REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO

IJU 2015

Vzpostavitev security operational centra DRO

mag. Damijan Marinšek

Ministrstvo za javno upravo
Direktorat za informatiko
Sektor za informacijsko varnost

15. 12. 2015

Kazalo

Trenutno stanje v državni upravi - Pretekle aktivnosti

V preteklosti smo izvajali operativne naloge informacijske varnosti:

- izvajanje varnostnih pregledov informacijskih sistemov državne uprave od zunaj (od leta 2007)
- izvajanje varnostnih pregledov informacijskih sistemov državne uprave od znotraj (od leta 2011)
- Odzivanje na incidente tudi s sporazumom s SI-CERT od leta 2010
- Anonymous 2012
- Obveščanje
- Preverjanje aplikacij in gradnikov pred produkcijo 2015

Vizija – želeno stanje do leta 2020

Ozaveščeni in strokovno usposobljeni zaposleni v državni upravi z uveljavljanjem potrjenih varnostnih politik v praksi in z ravnanjem v skladu z veljavno Uredbo o informacijski varnostni politiki začnejo zagotavljati predpisano stopnjo informacijske varnosti.

Sektor za informacijsko varnost
Naloge

Preventivno delovanje za večjo varnost informacijskih sistemov:

- verifikacija in implementacija varnostnih rešitev,
- sistematično odkrivanje in preprečevanje ranljivosti ter varnostnih groženj v informacijskih sistemih,
- varnostna analiza informacijskih sistemov (omrežja, operacijski sistemi, aplikacije, podatkovne zbirke),
- sistematično izvajanje preventivnih varnostnih preizkusov informacijskih sistemov,
- priprava ukrepov za odpravo varnostnih pomanjkljivosti in izboljšanje varnosti.

Obravnava varnostnih incidentov (SIGOV-CERT)**:**

- sprejem in zaznava incidentov,
- zamejitev škode,
- obravnavanje incidentov,
- predlaganje in izvajanje ukrepov,
- izdelava poročil.

Obveščanje, ozaveščanje in sodelovanje:

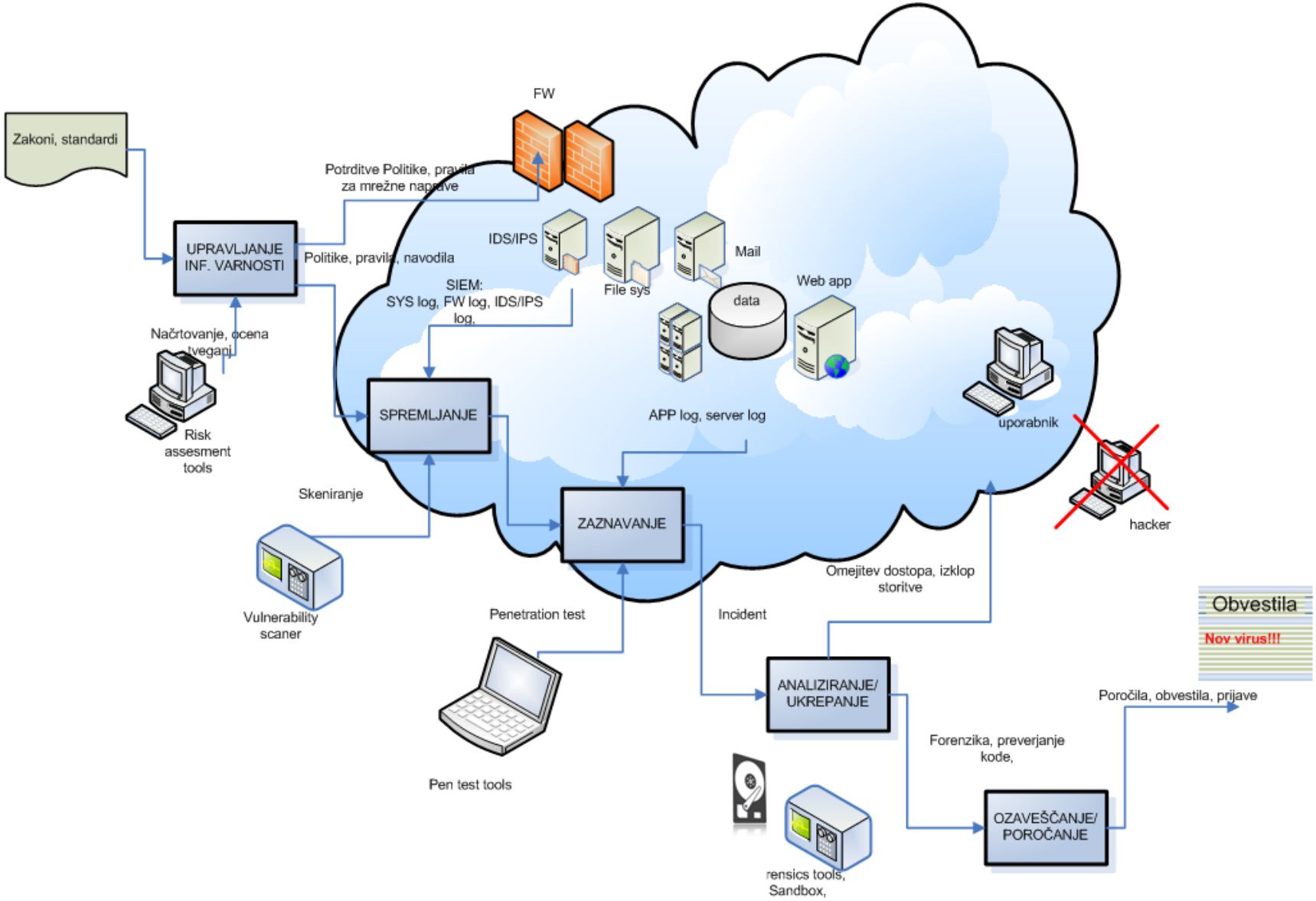
- obveščanje in ozaveščanje skrbnikov sistemov in uporabnikov,
- izvajanje izobraževanja na področju informacijske varnosti.

