Univerza v Mariboru

Fakulteta za organizacijske vede

Magistrsko delo

Organizacija in management informacijskih sistemov

ZAŠČITA RAČUNALNIŠKIH OMREŽIJ V VZGOJNO IZOBRAŽEVALNIH ZAVODIH

Mentorica: doc. dr. Alenka Brezavšček

Kandidat: Jure Knez

Kranj, september 2014

ZAHVALA

Zahvaljujem se mentorici, doc. dr. Alenki Brezavšček, za napotke, svetovanje in pomoč pri izdelavi magistrskega dela.

Zahvaljujem se tudi moji Martini za pomoč pri oblikovanju in Aniti Leskovar za lektoriranje magistrskega dela.

POVZETEK

Varnost informacijskih sistemov v vzgojno-izobraževalnih zavodih je na prvi pogled videti enostavna. Vendar, kot je pokazala raziskava, na zavodih večinoma nimajo osebe, ki bi primarno skrbela za informacijski sistem. Še največkrat so to učitelji, ki poleg svojega rednega dela (poučevanja) skrbijo še za informacijski sistem in nimajo ustreznega znanja o vzdrževanju in primerni varnosti. V Sloveniji jim pri nasvetih za lokalna omrežja in strežnike svetuje Arnes, znotraj Arnesa pa glede varnosti SI-CERT in njegov projekt ozaveščanja, Varni na Internetu.

V nalogi je predstavljeno stanje varnosti v vzgojno-izobraževalnih zavodih v Sloveniji. Raziskali smo tudi dobre prakse v tujini.

Na podlagi rezultatov ankete in dobrih praks iz tujine smo podali mnenja, kaj bi lahko, za dodatno varnost informacijskih sistemov v vzgojno-izobraževalnih zavodih, storili država, Arnes in sami zavodi.

Kot pomoč zavodom pri vzpostavitvi varnega računalniškega omrežja smo pripravili tudi nasvete za vzpostavitev varnostne politike in priporočila za zaščito računalniških omrežij.

KLJUČNE BESEDE:

- vzgojno-izobraževalni zavod
- varnost
- informacijski sistem
- računalniško omrežje
- priporočila

ABSTRACT

IT security in educational organizations seems anything but hard at a first glance. However as the research has shown, educational institutions don't have dedicated IT persons to take care of their informational system. This job is mostly run by teachers who in addition to their teaching also take care of the institution's information system, even though they are not properly educated. In Slovenia Arnes is advising them how to manage their local connections and Si-Cert, who is a part of Arnes, with their project Safe on the internet about managing security.

Thesis presents the state of security in Slovenian educational organizations. We have researched best practices abroad.

Based on the pole results and cases of best practices from abroad, we passed an opinion what could do Arnes, the state and institutions for the security of their information system. As assistance on how to safely connect to the network, we have also prepared additional guidelines how to establish security policy and recommendations on protecting computer network.

KEYWORDS

- educational organization
- security
- information system
- computer network
- recommendations

KAZALO

1. UVOD 1
   1.1. Predstavitev problema 1
   1.2. Cilji in namen naloge 3
   1.3. Predpostavke in omejitve 4
   1.4. Metode dela 4
2. OSNOVNI POJMI S PODROČJA INFORMACIJSKE VARNOSTI 5
   2.1. Varnost informacijskega sistema 5
   2.2. Grožnje varnosti 7
   2.3. Varovalni ukrepi zoper uresničitev groženj 8
3. ZAGOTAVLJANJE VARNOSTI V RAČUNALNIŠKEM OMREŽJU 13
   3.1. OSI model 13
      3.1.1. Fizična plast 14
      3.1.2. Povezovalna plast 15
      3.1.3. Omrežna plast 16
      3.1.4. Prenosna plast 17
      3.1.5. Plast seje 19
      3.1.6. Predstavitvena plast 20
      3.1.7. Aplikacijska plast 21
   3.2. Vloga človeka pri zagotavljanju varnosti v računalniškem omrežju 21
   3.3. Najpogostejši napadi na računalniška omrežja 22
      3.3.1. Kraja podatkov 22
      3.3.2. Napadi na strojno opremo 23
      3.3.3. Prisluškovanje 23
      3.3.4. Napad onemogočanja 24
      3.3.5. ARP napadi 24
      3.3.6. Preskakovanje med VLAN-i (angl. VLAN hopping) 25
      3.3.7. Napad na telefonski (angl. Voice) VLAN 25
      3.3.8. DHCP napadi 26
      3.3.9. Napadi na brezžična omrežja 26
      3.3.10. Napadi na IPv4 protokol 27
      3.3.11. Napadi na IPv6 protokol 29
      3.3.12. Napadi na usmerjevalnik in usmerjanje 31
      3.3.13. SYN napad 31
      3.3.14. Kraja/ugrabitev seje (Session Hijacking) 32

3.3.15. DNS zastrupljanje (Domain Name System Poisoning) 33
3.3.16. NetBIOS napadi 33
3.3.17. Vohljanje šifriranega prometa (Sniffing Encrypted Traffic) 34
3.3.18. SQL vrinjenje (SQL Injection) 34
3.3.19. Vrinjenje kode (Code Injection) 35
3.3.20. XSS napad (Cross-Site Scripting – XSS) 36
3.3.21. Napad z DNS odbojem (DNS reflection, DNS amplification) 36
3.3.22. "Heartbleed" ranljivost 37
3.3.23. Socialni inženiring 37
4. ZAGOTAVLJANJE VARNOSTI RAČUNALNIŠKIH OMREŽIJ V VIZ 42
4.1. Stanje v Sloveniji 42
4.1.1. Vloga posameznih državnih organizacij 43
4.1.2. Analiza obstoječega stanja v slovenskih VIZ 49
5. PRIMERI DOBRIH PRAKS IZ TUJINE 80
5.1. Hrvaška 80
5.2. Estonija 82
5.3. Anglija 83
5.4. Norveška 85
6. PREDLOGI ZA IZBOLJŠANJE VARNOSTI RAČUNALNIŠKIH OMREŽIJ VIZ V SLOVENIJI 90
6.1. Kaj je potrebno urediti na nivoju države? 90
6.2. Kaj lahko stori Arnes? 91
6.3. Naloge vodstva VIZ in skrbnika računalniška sistema VIZ 92
7. ZAKLJUČEK 95
LITERATURA IN VIRI 97

1. UVOD

1.1. Predstavitev problema

Z nezadržno širitvijo interneta postaja varovanje računalniških sistemov, ki so povezani v lokalna omrežja in svetovni splet, vse bolj pomembno. Vzrok za širitev je cenovna dostopnost in pa številne prednosti uporabe informacijsko komunikacijske tehnologije (v nadaljevanju IKT). Vendar pa mnogi ne razmišljajo o slabostih, ki jih prinaša uporaba IKT. Mnogi namreč ne razmišljajo o varnosti.

Mnoga podjetja kljub številnim poročilom o kršitvah varnosti in o odpovedih sistemov še vedno zanemarjajo varnost, saj je draga in jim ne predstavlja ključnega dela poslovanja. Poleg tega odžira denar, ki ga vodstva raje porabijo za druge namene (Greengard, 2014).

