobilne naprave	4	3	12	MDM remote wipe, šifriranje	2	8	Sprejem tveganja
13	IT-INF-006	WiFi omrežje	Infrastruktura	Povezljivost	3	3	4	3	Brez WIPS (Wireless Intrusion Prevention	DoS motnje na WiFi	4	2	8	RF (Radio Frequency) monitoring	1	4	Sprejem tveganja
14	IT-INF-013	Testni strežnik	Infrastruktura	Testno okolje	2	2	2	2	Neredno patchanje	Zakasneli patchi v testnem okolju	2	3	6	Osnovni patching cikli se izvajajo	2	4	Sprejem tveganja
15	OT-011	HVAC	OT sistem	Klimatizacija strežnikov	3	3	5	3	Enojna klima; brez N+1	Izpad HVAC → pregrevanje strežnikov	5	3	15	Osnovni alarmi BMS (building management system)	2	10	Zmanjšanje tveganja
16	OT-011	HVAC	OT sistem	Klimatizacija strežnikov	3	3	5	3	Privzeta gesla	Neavtoriziran oddaljen dostop do HVAC	5	2	10	VPN; omejeni IP dostopi	1	5	Sprejem tveganja
17	OT-009	EMS	OT sistem	Energetski nadzor	4	4	4	4	Nepodpisani podatkovni tokovi	Manipulacija odčitkov energije	4	3	12	RBAC; osnovne validacije	2	8	Sprejem tveganja

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

HVALA ZA POZORNOST

Agamemnonos 14, Chalandri 15231
Attiki, Greece

osu-ms-support@enisa.europa.eu

www.enisa.europa.eu