EUROPEAN UNION AGENCY
FOR CYBERSECURITY

OPREDELITEV KLJUČNIH OBVEZNOSTI ZAVEZANCEV S POUDARKOM NA PRIPRAVI VARNOSTNE DOKUMENTACIJE

Božidar DAJČMAN, ICS-Ljubljana

28 | 01 | 2026

KAJ PRINAŠATA NIS2 IN ZINFV-1 ZA ZAVEZANCE?

Samoregistracija

Vsak zavezanec se mora samoprepoznati oziroma samoregistrirati preko mehanizma za samoregistracijo URSIV.

Priglasitev pomembnih incidentov

Subjekti javne uprave na državni in lokalni ravni ter ponudniki storitev zaupanja, ki jih izvajajo subjekti državne uprave.

→ SIGOV-CERT (v okviru URSIV)

Zavezanci, ki niso zajeti v pristojnosti SIGOV-CERT in prostovoljna priglasitev subjektov, ki niso zavezanci po ZInfV-1.

→ SI-CERT (v okviru ARNES)

Ukrepi za obvladovanje tveganj

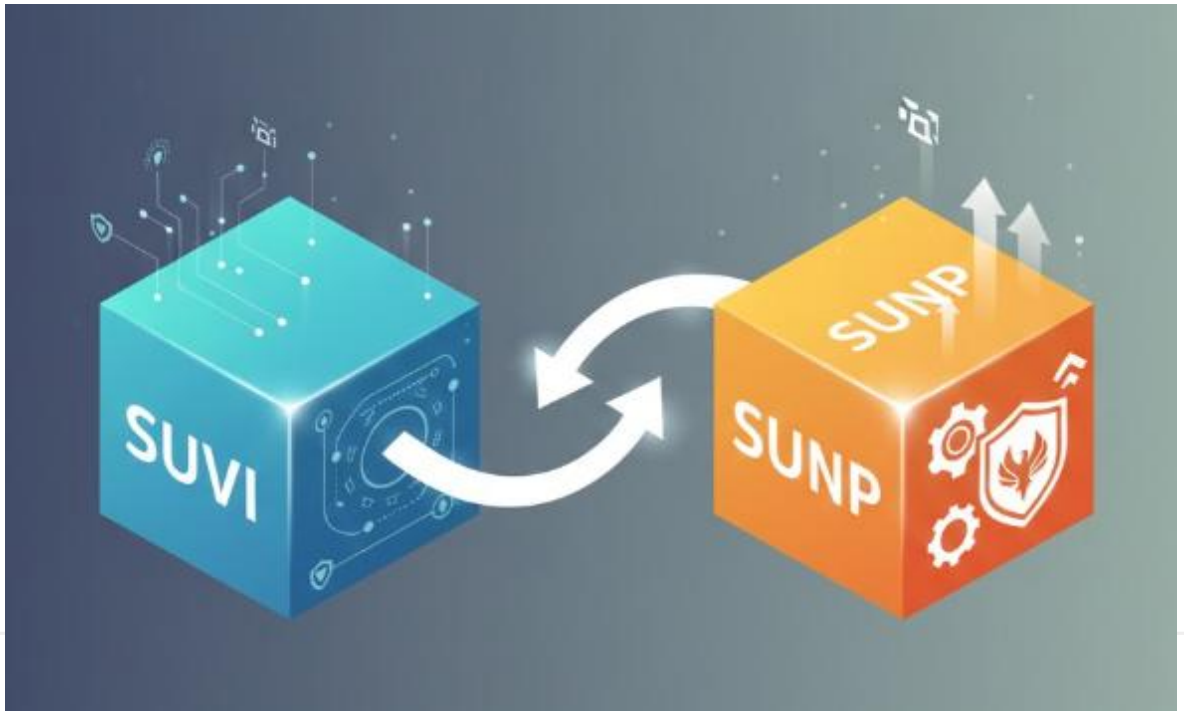
Zavezanci morajo sprejeti konkretne ukrepe za obvladovanje tveganj, ki grozijo njihovim informacijskim in omrežnim sistemom.