Ko se varnostna grožnja pojavi in ni nikogar, ki bi ukrepal, lahko zapoznelo ukrepanje in neodločnost onemogočita učinkovit odziv. Danes lahko namreč številne organizacije prepoznajo varnostne incidente v svojem okolju IT, a se ne zmorejo učinkovito odzvati − še zlasti na nove grožnje (Greengard, 2014).

Ker se varnostne grožnje nenehno spreminjajo, morajo organizacije obvladovati množico programov, konfiguracij strojne opreme, notranjih skrbnikov, programskih kod in svetovalcev − vse to lahko povzroči neobvladljivost in neučinkovitost. Na določeni točki ves sistem odpove in podjetje se znajde v godlji (Greengard, 2014).

V današnjih dneh napadalci vse bolj izkoriščajo naivnost uporabnikov (socialni inženiring, ribarjenje …), na udaru so tudi naprave in programi z varnostnimi luknjami. Hkrati je čedalje več groženj, zasnovanih tako, da izkoriščajo najšibkejši varnostni člen v verigi, to so zaposleni. Še zlasti tehnike socialnega inženiringa, kot sta lažno predstavljanje in usmerjeno lažno predstavljanje (slednje je usmerjeno na določeno osebo ali manjšo skupino), so zelo nevarne.

Analize kažejo, da iz leta v leto število napadov na računalniške sisteme raste. Če pogledamo slovensko statistiko, je od leta 2008 do konca leta 2013 število obravnavanih incidentov Slovenskega nacionalnega centra za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij naraslo s 328 na 1513, torej za dobrih 360 %, letos pa jih pričakujejo čez 2000 (SI-CERT, 2014).

Vpeljava sistema za zagotavljanje informacijske varnosti je za organizacijo lahko zelo dolg in zelo drag projekt, ki ga morajo voditi kot kontinuiran proces, če želijo doseči čim višjo stopnjo informacijske varnosti. Ravno zaradi tega je veliko organizacij (vodstev) zadovoljnih že z enostavnim protivirusnim programom, ki naj bi rešil vse težave. Prav tako vodstvo ne vidi vseh potencialnih groženj, ki pretijo informacijskemu sistemu, veliko informatikov pa se na tem področju premalo izobražuje. Za številna podjetja je izobraževanje drugotnega pomena ali pa se jim zdi zelo stroškovno neučinkovito ljudi odmikati od dela (Greengard, 2014).

Na koncu so informatiki tisti, ki bi morali vodstvu svetovati in predlagati varovalne ukrepe za zmanjšanje tveganja na sprejemljivo raven.

Na grožnjo se je preprosto odzvati z blokiranjem neposrednega sporočanja ali s prepovedjo uporabe pomnilniških naprav USB, s katerimi je mogoče prenašati podatke zunaj fizičnih zidov pisarne. Videz večje varnosti se lahko ustvari tudi tako, da se od zaposlenih zahteva, naj vsak mesec spremenijo geslo. Žal pa lahko takšna nadležna pravila zmanjšajo storilnost ali celo spodbudijo zaposlene, da jih zaobidejo. Neustrezni pravilniki lahko postanejo ovira za delovno storilnost in dejansko povečajo varnostno tveganje (Greengard, 2014).

Poleg »hekerjev« in vdiralcev se številne varnostne kršitve dogajajo znotraj podjetja. Nezadovoljni ali nepošteni zaposleni so stalna grožnja in neprevidnost ima lahko hude posledice. Še zlasti jo lahko izkoristijo nepridipravi s prenosnimi računalniki in pametnimi telefoni ali tablicami. Osebja na visokih položajih in skrbnikov s praktično neomejenimi pooblastili za dostop skoraj ni mogoče zaustaviti. Dodatna skrb so tudi dostavno osebje, začasni delavci in celo vratarji, ki jim je pogosto dovoljeno nemoteno gibanje po prostorih podjetja.

Popolnoma odprti ali slabo zavarovani sistemi so lahka tarča napadalcev, ki take sisteme pogosto izkoristijo kot odskočne deske pri vdiranju v druge sisteme. S slabo zaščitenim ali celo nezaščitenim računalniškim sistemom lahko povzročimo neljube dogodke, ki imajo v najslabšem primeru za posledico izpad in nedostopnost informacijskega sistema, zato je potrebno zmanjšati take neljube dogodke.

Tudi v vzgojno-izobraževalnih zavodih (v nadaljevanju VIZ) se IKT vedno bolj uveljavlja. Pedagoški proces je iz leta v leto bolj usmerjen v uporabo sodobnih tehnoloških pripomočkov, ki odpirajo nove možnosti in priložnosti za poučevanje in izobraževanje (elektronske table, tablice …) na eni strani, na drugi strani pa se tudi administrativni postopki (e-redovalnica, e-dnevnik, nacionalno preverjanje znanja, računovodstvo …) selijo v elektronsko obliko in na internet.

Štraser(2012) v svojem magistrskem delu navaja, da je bila Slovenija sicer ena izmed prvih evropskih držav, ki je v letu 1993 zagotovila pogoje za dolgoročni sistematični preskok na področju uporabe IKT pri poučevanju in učenju. Definirana so bila tri glavna področja vlaganja sredstev in izvajanja dejavnosti:

- izobraževanje učiteljev;
- opremljanje vzgojno-izobraževalnih zavodov (strojna in programska oprema, lokalna omrežja z dostopom do interneta);
- raziskovanje in razvoj (strateški raziskovalni projekti, razvojni projekti, evalvacije).

Na VIZ večinoma uporabljajo Windows strežnike in delovne postaje, ki so zaradi številnih ranljivosti za napadalce najbolj zanimivi. Administratorji sistemov se zaradi nepoznavanja delovanja sistemov pogosto odločijo, da bodo do teh strežnikov omogočili ves promet z interneta. Poleg operacijskih sistemov so ranljivi tudi sistemi, ki tečejo na teh strežnikih (Joomla, Moodle …), saj jih administratorji, pogosto zaradi neznanja, ne posodabljajo. Prav tako je posebno pozornost potrebno nameniti tudi infrastrukturi (stikala, dostopne točke, napajanje, razni krmilniki (npr. SCADA), dostop do infrastrukture). Krivde ne moremo zvaliti samo na administratorje sistemov. Precejšni del odgovornosti nosi pristojno ministrstvo, saj je v sistematizaciji delovnih mest medlo opredeljeno

delovno mesto informatika. Večji centri imajo polno zaposlenega informatika, medtem ko v osnovnih šolah za to skrbijo učitelji, ki s samim poukom ne dosežejo zahtevanega števila ur, tako npr. učitelj angleščine ali športne vzgoje res ne more poznati delovanja informacijskega sistema.

Pri varnosti VIZ ima Akademska in raziskovalna mreža Slovenije (v nadaljevanju Arnes) pomembno vlogo, saj s svojimi nasveti poskuša čim bolj pomagati skrbnikom na šolah, ki tega znanja nimajo. V okviru Arnesa deluje tudi Slovenski nacionalni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij (v nadaljevanju SI-CERT) in pod njegovim okriljem projekt Varni na internetu. Vendar se zopet pojavi težava v pomanjkanju kadra, ki bi se lahko posvetil izobraževanju kadrov na VIZ. Na drugi strani je težava tudi v samih kadrih VIZ-a, saj nekateri želje po samoizobraževanju nimajo.