Projekt – DRO 6

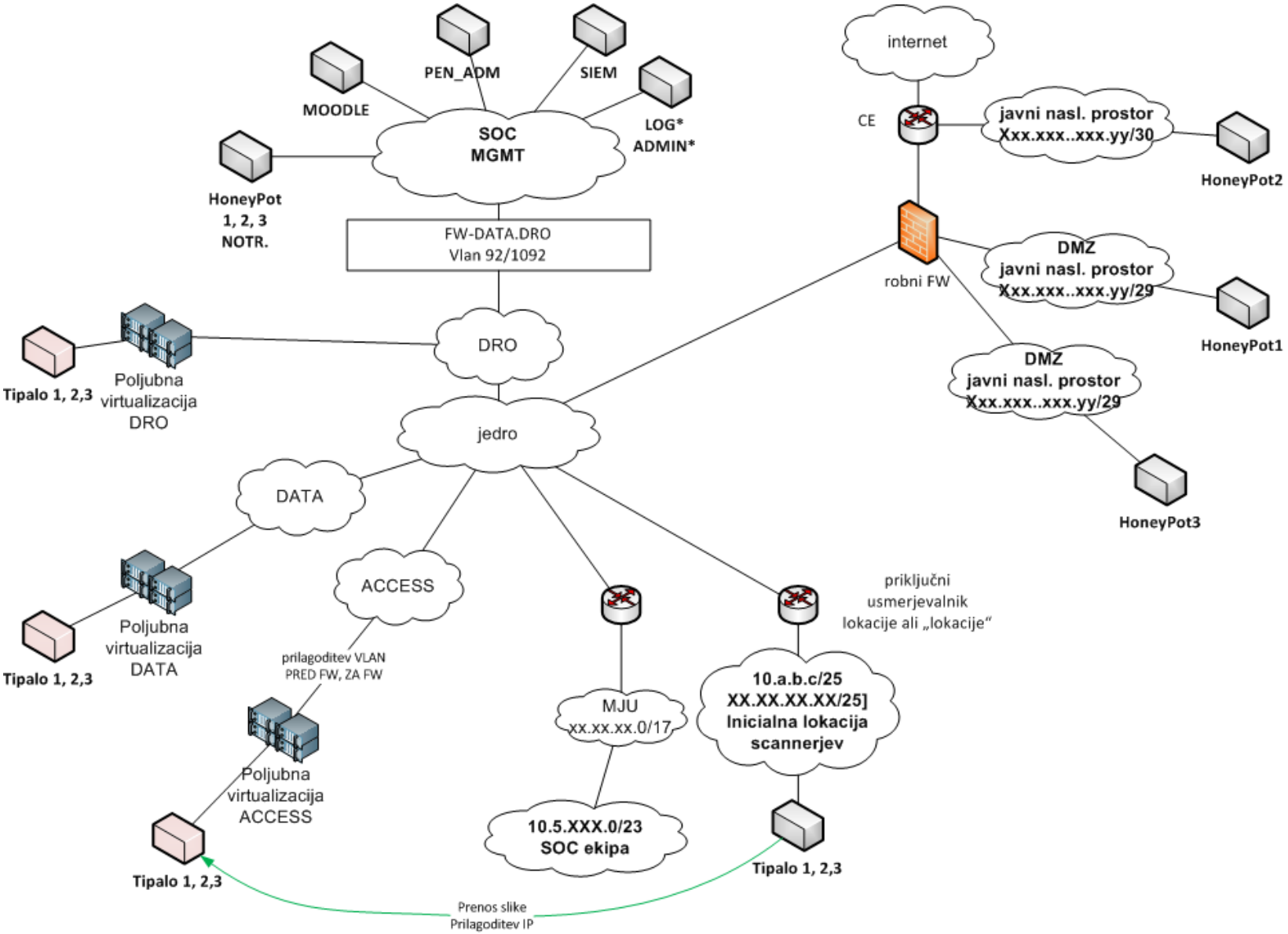
- **Nabava potrebne strojne in programske opreme** za izvajanje informacijske varnosti - Security Operational Center, naročilo DRO št.6 :
  - za zajem mrežnega prometa,
  - odkrivanje ranljivosti,
  - izvajanje penetracijskih testov,
  - preverjanje izvorne kode,
  - forenzično analizo,
  - platformo za incident management
  - platformo za ozaveščanje.
- **Izobraževanje in usposabljanje**:
  - tečaji in delavnice za informatike
  - obveščanje in opozarjanje uporabnikov