DOKUMENTACIJA

Bistveni in pomembni subjekti vzdržujejo dokumentirani sistem upravljanja varovanja informacij in sistem upravljanja neprekinjenega poslovanja

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

VARNOSTNA DOKUMENTACIJA – POLITIKA

Politika ali področne politike o varnosti omrežnih in informacijskih sistemov.

Krovna politika predstavlja osnovo varnostnega sistema organizacije in določa splošna načela ter odgovornosti. Na njej temeljijo področne varnostne politike, ki urejajo posamezna operativna področja varnosti.

/predstavljeno podrobneje v posebnem delu delavnice

VARNOSTNA DOKUMENTACIJA – POPIS SREDSTEV

Natančen in posodobljen popis informacijskih in drugih sredstev in podatkov, potrebnih za nemoteno delovanje omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev, ter njihove upravljavce.

Popis informacijskih sredstev je osnovni gradnik, na katerem temeljijo procesi obvladovanja tveganj, načrtovanja varnostnih ukrepov ter odzivanja na incidente.

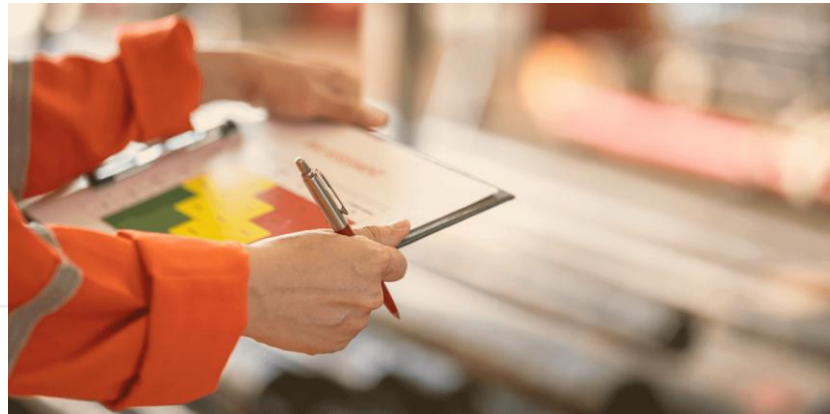
/predstavljeno podrobneje v posebnem delu delavnice

VARNOSTNA DOKUMENTACIJA – ANALIZA TVEGANJ

Analiza obvladovanja tveganj, vključno z določitvijo sprejemljive ravni tveganja in opisom uporabljene metodologije.

Analiza tveganj temelji na strukturiranem pristopu k ocenjevanju stopnje tveganja. Na podlagi rezultatov se določijo primerne strategije obravnave, prioritete ter ukrepi za obvladovanje tveganj.

/predstavljeno podrobneje v posebnem delu delavnice



VARNOSTNA DOKUMENTACIJA – NEPREKINJENO POSLOVANJE

Politika in načrt neprekinjenega poslovanja, vključno z:

- oceno vpliva na poslovanje,

- navedbo postopkov zagotavljanja neprekinjenega poslovanja,

- določitvijo minimalne ravni poslovanja,

- upravljanjem varnostnih kopij ter

- določitvijo vlog in odgovornosti.

Politika neprekinjenega poslovanja je osrednji dokument, ki določa zavezo organizacije, da bo tudi ob resnih motnjah, izrednih dogodkih ali krizah zagotavljala kontinuirano izvajanje svojih ključnih storitev.

Načrt neprekinjenega poslovanja je osrednji izvedbeni dokument politike.

VARNOSTNA DOKUMENTACIJA – NAČRT OBNOVITVE

Načrt obnovitve in ponovne vzpostavitve delovanja omrežnih in informacijskih sistemov, ki jih potrebujemo za svoje delovanje ali opravljanje storitev, vključno z opisom odgovornosti in postopkov za obnovitev delovanja teh sistemov po dogodku, ki povzroči prekinitev njihovega delovanja.