Prej omenjena težava v sistematizaciji delovnih mest ima za posledico neizobražene skrbnike informacijskih sistemov. Skrbniki sistemov v šolstvu nimajo posebnih izobraževanj na temo varnosti informacijskih sistemov, zato bomo na podlagi analize najpogostejših napadov, trenutnega stanja na VIZ in podatkov, kako se tega lotevajo v tujini, podali priporočila za zaščito omrežij v slovenskih VIZ. Z njihovo pomočjo bi skrbniki sistemov v VIZ lažje vzdrževali omrežja in s tem doprinesli k višjemu nivoju varnosti. Iskanje rešitve po tem, ko do težave že pride, je večinoma prepozno. Varnostno politiko je v prvi vrsti potrebno ustrezno načrtovati, izdelati ukrepe ob morebitnem varnostnem incidentu in skrbeti tudi za ozaveščanje uporabnikov o njej.

1.2. Cilji in namen naloge

Namen magistrskega dela je proučiti stanje na področju zagotavljanja informacijske varnosti na VIZ in izdelati celovita priporočila za zaščito omrežij v VIZ.

Delo bo na ta način poenostavljeno in olajšano, hkrati bo ob upoštevanju priporočil dosežena ustrezna stopnja informacijske varnosti.

Magistrsko delo je sestavljeno iz teoretičnega dela, ki vsebuje:

- opredelitve osnovnih pojmov s področja informacijske varnosti,
- predstavitev in analizo groženj na posamezni plasti OSI modela,
- vlogo človeka pri zagotavljanju varnosti v računalniškem omrežju,
- dobre prakse pri uvajanju informacijske varnosti v šolstvu doma in v tujini.

Aplikativni del naloge vsebuje:

- analizo stanja varovanja omrežij v slovenskih VIZ zavodih,
- predloge za izboljšanje varnosti računalniških omrežij v Sloveniji,
- priporočila za zaščito računalniških omrežij v slovenskih VIZ zavodih.

Končni cilj magistrskega dela je izdelati predloge za izboljšavo varnosti računalniški omrežij v Sloveniji. Podali bomo naša mnenja, kaj lahko za to storijo

država, Arnes in sami VIZ. Obenem bomo podali tudi enotna priporočila, ki jih bodo lahko uporabili vzdrževalci omrežij v VIZ, za kar se da dobro zavarovanje njihovih računalniških omrežij.

1.3. Predpostavke in omejitve

Arnes je javni zavod, ki zagotavlja omrežne storitve organizacijam s področja raziskovanja, izobraževanja in kulture. Omogoča tudi njihovo povezovanje in medsebojno sodelovanje ter sodelovanje s sorodnimi organizacijami v tujini. V omrežje ARNES je povezanih več kot 1000 slovenskih organizacij s področja raziskovanja, izobraževanja in kulture. Na vsaki od njih Arnes upravlja z napravo za dostop (Cisco usmerjevalnik, stikalo), kjer se ščiti omrežje s pomočjo filtrov (angl. access-list) in delitvijo omrežja na virtualna omrežja (VLAN).

Omejitev pri izdelavi magistrske naloge prestavlja dejstvo, da je težko pridobiti podatke o varovanju VIZ omrežij v tujini, kajti v večini skrbniki nacionalnega raziskovalnega in izobraževalnega omrežja (NREN) skrbijo samo za univerze, kjer že imajo ustrezno izobražen kader, ki skrbi za računalniška omrežja.

Zaradi poznavanja delovanja naprav in omrežij, upoštevanja varnostnih protokolov in stalnega nadzora se bomo v magistrskem delu omejili predvsem na VIZ, ki so povezani v omrežje ARNES.

1.4. Metode dela

V raziskavi se bomo z deskriptivno metodo sistematično lotili analize javno objavljenih podatkov o napadih na računalniške sisteme. Pomagali si bomo z literaturo in viri, ki so dosegljivi na spletu, strokovnih in znanstvenih prispevkih, predstavitvah predstavljenih na konferencah, delavnicah in seminarjih.

Glede na izkušnje pri delu z VIZ in z izvedeno anketo o varnosti informacijskega sistema v VIZ bomo predstavili stanje na slovenskih VIZ, katerih skrbniki bodo izpolnili anketo. Od hrvaškega NRENa (CARNET) in estonskega doktorskega študenta bomo pridobili podatke, kako se z varovanjem omrežij spopadajo pri njih.

2. OSNOVNI POJMI S PODROČJA INFORMACIJSKE VARNOSTI

2.1. Varnost informacijskega sistema

Vse informacije, ki se nahajajo v neki organizaciji in predstavljajo zanjo vrednost ali korist, moramo obravnavati kot dobrino. Dobrine kot take je potrebno varovati pred uresničitvijo groženj (Brezavšček, 2008). Dobrine lahko razvrstimo na naslednji način:

- otipljive:
  - strojna oprema,
  - ljudje.
- neotipljive so logične entitete, ki jih predstavljajo:
  - programska oprema,
  - podatki,
  - informacije.

Področje informacijske varnosti se je močno razmahnilo in se v zadnjih letih močno razvija, zaradi tega postaja varovanje računalniških sistemov, ki so povezani v lokalna omrežja in svetovni splet, vse bolj pomembno. IKT postaja čedalje bolj cenovno dostopen ter prinaša številne prednosti, vendar se pogosto ne razmišlja o slabostih in nevarnostih, ki jih IKT prinaša s sabo.

Varnost informacijskega sistema lahko definiramo kot sposobnost, da informacijski sistem pri določenih pogojih zadovoljivo opravlja zahtevane funkcije brez nezaželenih dogodkov, ki bi negativno vplivali na zaupnost, celovitost ali razpoložljivost informacijskega sistema (Brezavšček, 2008). Temelji informacijske varnosti so torej:

a) Zaupnost (angl. confidentiality)

Zagotavljanje zaupnosti pomeni preprečevanje nepooblaščenega razkritja občutljivih podatkov/informacij. Dejansko ni mogoče dobiti vozniškega dovoljenja, najeti apartmaja, prejeti zdravstvene oskrbe ali najeti posojila brez, da bi povedali zelo zaupne informacije o sebi, kot so ime, naslov, telefonska številka, datum rojstva, EMŠO, davčna številka, materialni status, število otrok, materin dekliški priimek, dohodek, delovno mesto, zgodovina zdravja itn. To so vse zaupni podatki, ki se od nas zahtevajo za izvršitev določenega posla. Običajno upamo, da bo oseba ali institucija, ki ji zaupamo, zasebne informacije zaščitila pred nepooblaščenim odkritjem, slučajnim ali namernim, in da bodo naše informacije posredovane ljudem, institucijam, ki so pooblaščene za dostop in jih resnično potrebujejo.

Informacije, ki so mišljene kot zaupne že po naravi, morajo biti dostopne, uporabljene ali razkrite osebam, ki imajo pooblastilo za njih, in takrat, ko je to resnično potrebno. Do kršitve zaupnosti pride, ko je informacija, ki je že po naravi mišljena kot zaupna ali bi to morala biti, uporabljena, kopirana ali razkrita od nekoga, ki ni pooblaščen za dostop do nje.

