
SMART
COM
UDEJANJAMO VAŠE VIZIJE

Nova pravila, višja raven informacijske varnosti

Kako pristopiti k izpolnjevanju zahtev direktive NIS 2?

Igor Mlakar, direktor operative

CIS-A, CIS-M

Vsebina

- Spremembe, ki jih prinaša direktiva NIS 2
- Področja uporabe
- Prilagoditev procesov
- Naslednji korak

Spremembe, ki jih prinaša direktiva NIS 2

Odziv EU na neposredne grožnje Januar 2023

Priporočilo Sveta EU, da se zaradi obravnavanja groženj, ki izhajajo iz ruske vojne agresije proti Ukrajini:

- pospeši sprejemanje in izvajanje ukrepov EU za povečanje odpornosti kritične infrastrukture,
- zagotovi usklajevanje na ravni EU za učinkovito pripravljenost in odzivanje,
- države članice pozove, da pospešijo prenos CER in NIS 2 v nacionalne predpise in omogočijo čimprejšnje izvajanje novih ukrepov za zagotavljanje odpornosti kritičnih subjektov in kibernetske varnosti.

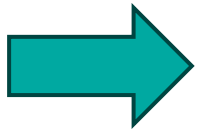
Cilji NIS 2

- Odprava velikih razlik med državami članicami glede ravni kibernetske odpornosti.
- Razširitev ukrepov na večji del gospodarstva – pokrivanje bistvenih sektorjev in storitev.
- Poenotiti merila za vključevanje subjektov – zavezancev.
- Podpiranje in ohranjanje zanesljivega, odpornega in varnega sistema domenskih imen (DNS).
- Upoštevanje varnosti pri uvajanju naprednih tehnologij.
- Zagotavljanje varnosti v celotni oskrbni verigi.
- Ozaveščanje o kibernetski varnosti.

Od NIS do NIS 2

NIS

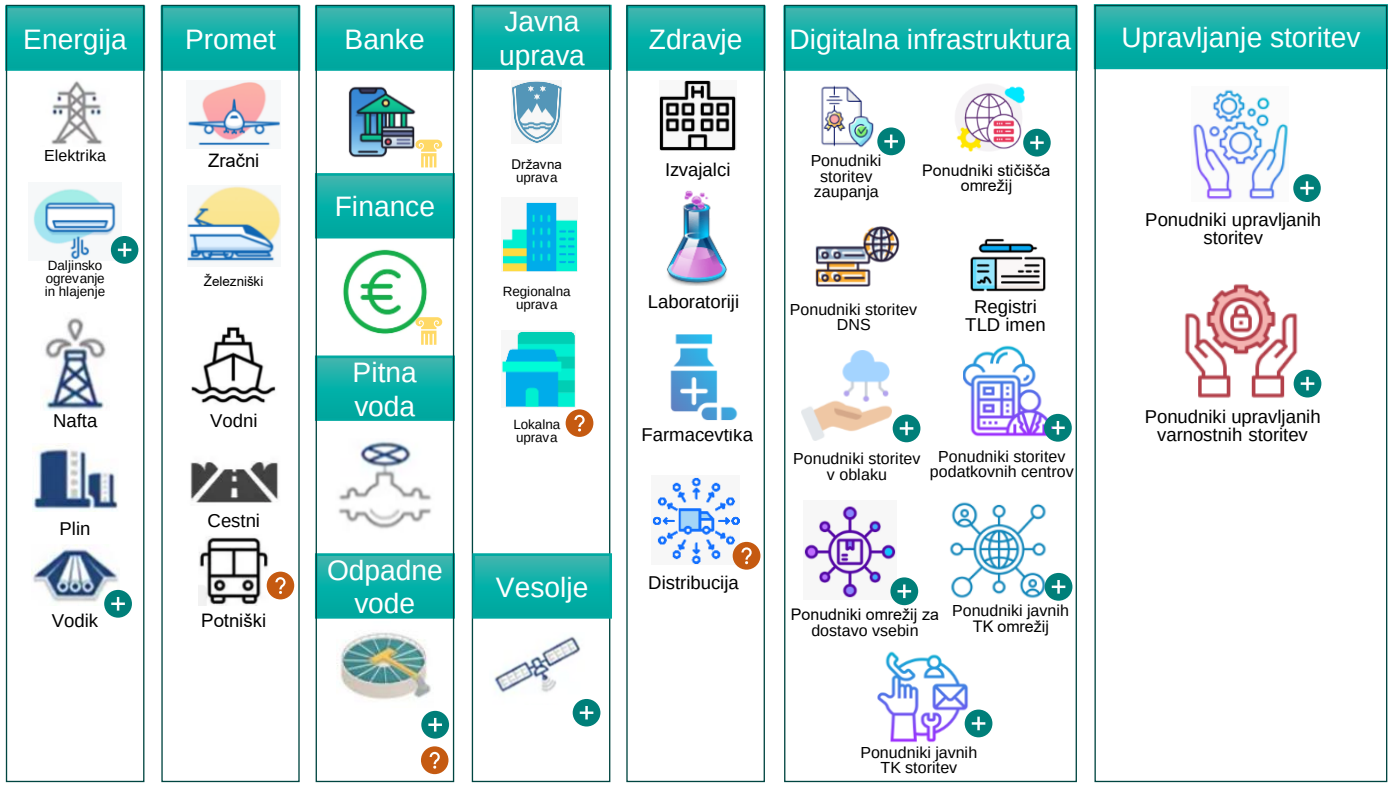
- Kritična infrastruktura, pomembni ponudniki digitalnih storitev
- Po izbranih sektorjih
- 7 sektorjev
- 30 tipov entitet
- Le "risk-based" brez potrebe po dokazovanju skladnosti
- Sankcije po presoji države članice