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO

Sektor za informacijsko varnost
Security Operational Center SOC

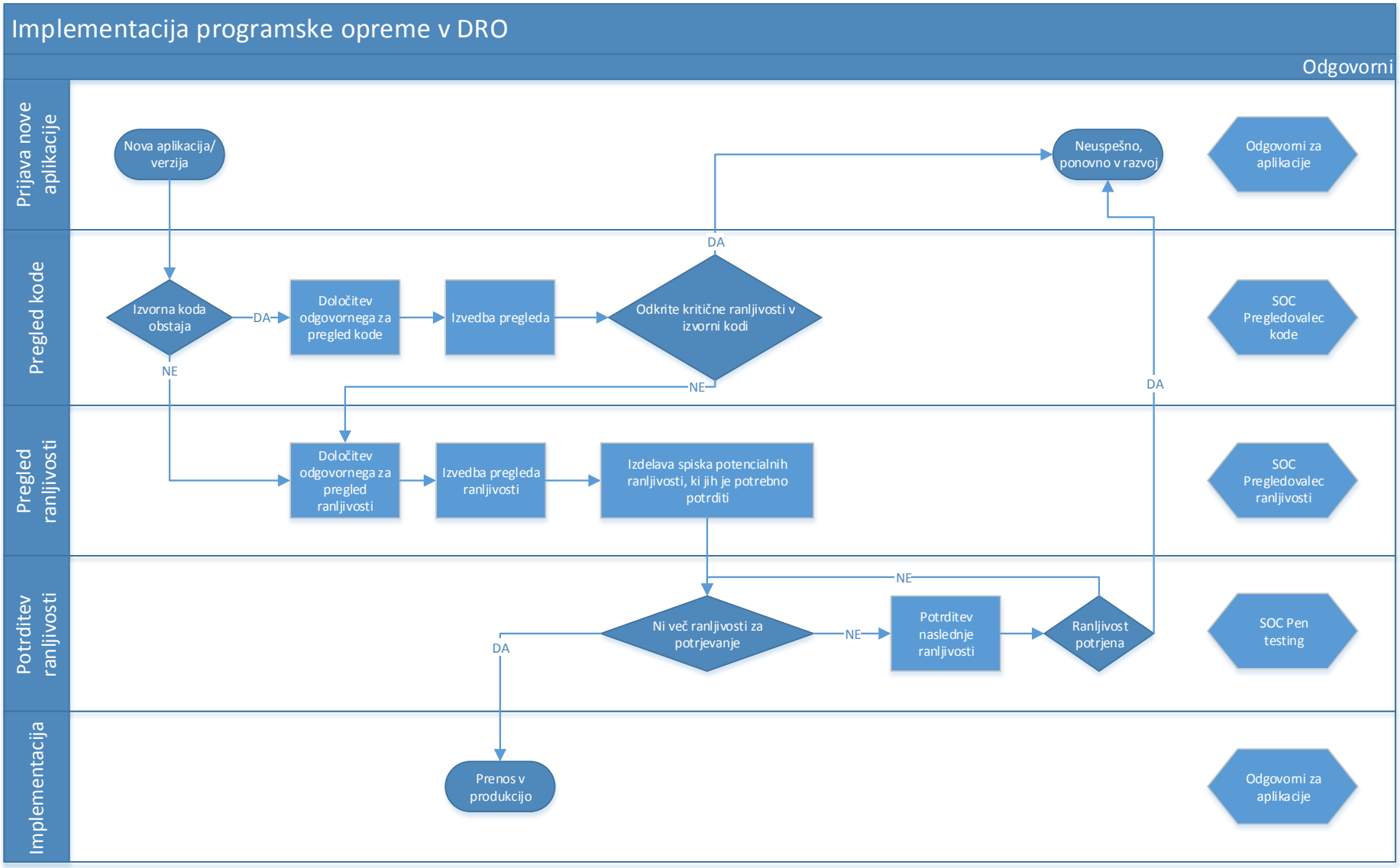


Sektor za informacijsko varnost
Network shema SOC



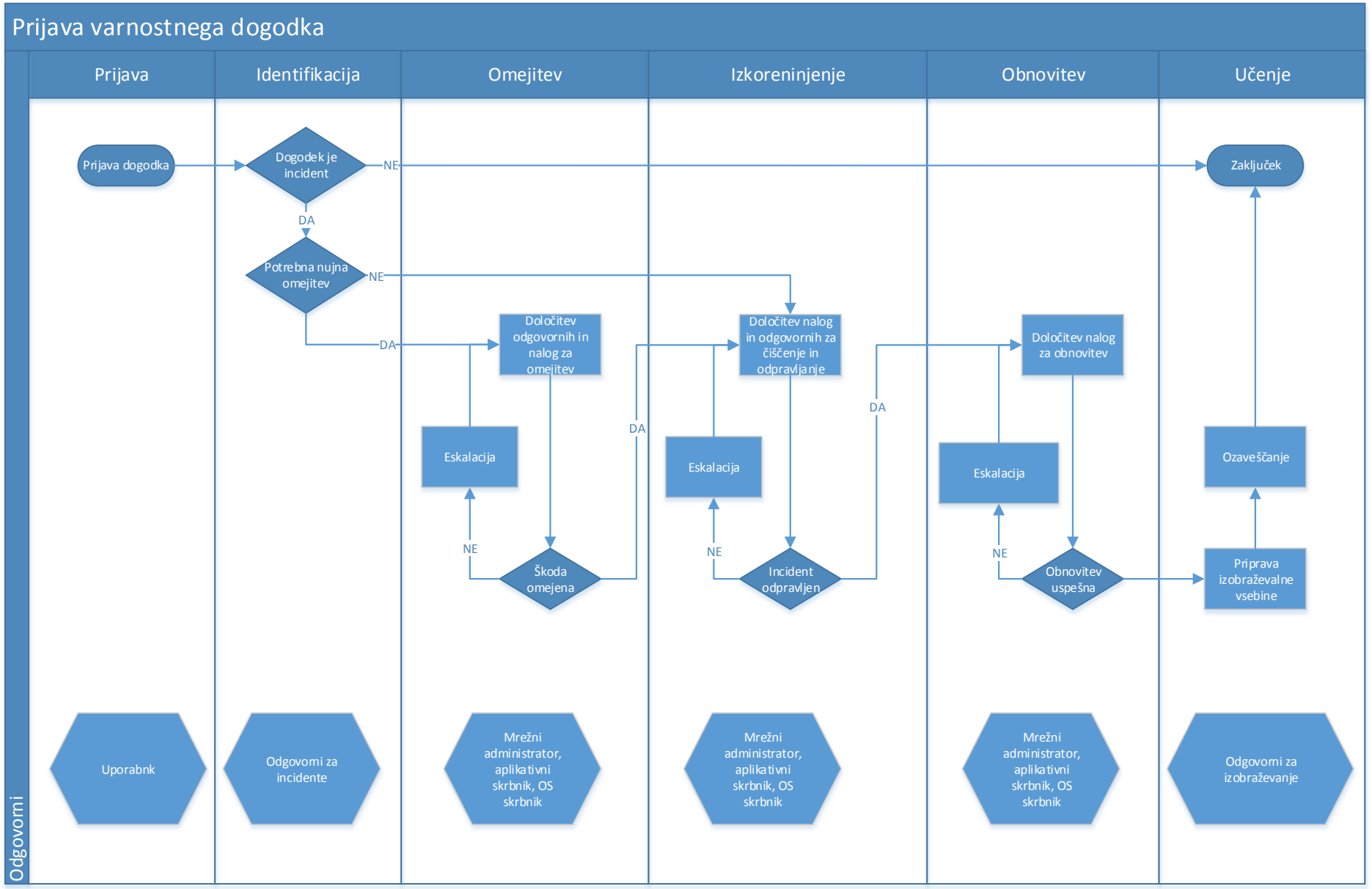
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO

Sektor za informacijsko varnost
Proces SOC (1)