Vlada, vojska, finančne institucije, bolnišnice in privatna podjetja kopičijo velike količine zaupnih informacij o njihovih zaposlenih, strankah, proizvodih, raziskavah in finančnem položaju. Večina teh informacij je zbrana, obdelana in shranjena na računalnikih in prenesena skozi mreže na druge računalnike. Zaupni podatki o poslovnih strankah ali financah nove proizvodne linije bi lahko padli v roke konkurenta, posledično lahko vodijo v izgubo posla. Varovanje zaupnih podatkov je tako poslovna kot v mnogih primerih tudi etična in pravna zahteva (Informacijska varnost. Wikipedija, 2014).

Primer: dovoliti nekomu, da gleda čez tvojo ramo na ekran računalnika, ko imaš na njem zaupne podatke, je kršitev zaupnosti, če oseba ni pooblaščena za dostop do teh informacij. Ukradeni prenosni računalnik iz avtomobila, ki vsebuje informacije o zaposlitvi in zaslužkih okrog 100.000 zaposlenih, pomeni kršitev zaupnosti, ker so informacije sedaj v rokah nekoga, ki ni pooblaščen, da bi jih imel (Informacijska varnost. Wikipedija, 2014).

b) Celovitost/neokrnjenost (angl. integrity)

Zagotavljanje celovitosti pomeni, da informacijski sistem opravlja svojo funkcijo na predviden način, brez namernih in nenamernih posegov vanj, ki bi povzročili njegovo spremembo (Štraser, 2012).
Celovitost, v sklopu pojma informacijske varnosti, pomeni, da podatki ne smejo biti ustvarjeni, spremenjeni ali uničeni brez pooblastila. Prav tako pomeni, da so podatki shranjeni v enem delu informacijskega sistema, v skladu z drugimi sorodnimi podatki, shranjenimi v drugem delu informacijskega sistema (ali v drugem sistemu).

Primer: do izgube celovitosti lahko pride, ko informacijski sistem ni primerno zaustavljen ali ko informacijski strežnik nenadoma izgubi električno energijo. Izguba celovitosti pomeni tudi nenameren ali zlonameren izbris pomembne informacijske datoteke (Informacijska varnost. Wikipedija, 2014).

c) Razpoložljivost (angl. availability)

Razpoložljivost informacijskega sistema razumemo kot njegovo dostopnost za pooblaščenega uporabnika, kadar koli ga le-ta potrebuje.
Izguba razpoložljivosti lahko povzroči nedostopnost informacijskega sistema ali zahtevane informacije, v skrajnem primeru pa tudi njegovo uničenje (Brezavšček, 2008).

Informacijska varnost pomeni varstvo podatkov in informacijskih sistemov pred nezakonitim dostopom, uporabo, razkritjem, ločitvijo, spremembo ali uničenjem. Izrazi informacijska varnost, varovanje računalniških sistemov, varstvo informacij se pogosto uporabljajo kot sinonimi. Kljub temu, da so ta področja v medsebojnem odnosu in si delijo skupne cilje varstva zaupnosti, neokrnjenosti in razpoložljivosti informacij, obstajajo med njimi komaj opazne razlike. Informacijska varnost je mišljena kot zaupnost, neokrnjenost in razpoložljivost podatkov ne glede na njihovo obliko: elektronsko, tiskano ali katero drugo (Informacijska varnost. Wikipedija, 20014).

2.2. Grožnje varnosti

Grožnja varnosti je kakršen koli neželen dogodek, ki če se zgodi, negativno vpliva na katero koli dobrino informacijskega sistema organizacije (Brezavšček, 2008). Informacijski sistemi v organizacijah so podvrženi številnim grožnjam, ki lahko povzročijo nepopravljivo škodo. Posledice uresničenih groženj se raztezajo od izgube ali nerazpoložljivosti podatkov in vse do uničenja celotnega informacijskega sistema organizacije (Vehar, 2012).
Grožnje varnosti lahko razdelimo glede na (Brezavšček, 2008):

- **izvor grožnje:**
  - **izredni dogodki:**
    - požar,
    - poplava, padavine,
    - izpad, nihanje električne energije,
  - **naključni dogodki:**
    - odpoved strojne opreme,
    - odpoved programske opreme,
    - odpoved človeka,
  - **človekova dejavnost:**
    - vlom (kraja, vandalizem),
    - sabotaža,
    - nepooblaščen dostop do sistema − logični vdor,
    - programski vsiljivci,
    - vdor v komunikacijo,
    - ohromitev strežnika,
    - zanikanje udeležbe v komunikaciji,
    - izkoriščanje organizacijske pomanjkljivosti,
- **na naravo dobrine, kateri grožnja preti:**
  - **fizične grožnje:**
    neposredno ogrožajo otipljive, posredno tudi neotipljive, dobrine informacijskega sistema (izredni dogodki, človekova dejavnost);
  - **logične grožnje**
    ogrožajo neotipljive dobrine informacijskega sistema (človekova dejavnost);
- **učinek grožnje:**
  - **aktivne grožnje:**
    kadar se realizira, povzroči določeno škodo kakor tudi poškoduje ali celo uniči dobrino informacijskega sistema (npr. nepooblaščena sprememba podatkov);
  - **pasivne grožnje**
    kadar se realizira, povzroči določeno škodo, vendar dobrine informacijskega sistema ne spremeni (npr. nepooblaščeno razkritje oz. kraja zaupnih podatkov).

Do same grožnje in njene uresničitve pride zaradi ranljivosti. Ranljivost je vsaka pomanjkljivost dobrine ali skupine dobrin, ki jo lahko določena grožnja izkoristi. Je posledica bodisi slabe zaščite dobrine zoper določeno grožnjo bodisi atraktivnost dobrine za napadalca. Od obstoječe zaščite je odvisna stopnja ranljivosti, medtem ko je pogostost uresničitve grožnje od nje neodvisna (Brezavšček, 2008).

Izraba ranljivosti ima lahko negativne posledice za organizacijo. Delimo jih na:

- primarne posledice:
  - nedostopnost ali uničenje katere koli dobrine (prizadeta razpoložljivost),
  - sprememba katere koli dobrine (prizadeta celovitost),
  - razkritje podatkov/informacij (prizadeta zaupnost),
- sekundarne posledice – neposredni ali posredni stroški.

2.3. Varovalni ukrepi zoper uresničitev groženj

Da bi lahko preprečili grožnje informacijskemu sistemu ali zmanjšali stopnjo ranljivosti, je pomembno znanje, kako grožnje zaznati in se jim z uvedbo ustreznih zaščitnih ukrepov izogniti. Varovalni ukrep je kontrola, postopek ali mehanizem, s katerim želimo odpraviti obstoječe ranljivosti informacijskega sistema. Delitev varovalnih ukrepov:

a) Fizična zaščita

Gre za ustrezno zunanje in notranje varovanje. Omejiti je potrebno dostop do prostorov, v katerih se nahajajo ključne sestavine informacijsko komunikacijskega sistema. To so (Vehar 2012):

- strežniki;
- diskovna polja;
- usmerjevalniki, stikala, modemi;
- električni in telekomunikacijski vodi;
- požarni zid;
- brezprekinitveno napajanje UPS;
- fizični nosilci ključnih podatkov.