NIS 2

- Bistveni in pomembni subjekti
- Po sektorjih in velikosti subjektov
- 18 sektorjev
- 67 tipov entitet
- Obvezno obvladovanje tveganj
- Nadzor preko poročil in s pregledi v organizaciji
- Varnostni pregledi in presoje
- Varovanje oskrbne verige
- Osebna odgovornost poslovodstva
- Jasna politika kaznovanja, stroge kazni
- Formalizirano poročanje o incidentih

Visoko kritični sektorji (Priloga 1)



Novo v NIS 2

Dodatni pogoji

DORA Lex Specialis

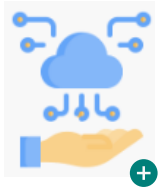
Ostali kritični sektorji (Priloga 2)

Poštne in kurirske storitve

Ravnanje z odpadki

Pridelava, predelava in distribucija živil

Digitalni ponudniki



Izdelava, proizvodnja in distribucija kemikalij

Raziskave

Raziskovalne institucije

Izobraževalne institucije

Proizvodnja

Proizvodnja medicinskih pripomočkov ter in vitro diagnostičnih medicinskih pripomočkov

Proizvodnja električnih naprav

Proizvodnja motornih vozil, prikolic in polprikolic

Proizvodnja računalnikov, elektronskih in optičnih izdelkov

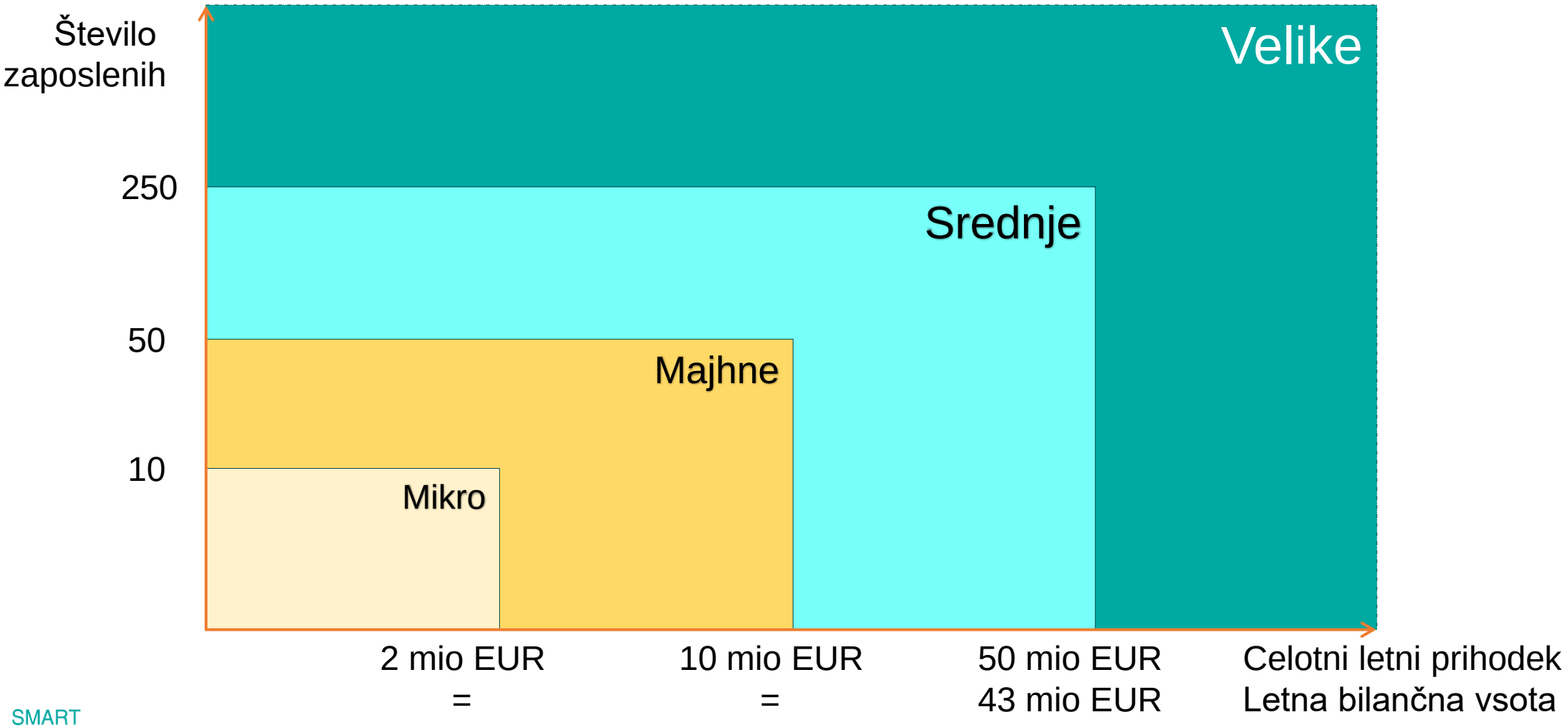
Proizvodnja drugih strojev in naprav

Proizvodnja drugih vozil in plovil

+ Novo v NIS 2

? Dodatni pogoji

Pravilo velikosti organizacij



Vir: Evropska komisija, Smernice za opredelitev MSP 2020

Obseg

- NIS (Direktiva (EU) 2016/1148 z dne 6. 7. 2016) - ZinfV

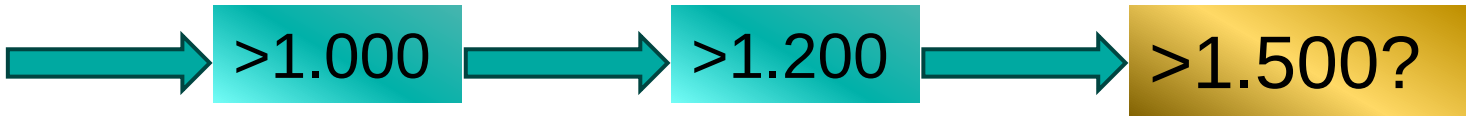
  68 zavezancev

  - 49 – izvajalci bistvenih storitev
  - 18 – organi državne uprave
  - 1 – ponudnik digitalnih storitev

- NIS 2 - ZinfV-1 (ocena)

  923 zavezancev

  - 219 – velika podjetja
  - 704 – srednje velika podjetja



Vir: URSIV, 10.10.2023

Kaj še prinaša direktiva

- Poenostavitev določitve subjektov
- Sodelovanje med pristojnimi organi
- Poročanje o incidentih
- Nadzor nad ključnimi oskrbnimi verigami
- Odgovornost poslovodstva
- Sodna pristojnost
- Strožje kazni

Področja uporabe

Grožnje (obdobje od 2022-07 do 2023-06)

TRENDI

Na vrhu so izsiljevalski napadi in napadi na razpoložljivost

Phishing predstavlja najbolj pogost vektor napada

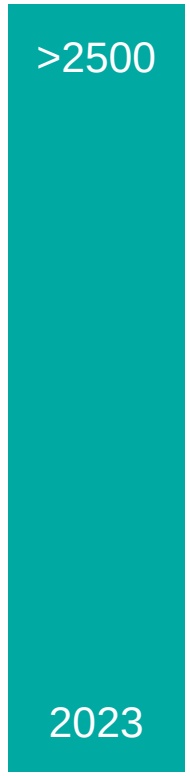
Ogroženost podatkov še vedno narašča

Vpliv geopolitike narašča (prirejanje informacij …)

