**Preduvjeti za implementaciju nadzora mreže**

U ovom dokumentu su navedeni preduvjeti za implementaciju nadzora mreže.

# Mrežna oprema

Na segmentima mreže na kojima je implementiran NAT (network address translation), promet je potrebno nadzirati s „unutrašnje“ strane mreže, prije nego što se NAT-ira, kako bi se u slučaju detekcije malicioznog prometa moglo utvrditi koje računalo je kompromitirano.

Preklopnici (engl. switch) kroz koje promet prolazi prije nego što se NAT-ira moraju podržavati *port mirroring,* kako bi se dio prometa ili sav promet kroz preklopnik mogao usmjeriti u nadzornu opremu (senzor) koja će ga analizirati.

# Dnevnički zapisi (engl. Logs)

Potrebno je imati DHCP dnevničke zapise koji će nedvojbeno pokazivati koje računalo je imalo koju IP adresu u koje vrijeme.

Poželjno je imati i mogućnost povezivanja MAC adrese s fizičkom utičnicom, dakle potrebno je moći doći do informacije o tome:

* Na koji priključak (engl. Port) preklopnika je povezana MAC adresa (obično dostupno kroz admin sučelje preklopnika). Time se može fizičkim uvidom u spojeve opreme provjeriti je li bilo neovlaštenih radnji.
* U kojoj prostoriji ustanove se nalazi utičnica koja je povezana na taj priključak. Time se omogućava brzo pronalaženje kompromitirane opreme i fizički uvid u nju, kao i djelovanje za ispravljanje ranjivosti.

Ako se želi nadzirati i segment mreže u kojeg se studenti ili djelatnici povezuju vlastitim uređajima (npr. eduroam WiFi) potrebno je i za njega imati dnevničke zapise o tome koji se korisnik spojio na mrežu u koje vrijeme i koja IP adresa mu je bila dodijeljena.

# Senzori

Senzori su računala će prikupljati i analizirati promet na preklopniku.

Ta računala trebaju imati sljedeće dijelove i svojstva:

* CPU s x86-64 ili aarch64 arhitekturom (jedna jezgra je dovoljna)
* Bar 4GB RAM-a
* Bar 18GB diskovnog prostora
* Ethernet priključak koji podržava brzinu od najmanje 1Gbps
* Drugi ethernet priključak ili USB priključak na koji će se moći priključiti ethernet dongle (brzina nije osobito bitna, taj priključak će se koristiti za upravljanje senzorom)

Senzor bi trebao biti, koliko je to moguće, fizički zaštićen (npr. biti u mrežnom ormariću s preklopnikom, zaključan).

Mini PC može biti dobar izbor za senzor zbog niske cijene i malih dimenzija, ali može se koristiti i bilo koje drugo računalo koje zadovoljava specifikacije.

# Poslužitelj za upravljanje senzorima i prikazivanje rezultata

Potrebna je Linux virtualna mašina ili fizički server s barem 2GB RAM-a i barem 18GB diskovnog prostora

# Slanje upozorenja elektroničkom poštom

Ako je detektiran događaj visoke ozbiljnosti (npr. detektiran je promet prema poznatoj *malware* domeni), upravljački server će automatski poslati e-mail Nacionalnom CERT-u.

Moguće je koristiti vanjski SMTP server ili SMTP server ugrađen u upravljačku aplikaciju.

Ako se koristi vanjski SMTP server, potrebno je stvoriti korisnički račun koji upravljačka aplikacija može koristiti za slanje.

Ako se koristi ugrađeni SMTP server, upravljački server mora imati statičku javnu IP adresu te se moraju konfigurirati ispravni SPF i DKIM DNS zapisi za domenu s koje se šalje.