Da bi lahko takšno zaščito izvajali, je potrebno v organizaciji sprejeti ukrepe za zaščito dobrin informacijskega sistema, saj je dobra fizična varnost predpogoj za ustrezno logično varnost (Brezavšček, 2008). Zagotavljanje fizične varnosti zajema zaščito zoper: požar, padavine in poplavo, izpad in nihanje električne energije, vlom, izgubo podatkov ter preprečevanje odpovedi strojne opreme.

V primeru, da organizacijo zajame požar, so ogrožene vse dobrine, možne posledice so: smrt ali poškodba ljudi, uničenje ali poškodba ostalih dobrin in nerazpoložljivost informacijskega sistema. Varovalni ukrepi zoper požar so (Brezavšček, 2008):

- zidovi in vrata v prostore, ki vsebujejo občutljive dobrine, naj bodo izdelani iz ognjevarnih materialov;
- v vseh prostorih morajo biti nameščeni javljalniki požara;
- v prostorih, ki vsebujejo občutljive dobrine, naj bodo nameščene protipožarne naprave oz. avtomatiziran protipožarni sistem;
- avtomatiziran sistem mora biti načrtovan tako, da je možnost poškodb osebja najmanjša;

- zaposleni morajo biti seznanjeni s protipožarnimi ukrepi in usposobljeni za uporabo protipožarnih naprav. Upoštevati morajo tudi pravilnik o protipožarni zaščiti;
- prepoved kajenja znotraj organizacije.

Drugi dejavnik, s katerim se je še težje boriti kot z ognjem, je voda. V primeru poplav ali padavin je ogrožena strojna in programska oprema ter podatki in informacije. Možne posledice vdora vode so: uničenje ali poškodba dobrin, delna ali popolna nerazpoložljivost sistema. Varovalni ukrepi zoper vodo ali padavine so (Brezavšček, 2008):

- prostor, ki vsebuje občutljive dobrine, naj bo lociran v pritličju na dvignjenem podu ali višje v zgradbi;
- v prostoru naj bodo nameščeni detektorji in javljalniki za naraščajočo vodo;
- strop naj bo brez kakršnih koli vodnih instalacij;
- strop naj bo brez odprtin in/ali dotrajanih mest, kjer bi voda lahko prodrla v prostor;
- v primeru padavin naj bo na razpolago plastična folija za pokrivanje opreme.

Izpad ali nihanje električne energije lahko povzroči poškodbo strojne opreme ter izgubo ali popačenje podatkov/informacij in nerazpoložljivost sistema. Varovalni ukrepi zoper izpad ali nihanje električne energije so (Brezavšček, 2008):

- električno napajanje naj se izklopi z enim samim stikalom;
- prostori naj bodo opremljeni s sistemom za uravnavanje napetostnih nihanj;
- prostori naj bodo opremljeni z nadomestnim virom napajanja;
- prostori naj bodo opremljeni s sistemom za preprečevanje poškodbe ob strelah.

Tudi pri vlomu gre za fizično grožnjo. Ogrožene so vse vrste dobrin, možne posledice so lahko: smrt ali poškodbe ljudi, uničenje ali poškodbe ostalih dobrin ter delna ali popolna nerazpoložljivost sistema. Varovalni ukrepi zoper vlom so (Brezavšček, 2008):

- prostor, ki vsebuje občutljive dobrine, naj bo lociran tako, da je lahek dostop omogočen samo pooblaščenim osebam;
- okna v prostoru naj bodo narejena tako, da ni mogoč dostop od zunaj ali zaščitena z mrežo;
- vsi dostopi skozi vhodna vrata naj bodo pod neposrednim nadzorom varnostnega osebja;
- območje gibanja strank naj bo urejeno tako, da se opazi, če obiskovalec kaj odloži;
- opaznost prostora, ki vsebuje občutljive dobrine, naj bo majhna;
- vsi zasilni izhodi naj bodo označeni in pod stalnim nazorom ali opremljeni z alarmnimi napravami.

Strojna oprema lahko odpove tudi brez posledice zunanjih vplivov. Posledice okvare so lahko: izguba ali popačenje podatkov/informacij, nerazpoložljivost strojne opreme, delna ali popolna nerazpoložljivost sistema. Varovalni ukrepi proti zoper okvaro strojne opreme so (Brezavšček, 2008):

- za gradnike strojne opreme, ki so s stališča zanesljivosti kritični, naj se uvede redundanca;
- zagotovijo naj se ustrezni obremenilni pogoji pri delovanju strojne opreme;
- oblikuje naj se učinkovita strategija vzdrževanja, ki naj se dosledno izvaja;
- v pogodbah o vzdrževanju je potrebno dokumentirati vse varnostne zahteve, ki jih mora osebje, ki izvaja vzdrževanje, izpolnjevati.

Ena najhujših posledic uresničitve katere koli izmed fizičnih groženj je izguba podatkov, ki se v informacijskem sistemu organizacije hranijo. To lahko preprečimo z naslednjima preventivnima ukrepoma:

- redno izvajanje varnostnih kopij,
- podvajanje podatkov v realnem času.

Za preprečevanje izgube podatkov je potrebno vpeljati postopek periodičnega izvajanja varnostnih kopij ključnih podatkov, ki so za nemoteno poslovanje organizacije nujno potrebni. Z varnostnim kopiranjem tako zagotovimo, da bodo ključni podatki razpoložljivi tudi v primeru uresničitve katere izmed groženj (Brezavšček, 2008). Ker ni primerno kopirati kar vsega, je potrebno določiti, kateri podatki in kako pogosto naj se kopirajo, katera tehnologija naj se uporablja, ter osebo, ki bo zadolžena za učinkovito izvajanje varnostnih kopij. Priporočila za hranjenje varnostnih kopij so:

- varnostne kopije naj se hranijo na oddaljeni lokaciji;
- če se hranijo na primarni lokaciji, je potrebno poskrbeti za zaščito;
- pomembni poslovni podatki naj se hranijo v vsaj treh kopijah;
- redno je potrebno kontrolirati berljivost varnostnih kopij in tudi postopke za restavriranje;
- kopiranje naj se izvaja v času manjše obremenitve sistema.

Pomemben člen v grožnjah so tudi organizacijske pomanjkljivosti, ki imajo lahko za posledico nepooblaščeno razkritje podatkov/informacij, uničenje ali popačenje dobrin in delno ali popolno nerazpoložljivost sistema. Priporočeni varnosti ukrepi so:

- dolžnosti naj bodo porazdeljene med več zaposlenimi;
- dolžnosti enakega profila naj med zaposlenimi periodično rotirajo;
- zaposlenim naj se prepreči dostop do občutljivih kombinacij podatkov/informacij;
- izdelana naj bodo navodila za varovanje osebnih podatkov v skladu z zakonom;
- izdelani naj bodo pravilniki o rokovanju z dobrinami informacijskega sistema;
- zagotovi naj se ustrezno usposabljanje zaposlenih;

- predvidene naj bodo kazni in sankcije za ravnanje, ki ogroža varnost informacijskih dobrin;
- izvaja naj se ustrezna kadrovska politika;
- izvajajo naj se postopki, ki zagotovijo uporabnikom ob prekinitvi delovnega razmerja izgubo vseh pooblastil;
- določeni naj bodo postopki za varno uničenje nosilcev občutljivih podatkov;
- organizirano naj bo redno izobraževanje in ozaveščanje zaposlenih o informacijski varnosti.

b) Logična zaščita

Pri logični zaščiti gre za varovanje neotipljivih dobrin informacijskega sistema. Uresničitev groženj ima lahko za posledico izgubo ali popačenje podatkov/informacij, delno ali celotno nerazpoložljivost sistema in uničenje ali popačenje podatkov. Med glavna področja zagotavljanja logične varnosti lahko uvrstimo (Brezavšček, 2008):

- zaščito zoper programske vsiljivce, katerih namen je sistemu povzročiti škodo (virus, črv, trojanski konj, zlonamerna prenosna koda);
- vzpostavitev učinkovite kontrole logičnega dostopa;
- mehanizme za varovanje podatkov med prenosom po omrežju.