'Cheap Fakes' in manipulacija informacij, ki jo omogoča UI

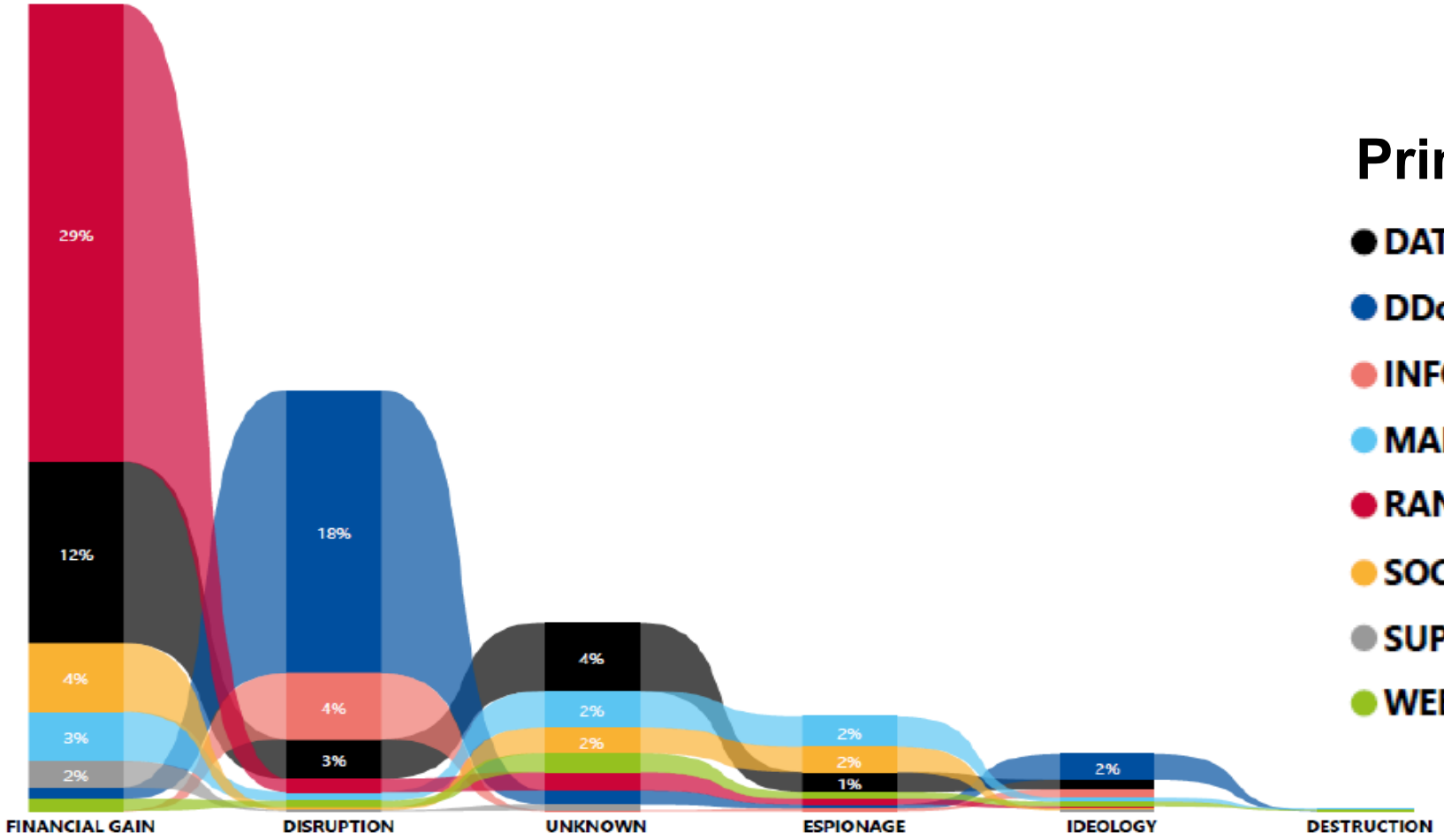
Povečana grožnja napadov na dobavno verigo – zaposleni kot vstopna točka

…



Vir: ENISA Threat Landscape 2023, oktober 2023

Motivi napadalcev



Primarna grožnja:

- DATA
- DDoS
- INFORMATION MANIPULATION
- MALWARE
- RANSOMWARE
- SOCIAL ENGINEERING
- SUPPLY CHAIN ATTACK
- WEB THREATS

Vir: ENISA Threat Landscape 2023, oktober 2023

Področja uporabe

1. VKLJUČENOST POSLOVODSTVA
2. VARNOSTNA POLITIKA ORGANIZACIJE
3. OZAVEŠČANJE OSEBJA O VARNOSTNIH GROŽNJAH
4. UPRAVLJANJE KLJUČNIH VIROV IKT

5. POSODABLJANJE PROGRAMSKE OPREME
6. UPRAVLJANJE DOSTOPA DO DELOVNIH POSTAJ IN OMREŽJA
7. ZAŠČITA DELOVNIH POSTAJ IN PRENOSNIH NAPRAV

8. ARHIVIRANJE PODATKOV
9. ZAŠČITA STREŽNIKOV IN OMREŽNIH KOMPONENT
10. VAREN ODDALJENI DOSTOP

11. ZAŠČITA PRED ZLONAMERNO PROGRAMSKO KODO
12. ZAŠČITA PRED DRUGIMI GROŽNJAMI
13. NEPREKINJENOST POSLOVANJA IN UPRAVLJANJE INCIDENTOV