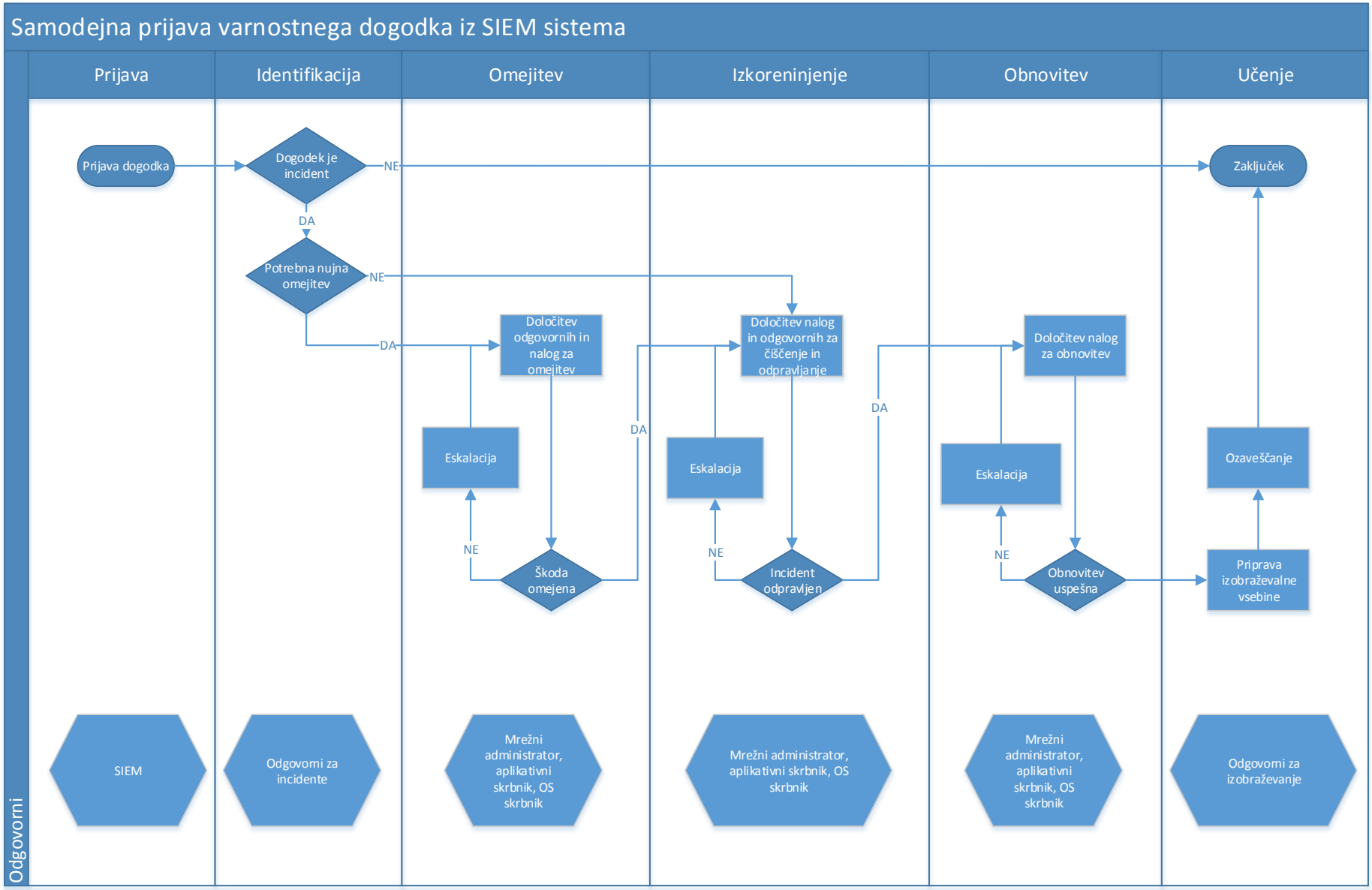
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO

Sektor za informacijsko varnost
Proces SOC (2)



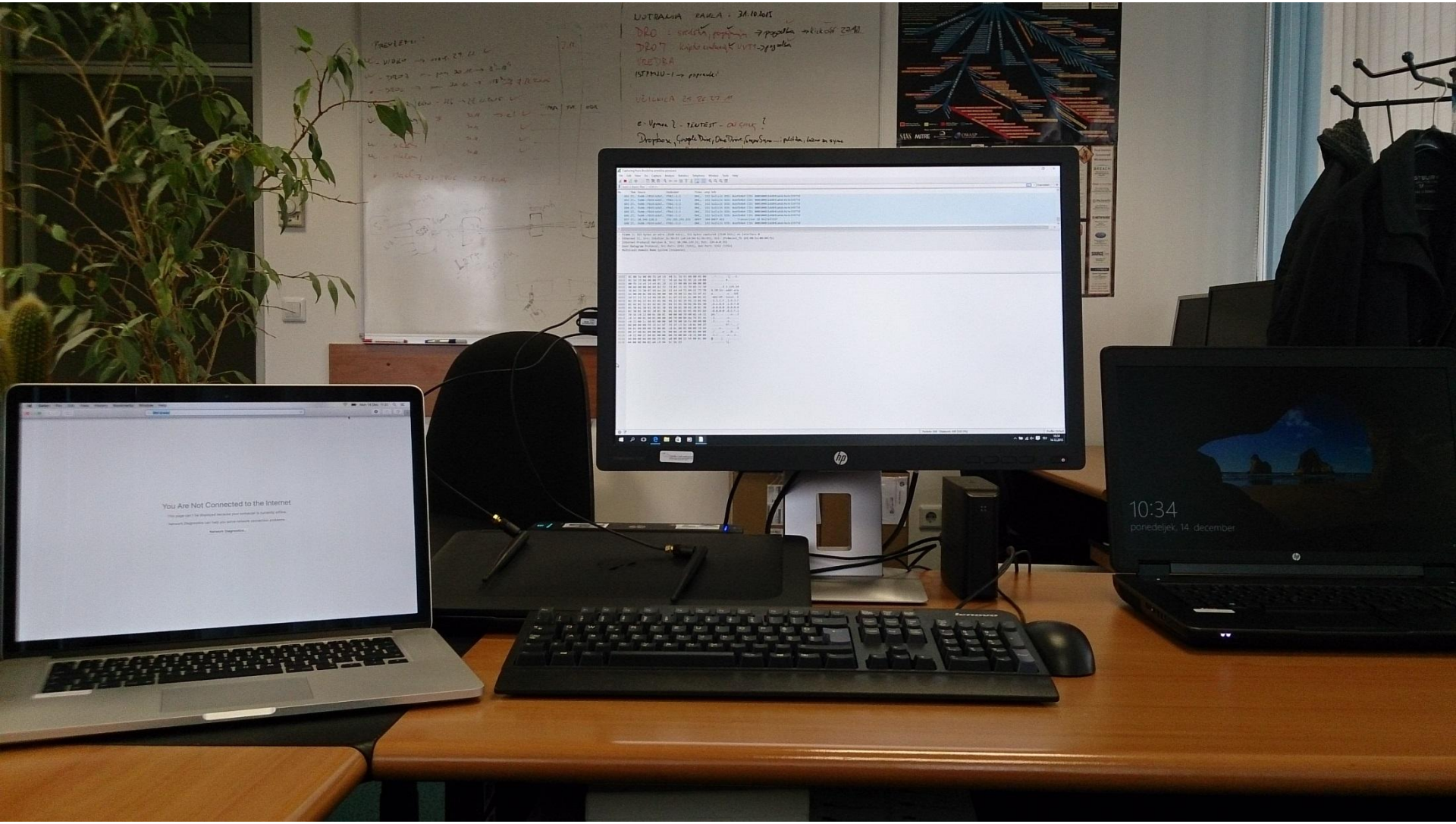
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO

Sektor za informacijsko varnost
Proces SOC (3)



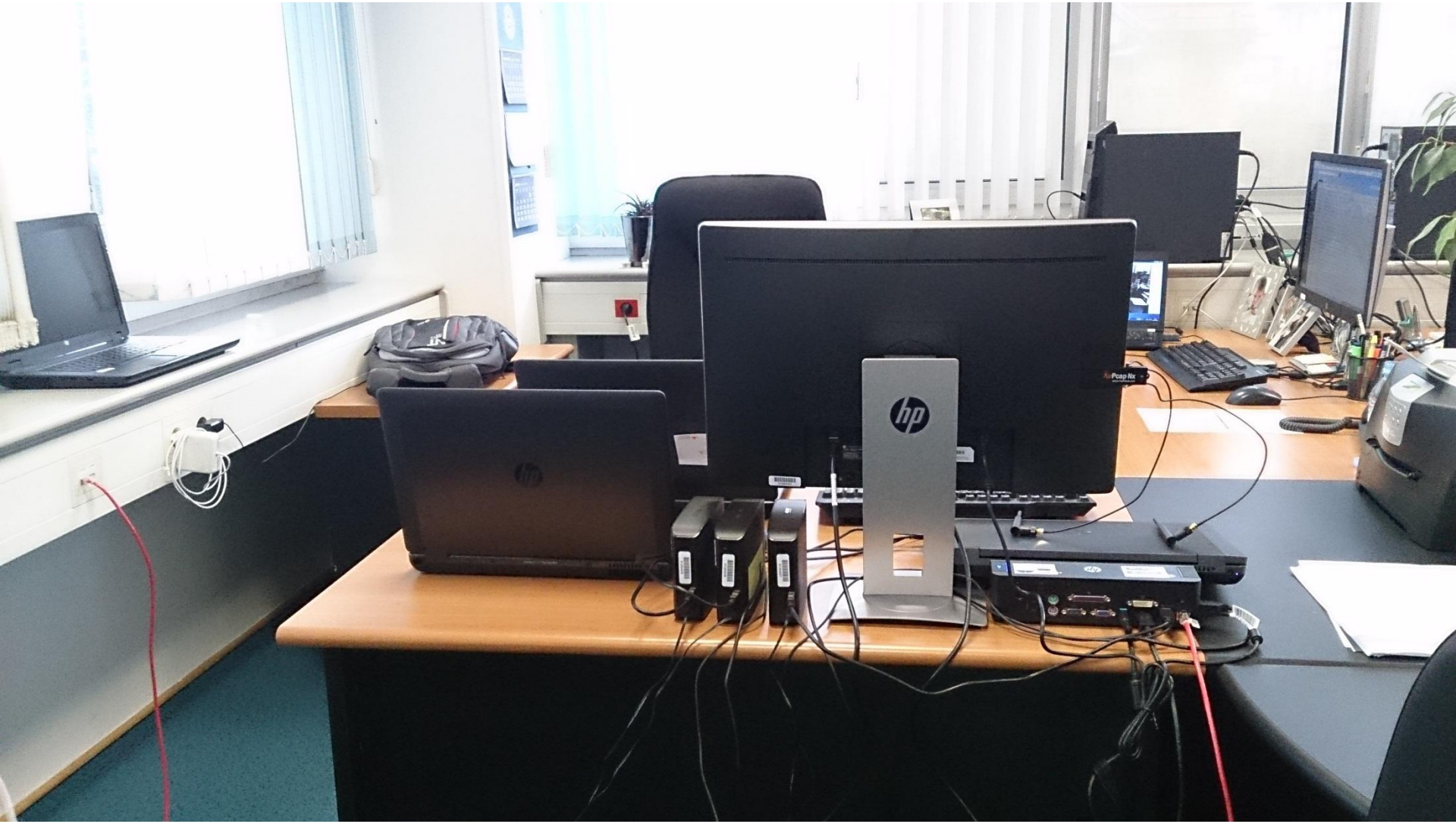
Oprema SOC

Oprema SOC


You Are Not Connected to the Internet
10:34
ponedeljek, 14. december