Osnovno pravilo pri zagotavljanju zaupnosti, celovitosti in razpoložljivosti podatkov je ustrezno kontroliran dostop do podatkov (Vehar, 2012). Vzpostavitev kontrole logičnega dostopa do informacijskega sistema zahteva jasno ločevanje med subjekti in objekti informacijskega sistema. Subjekt je vsaka entiteta informacijskega sistema, ki lahko v njem izvaja kakršne koli aktivnosti. Objekt je entiteta informacijskega sistema, katere dostop je potrebno kontrolirati (Brezavšček, 2008). Kontrola dostopov do podatkov pozna štiri funkcije, s katerimi se preverja upravičenost uporabnika za dostop do določenih podatkov. Funkcije kontrole dostopov so (Brezavšček, 2008):

- identifikacija,
- avtentikacija,
- avtorizacija,
- vodenje in pregledovanje dnevnika dostopov do informacijskega sistema.

Pri dostopu do podatkov v informacijskem sistemu se mora uporabnik naprej identificirati. V večini primerov gre za uporabniško ime, ponekod se v ta namen uporabljajo pametne kartice.

V drugem koraku mora uporabnik dokazati, da je oseba, za katero se predstavlja. V tem primeru gre za avtentikacijo. Avtentikacija se izvaja tako, da se z znano referenco preverja:

- nekaj, kar uporabnik ve (geslo, pin …);
- nekaj, kar uporabnik ima (kartica, digitalni certifikat, ključ);
- nekaj, kar uporabnik je (biometrične lastnosti).

V primeru, da se uporabnik uspešno avtenticira, pridobi dostop do informacijskega sistema. Ko poskuša uporabnik dostopati do določenih podatkov, se izvede korak avtorizacije, kjer se preveri, ali ima uporabnik dostop do podatkov in kaj lahko z njimi počne. Tukaj gre za vnaprej določena pravila, ki prestavljajo nivoje dostopov in pravice za delo s podatki.

Četrti korak se izvaja v odvisnosti od nastavitev beleženja dogodkov, ki jih je nastavil skrbnik informacijskega sistema. Beležijo se tako uspešni kot neuspešni vstopi v sistem ter vse akcije, ki jih je uporabnik naredil nad podatki. Včasih je dnevnik dogodkov edina sled, če pride do neljubega dogodka, zato je potrebno dnevnik redno spremljati.

3. ZAGOTAVLJANJE VARNOSTI V RAČUNALNIŠKEM OMREŽJU

Osnova za delovanje računalniških omrežij je Open Systems Interconnection (v nadaljevanju OSI) model, saj predpisuje, kako naj bo sporočilo preneseno med dvema točkama. V nadaljevanju bomo prestavili posamezne plasti OSI modela in najpogostejše napade v računalniških omrežjih.

3.1. OSI model

OSI referenčni model je razvil ISO (International Standard Organization) leta 1984 in velja za osnovni arhitekturni model komunikacije med računalniki. OSI referenčni model določa, kako se informacija iz aplikacije na enem računalniku preko omrežja prenese v aplikacijo na drugem računalniku. Sestavljen je iz sedmih plasti. Na vsaki plasti so definirane posamezne mrežne funkcije. Vsaka plast predstavlja zaključeno celoto, kar pomeni, da se opravila na posamezni plasti izvršujejo neodvisno od drugih plasti. Slika 1 prikazuje posamezne plasti OSI modela, primere ter naprave in protokole, ki tečejo na posamezni plasti.

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols		DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP	GATEWAY	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names		
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP	Can be used on all layers	Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**		

Slika 1: 7 plasti OSI modela (http://www.escotal.com/osilayer.html, 2014)

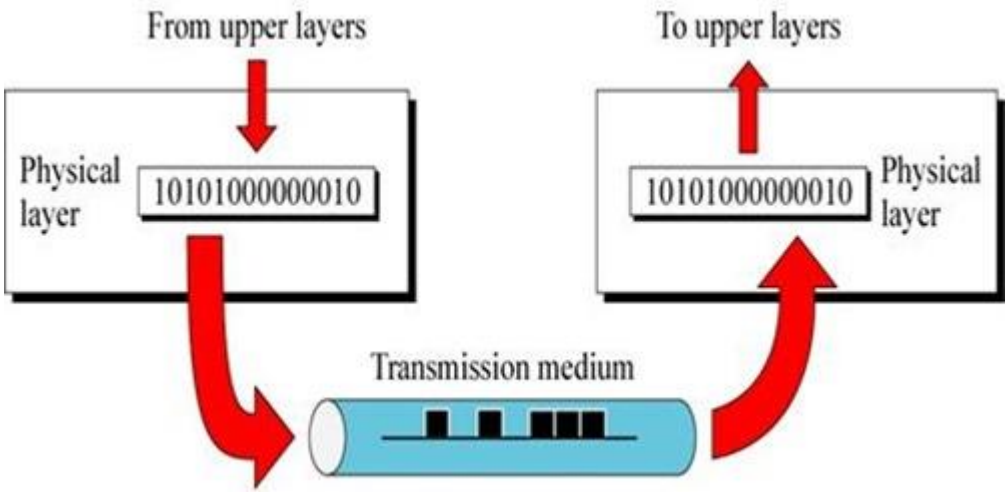
OSI model je sestavljen iz dela, ki predpisuje okvirje za razvoj standardov, in dela, ki ga tvorijo konkretni protokoli in se uporabljajo na posameznih plasteh referenčnega modela. Ti protokoli so standardizirani in omogočajo komunikacijo

računalniške opreme najrazličnejših proizvajalcev. Razdelimo jih lahko v štiri večje skupine:

- LAN protokoli so definirani na prvi in drugi plasti OSI modela in določajo komunikacijo po različnih medijih lokalnega omrežja;
- WAN protokoli so definirani na prvih treh plasteh OSI modela in določajo komunikacijo preko prostranega omrežja WAN (Wide Area Network);
- usmerjevalni protokoli omogočajo izbiro optimalne poti med usmerjevalniki;
- usmerjani protokoli so tisti protokoli, ki jih usmerjevalniki lahko usmerjajo in so definirani na 4.–7. plasti OSI modela.

3.1.1. Fizična plast

Je najnižja plast referenčnega modela OSI, ki predstavlja strojno opremo vmesnika za povezavo v omrežje. Opisuje mehanske lastnosti (kable, priključke), električne impedance, frekvence in napetosti ter procedurne karakteristike, potrebne za uporabo fizičnih medijev. Definira, kako dolg je vsak bit in kako je poslan oz. prejet. Združljivost na tem nivoju je obvezna. Sika 2 prikazuje naloge fizične plasti, ki so: prenos informacije po mediju, prevajanje analognih signalov v digitalne ter digitalnih informacij v analogne signale.