Operativni dokument, ki se uporablja v primeru večjih motenj ali prekinitve delovanja. Namenjen je predvsem krizni ekipi, ekipi za obnovo IT sistemov ter pogodbenim izvajalcem, ki sodelujejo pri obnovi in ponovni vzpostavitvi delovanja.

VARNOSTNA DOKUMENTACIJA – NAČRT ODZIVA NA INCIDENTE

Načrt odzivanja na incidente s protokolom obveščanja pristojne skupine CSIRT, vključno z opisom sistema za zaznavo in odziv na incidente ter opisom vlog in odgovornosti za odzivanje na incidente.

Dokument določa vloge, odgovornosti in postopke za pravočasno odkrivanje, analiziranje, omejevanje in dokumentiranje kibernetskih incidentov, odzivanje nanje ter obveščanje in poročanje o njih.

VARNOSTNA DOKUMENTACIJA – NAČRT VARNOSTNIH UKREPOV

Načrt varnostnih ukrepov za zagotavljanje celovitosti, avtentičnosti, zaupnosti in razpoložljivosti omrežnih in informacijskih sistemov oziroma za obvladovanje tveganj za informacijsko in kibernetsko varnost, pri čemer ta načrt upošteva tveganja in področne posebnosti bistvenega ali pomembnega subjekta.

1 Podpora vodstva in vključitev v poslovni načrt

2 Zagotavljanje integritete kadrov

3 Osnovne prakse kibernetske higiene in usposabljanje

4 Upravljanje dostopa in varnost človeških virov

5 Upravljanje varnostnih kopij

6 Dnevniški zapisi in revizijske sledi

7 Upravljanje omrežnih in informacijskih sistemov ter odgovornosti

8 Kriptografija in zaščita podatkov

9 Upravljanje prometa in omrežne komunikacije

10 Varnost dobavne verige

11 Fizična in okoljska varnost

12 Aplikacijska varnost in razvoj

13 Upravljanje in preprečevanje ranljivosti

14 Zaščita pred zlonamerno programsko kodo ter način zaznavanja poskusov vdorov

15 Avtentikacija in nadzor dostopov

16 Uporaba varnih komunikacij in sistemov komunikacije v sili

17 Oblačne storitve

VARNOSTNA DOKUMENTACIJA – PRESOJA UČINKOVITOSTI VARNOSTNIH UKREPOV

Politika s postopki za presojo učinkovitosti varnostnih ukrepov za obvladovanje tveganj za informacijsko in kibernetsko varnost, vključno z določitvijo kazalnikov učinkovitosti in izvedeno analizo zbranih podatkov.

Dokument predstavlja obvezno politiko in postopke za sistematično in dokazljivo preverjanje, ali varnostni ukrepi (tehnični, logično-tehnični in organizacijski) dejansko delujejo ter ali ustrezno obvladujejo tveganja za informacijsko in kibernetsko varnost.

VARNOSTNA DOKUMENTACIJA – SPLOŠNO

(21.2) Bistveni in pomembni subjekti določijo obseg sistema upravljanja in varovanja informacij ter neprekinjenega poslovanja ob upoštevanju rezultatov analize vpliva na poslovanje, pri čemer mora ta sistem obsegati najmanj tista informacijska, komunikacijska in druga **sredstva, podatke in procese, ki so potrebni za njihovo delovanje ali opravljanje storitev.**

(21.3) Če ima bistveni ali pomembni subjekt za zagotavljanje varnosti svojih omrežij in informacijskih sistemov že izdelano varnostno dokumentacijo **na podlagi drugih predpisov**, jo za potrebe izvajanja tega zakona **dopolni**, kot je to potrebno

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

HVALA ZA POZORNOST

Agamemnonos 14, Chalandri 15231
Attiki, Greece

osu-ms-support@enisa.europa.eu

www.enisa.europa.eu