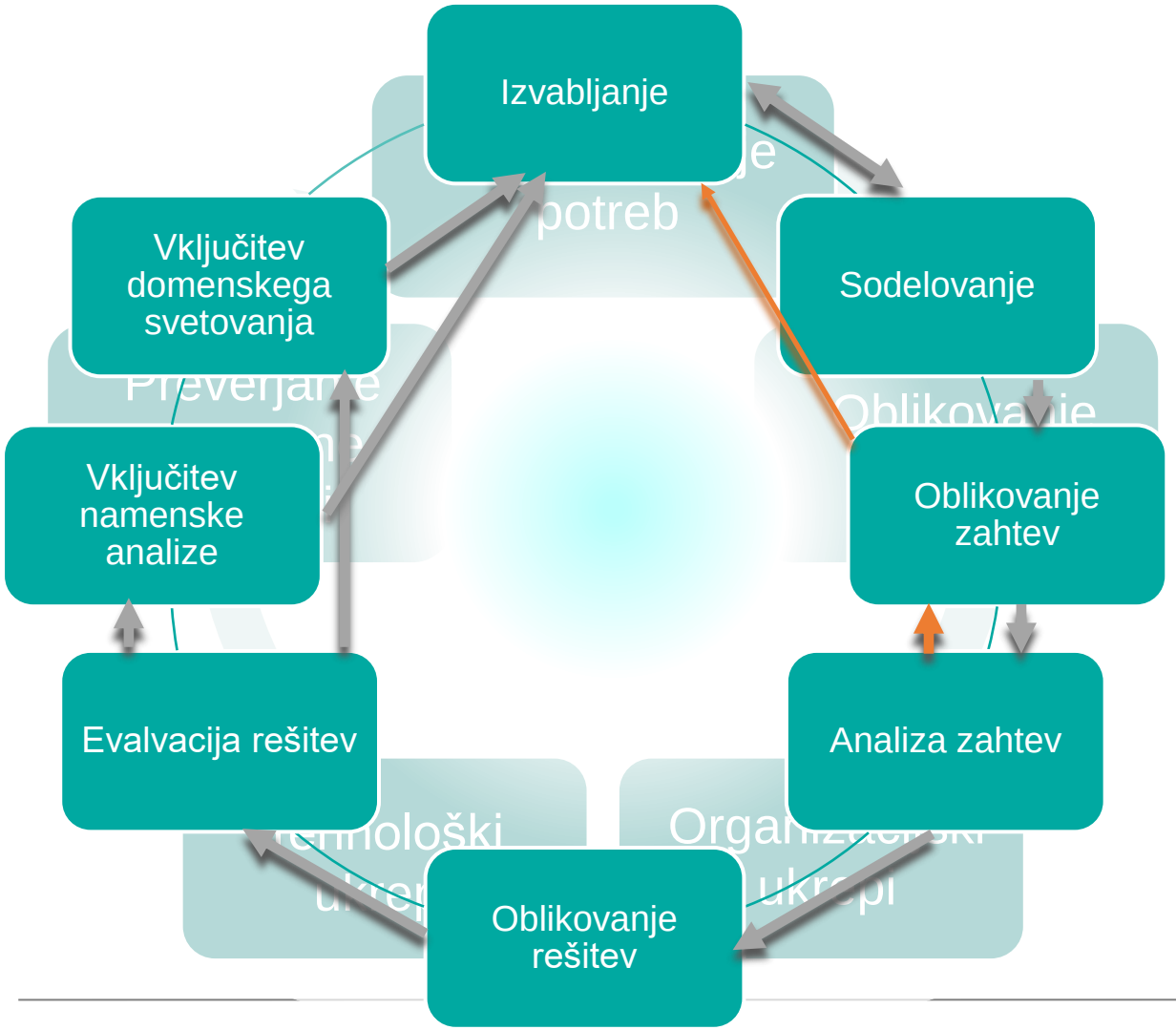
Priporočila

- Skozi oceno pripravljenosti po področjih uporabe preverite stopnjo zrelosti vašega poslovanja z vidika kibernetske varnosti.
- Na osnovi tehtnega premisleka se lahko odgovorno odločite za uvedbo ukrepov tam, kjer ugotovite, da vam preti največja grožnja oziroma na področju, kjer bo učinek spremembe največji.
- Razmislek lahko opravite sami, lahko pa poiščete pomoč pri zunanjih strokovnjakih za posamezno tehnološko področje oziroma za presojo in oblikovanje procesov.

Prilagoditev procesov

Koraki za oceno zrelosti

Koraki za oceno zrelosti



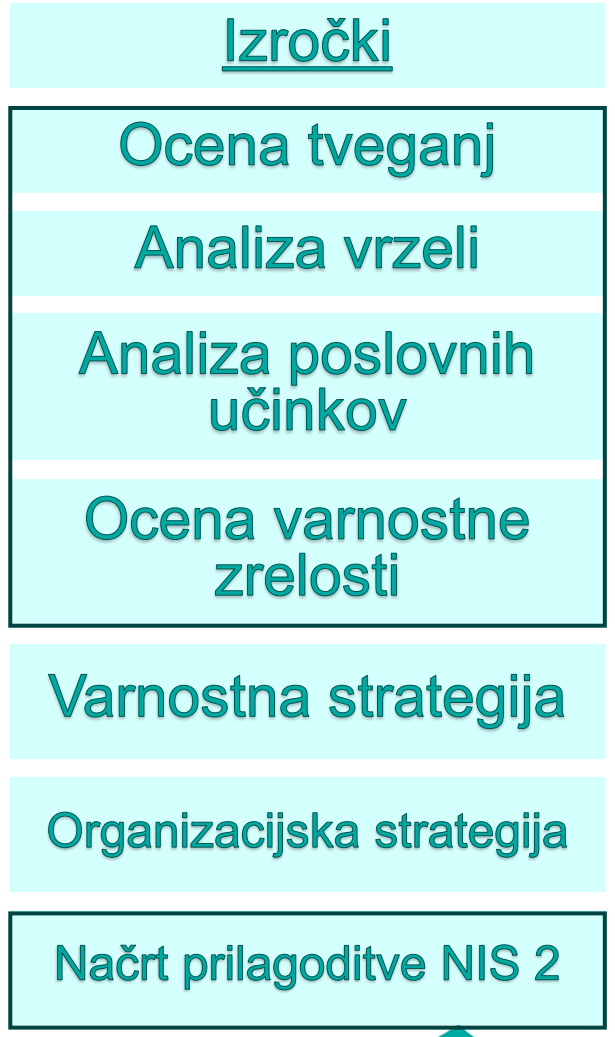
Strateška raven
- Preverjanje varnostne zrelosti
- Odločitev o načinu zagotavljanja skladnosti
- Varnostna strategija organizacije
- Organizacijska strategija - Procesi

Taktična raven
- Vpeljava organizacijskih sprememb
- Vpeljava procesnih sprememb
- Vpeljava tehnoloških sprememb
- Preverjanje in poročanje o spremembah

Operativna raven
- Izvajanje rednih aktivnosti
- Poročanje

Storitev procesnega svetovanja za prilagoditev organizacije zahtevam direktive NIS 2

- Vrednotenje trenutnega stanja in ravni kibernetske varnosti
- Prepoznavanje potreb
- Pomoč pri pripravi strategij in postavitvi zahtev glede na poslovne cilje organizacije
- Svetovanje pri vzpostavitvi oz. preoblikovanju procesov
- Pomoč pri oblikovanju zahtev za spremembe v smeri skladnosti z NIS 2



Naslednji korak

Imate vprašanja...

Igor Mlakar
E: igor.mlakar@smart-com.si