Slika 2: Naloga fizične plasti OSI modela (http://www.soopertutorials.com/technology/networks/139-open-system-interconnection-osi-model.html, 2014)

Medij na fizični plasti prestavljajo: bakreni vodniki (koaksialni kabel, utp kabel), optična vlakna, zrak ...

Protokoli, ki delujejo na fizični plasti, so: ITU-T V.92 (modem), IRDA, USB, EIA (RS-232, 422, 423, RS-449, RS-485), ETHERNET (10BASE-T, 10BASE2, 10BASE5, 100BASE-TX, 100BASE-FX, 100BASE-T, 1000BASE-T, 1000BASE-SX …), Wi-fi 802.11 različice, DSL, ISDN, T in E prenosni sistemi, SONET/SDH, OTN, Optical Transport Network), GSM, Bluetooth, IEEE 1394 vmesnik, Etherloop …

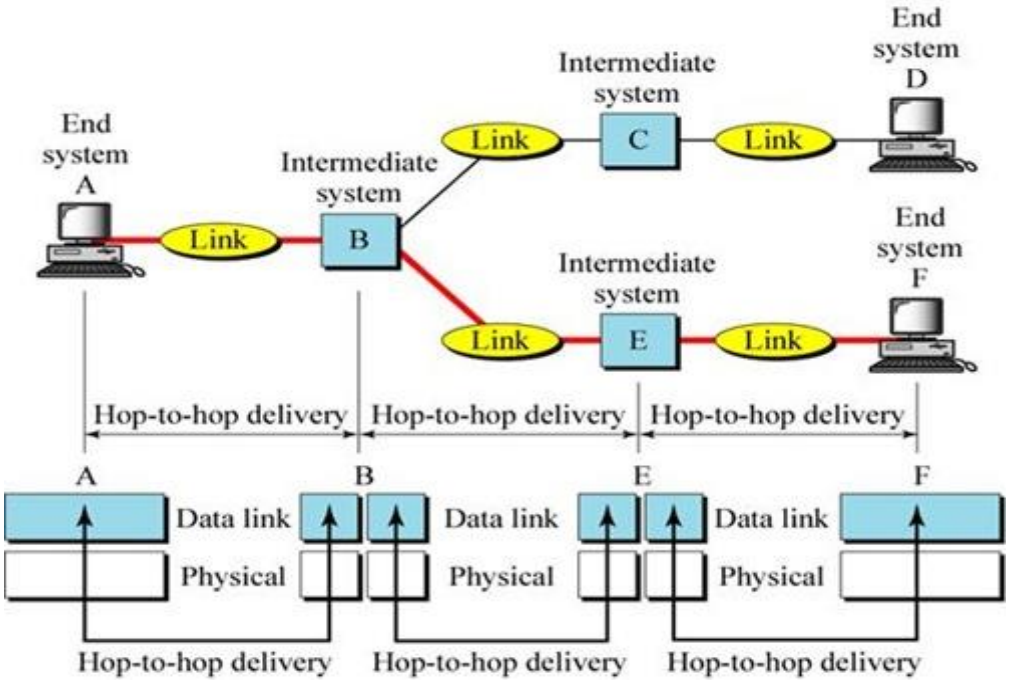
Na fizični plasti delujejo naslednje naprave: repetitor (angl. repeater), hub, modem, optični pretvornik …

Najpomembnejši vidik fizične varnosti je nadzor. Če napadalec pridobi fizični dostop do naprave, to običajno pomeni, da lahko prevzame nadzor nad delovanjem te naprave.

Obstaja veliko načinov napadov na fizično varnost (npr. kraja podatkov, nasilno odpiranje ključavnic, prisluškovanje …) (Greg, 2006). Ko napadalec enkrat spozna način varovanja, zlahka izdela načrt za napad. Večino orodij za te napade je mogoče kupiti na spletu.

3.1.2. Povezovalna plast

Določa način prenosa podatkov preko vzpostavljene povezave med dvema napravama v omrežju. Identificira bite in omejuje prenos števila bitov preko fizične plasti v standardni paket – okvir, za vsak okvir (angl. frame). Dejansko zagotavlja, da podatki zanesljivo dosežejo končno napravo. Naloga te plasti je odkrivanje napak prenosa in zagotavljanja mehanizmov za njihovo odpravo. V primeru, ko želi uporabniški program posredovati sporočilo določenemu strežniku, mora biti sporočilo opremljeno z dodatnimi podatki tako, da omrežje preko tretje plasti nedvoumno prepozna, kam naj ga pošlje. Ti dodatni podatki vsebujejo tudi informacijo, ki pomaga drugi plasti programske opreme ugotoviti napako pri prenosu. Slika 3 prikazuje omenjeno delovanje povezovalne plasti.



Slika 3: Delovanje povezovalne plasti (http://www.soopertutorials.com/technology/networks/139-open-system-interconnection-osi-model.html, 2014)

Na tej plasti delujejo naslednje naprave: stikalo (angl. switch), mostovi (angl. bridge), mrežne kartice (angl. Network interface card – NIC).
Protokoli, ki delujejo na povezovalni plasti, so: Ethernet, FDDI, PPP.

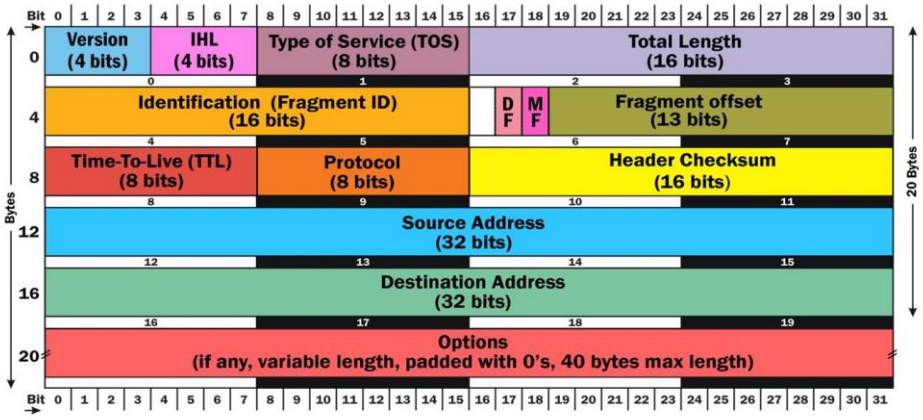
3.1.3. Omrežna plast

Skrbi za usmerjanje paketov skozi omrežja. Določa vmesnike uporabnikov omrežja, kot tudi vmesnike drugih omrežij, preko katerih podatki potujejo. Prav tako določa preklapljanje in usmerjanje ter komunikacije med omrežji (angl.: internetworking). Če mora sporočilo v drugo omrežje, določa programska oprema na tej plasti način, kako to drugo omrežje najti (usmerjevalni protokoli). Ta plast zagotavlja tudi vrstni red prenosa sporočil, kar pomeni, da bo zaporedje poslanih sporočil z ene strani na drugo sprejeto po istem vrstnem redu (fragmentacija). Zagotavlja tudi,da so prejeti paketi pravilni, saj opravlja preverjanje napak v IP glavi (angl. IP header error checking).