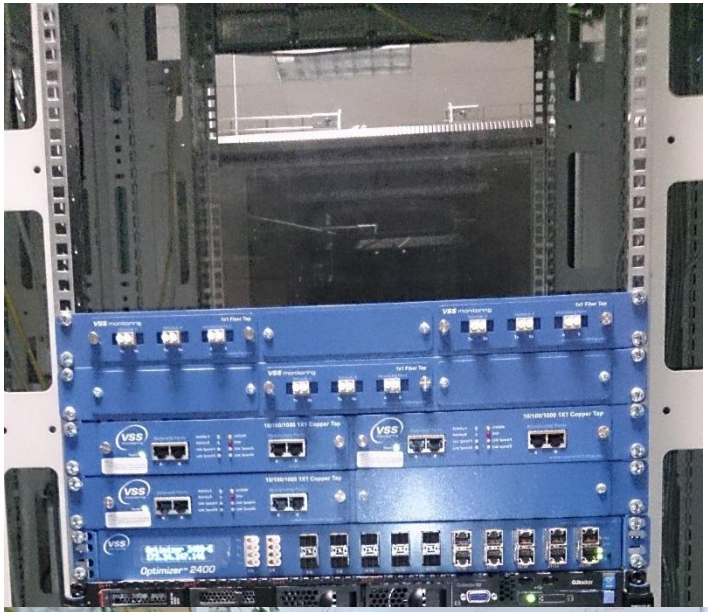
Oprema SOC

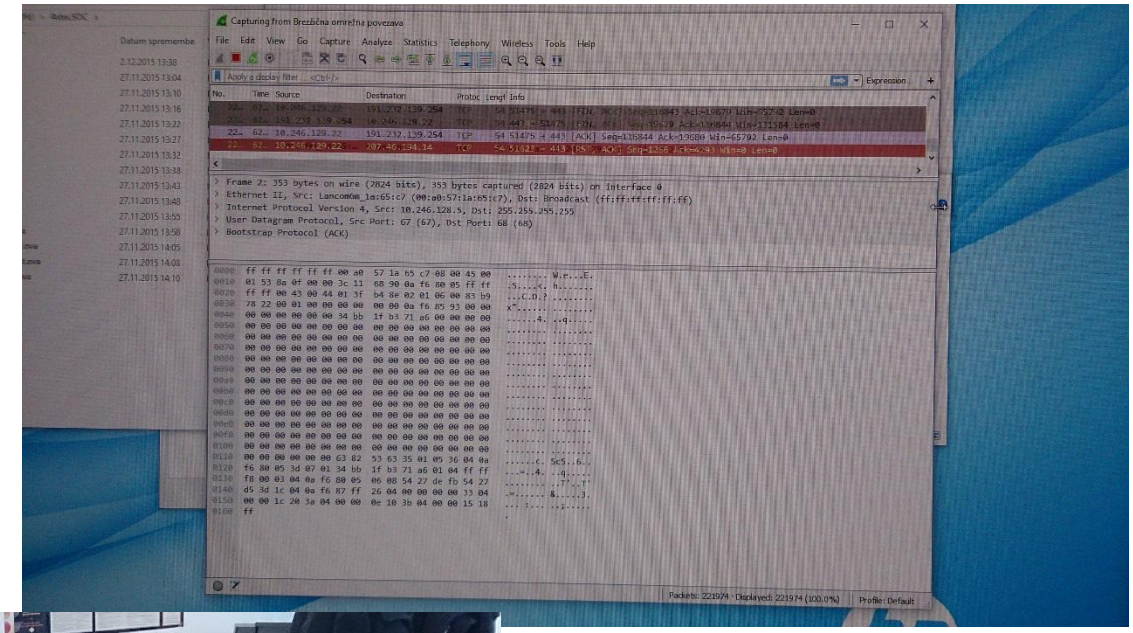
Oprema SOC



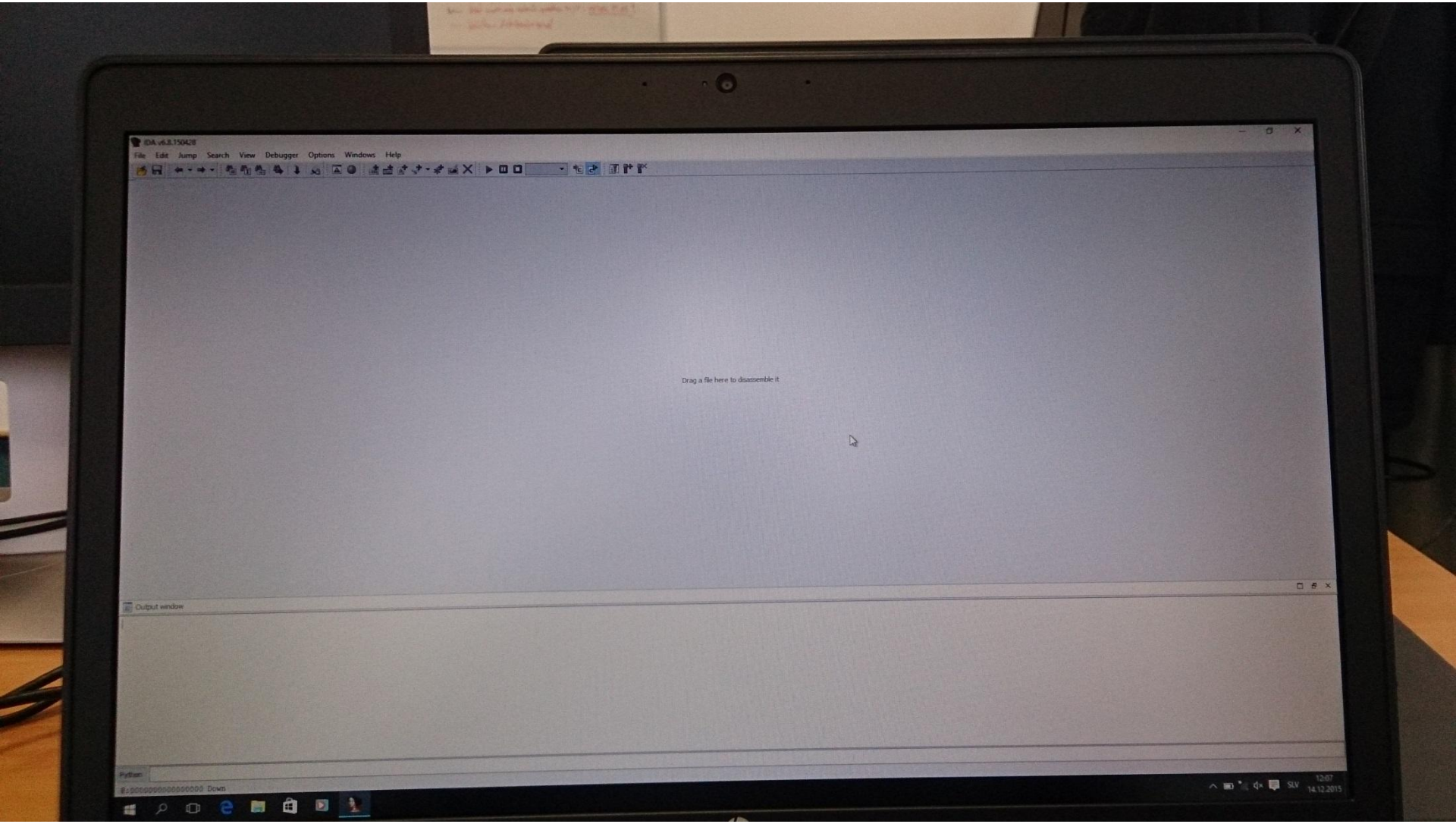
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO

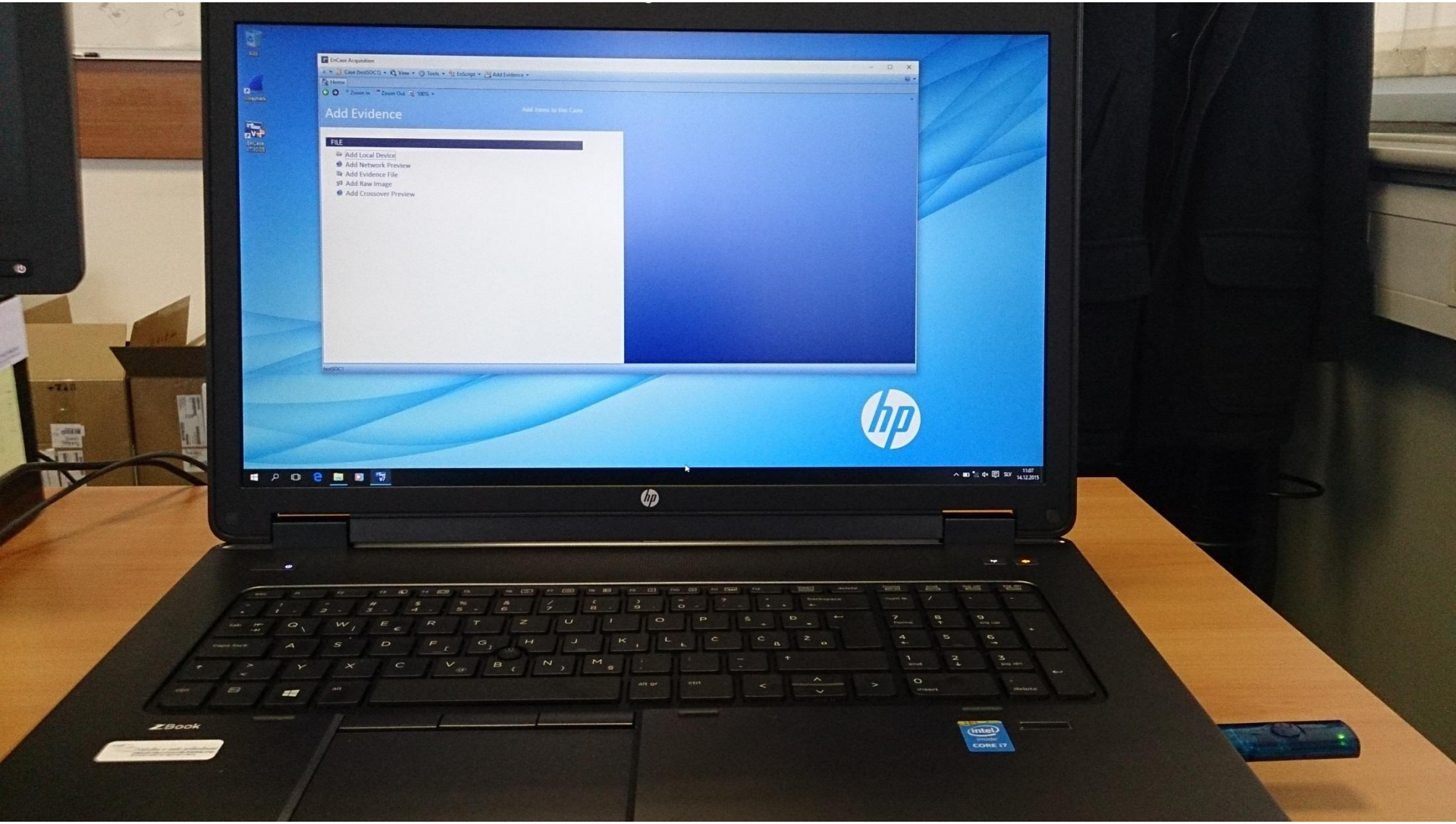
zajem mrežnega prometa



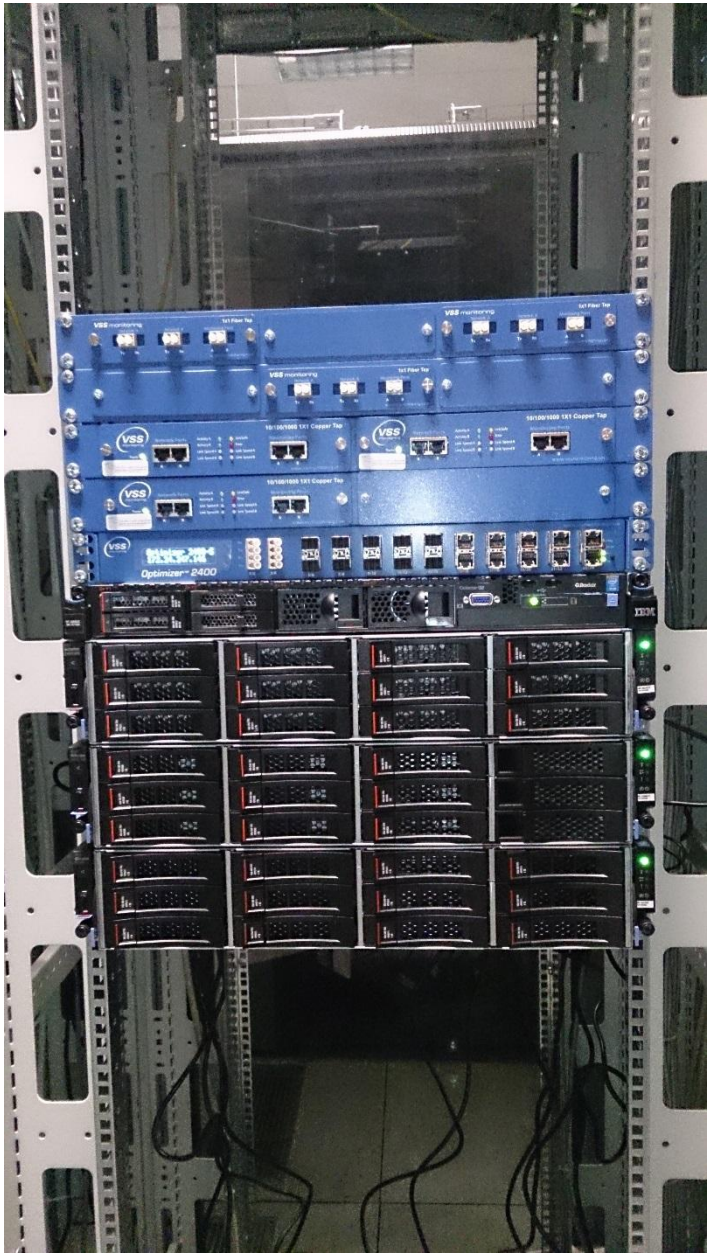


preverjanje izvorne kode

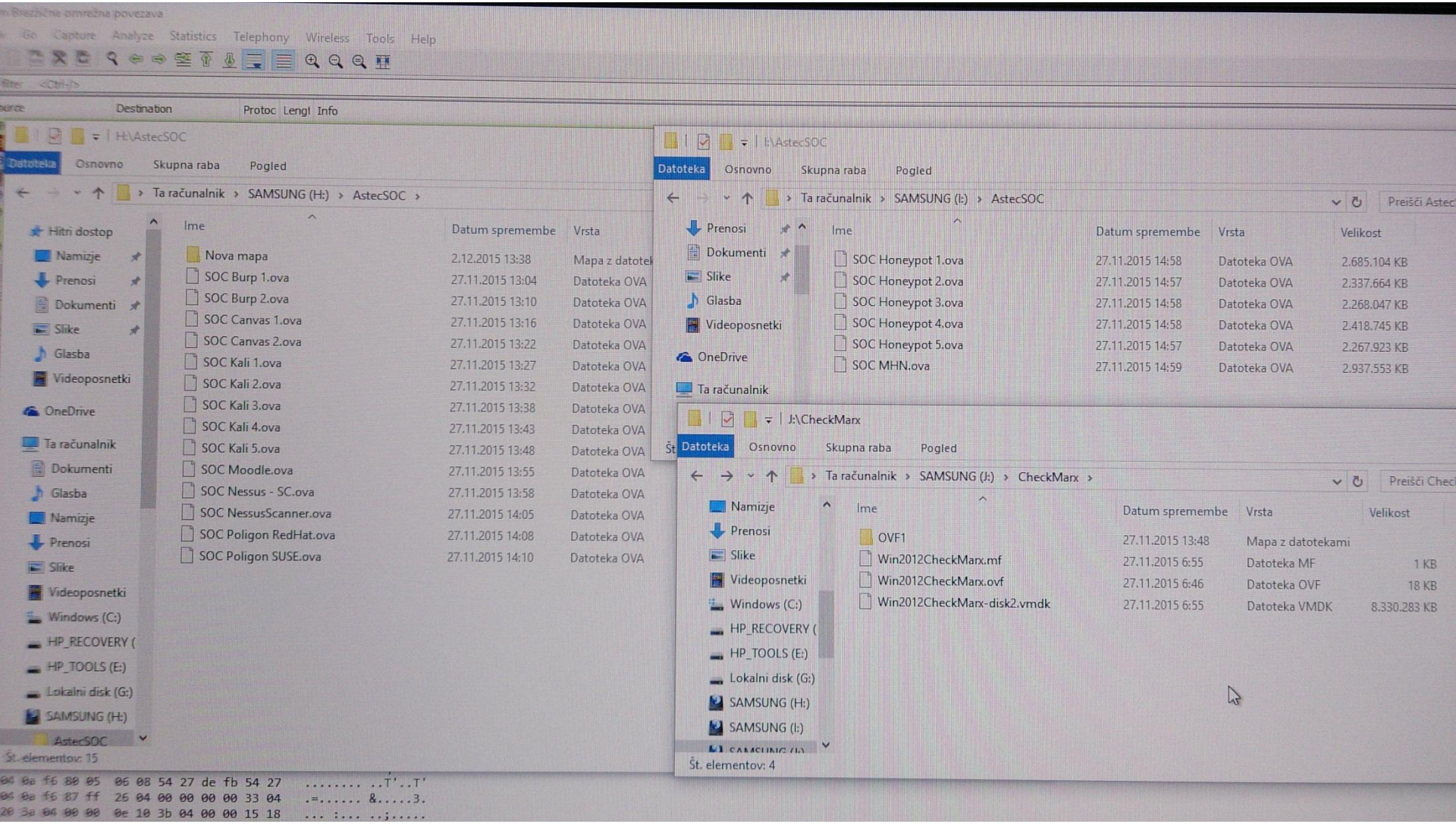



Add Evidence
FILE
Add Local Device
Add Network Preview
Add Evidence File
Add Raw Image
Add Crossover Preview
ZBook
CORE i7

zazanavanje incidentov



Penetration testing



Učinki

Neposredni:

- enotna informacijska varnost v državni upravi: prihranek pri nabavi opreme in izvajanju storitev
- upoštevanje varnostnih standardov pri razvoju programske opreme.

Posredni:

- boljše odzivanje na varnostne grožnje in incidente
- večja ozaveščenost in obveščenost uporabnikov
- zmanjšanje varnostnih incidentov.

„Brez projekta“:

- večja varnostna tveganja, možnosti vdorov, odtekanja podatkov
- ogrožanje in onemogočanje državne infrastrukture in servisov.

Hvala za pozornost!

mag. Damijan Marinšek
damijan.marinsek@gov.si