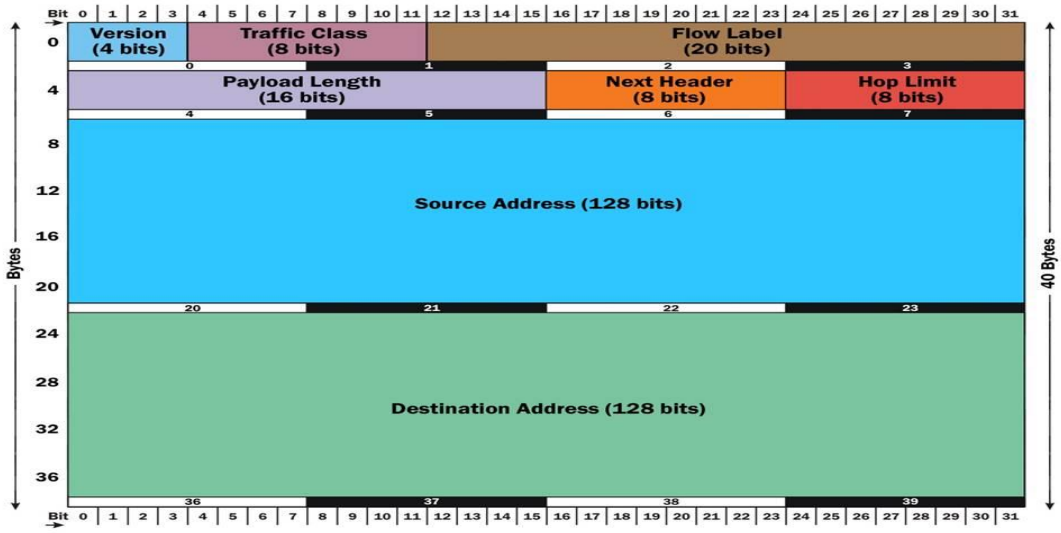
Na tej plasti delujejo naslednje naprave: usmerjevalniki in filtri paketov (angl. packet filters).

Protokoli, ki delujejo na omrežni plasti, so: IP, Ipx, DecNet, ICMP, usmerjevalni protokoli.

Slika 4 prikazuje glavo (header) IPv4 paketa. Vidimo, da je IPv4 naslov sestavljen iz 32 bitov in tako omogoča največ 2^{32} IP naslovov. Zato je bil leta 1990 sprejet standard za IPv6 protokol, kjer je dolžina naslova 128 bitov in tako na voljo 2^{128} IP naslovov. Glavo IPv6 paketa prikazuje slika 5.



*Slika 4: Glava IPv4 paketa (*http://www.sixscape.com/joomla/sixscape/index.php/ipv6-training-certification/ipv6-forum-official-certification/ipv6-forum-network-engineer-silver/network-engineer-silver-introduction/differences-between-ipv4-and-ipv6*, 2014)*



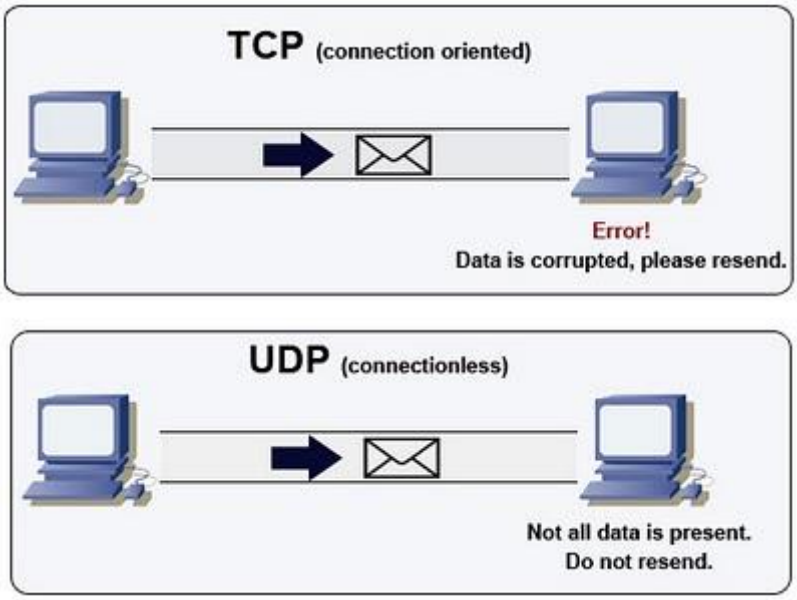
Slika 5: Glava IPv6 paketa (http://www.sixscape.com/joomla/sixscape/index.php/ipv6-training-certification/ipv6-forum-official-certification/ipv6-forum-network-engineer-silver/network-engineer-silver-introduction/differences-between-ipv4-and-ipv6, 2014)

3.1.4. Prenosna plast

Prenosna plast zagotavlja višje ležečim plastem povezavo med končnima računalnikoma. Na prenosni poti poskrbi za pravilen in zanesljiv prenos podatkov. Med drugim omogoča:

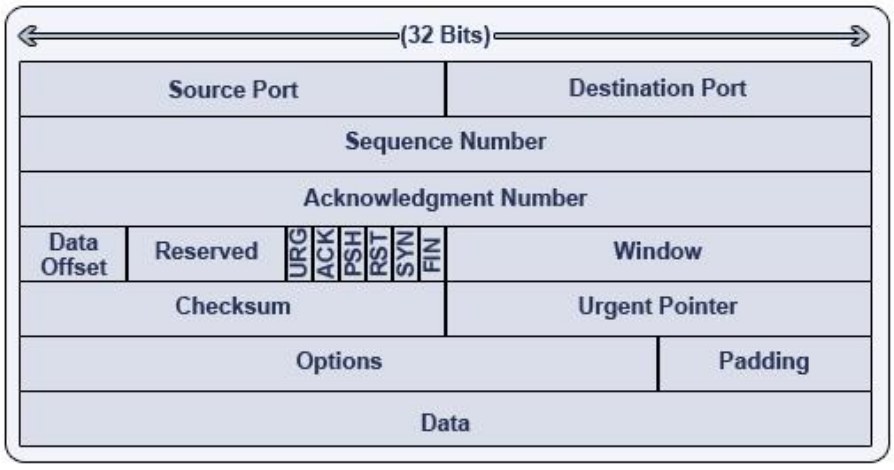
- razstavljanje dolgih sporočil na pakete (fragmentacija) ob oddajanju in sestavljanje sporočil iz paketov (defragmentacija) ob sprejemu. Pri tem je pomembna urejenost zaporedja paketov, saj lahko paketi prispejo v drugačnem vrstnem redu, kot so bili poslani;
- odkrivanje in odpravljanje napak: transportna plast odkriva napake in o tem obvesti plast, na kateri je do napake prišlo;
- vzpostavitev povezave med končnimi uporabniki;
- nadzor hitrosti pretoka podatkov tako, da določa velikost okna;
- definiranje pojma vrat.

Na prenosni plasti sta definirana protokola TCP (angl. Transmission Control Protocol), ki za prenos podatkov uporablja povezano storitev in protokol UDP (angl. User Datagram Protocol), le-ta uporablja nepovezano storitev. Primerjavo med njima prikazuje slika 6.



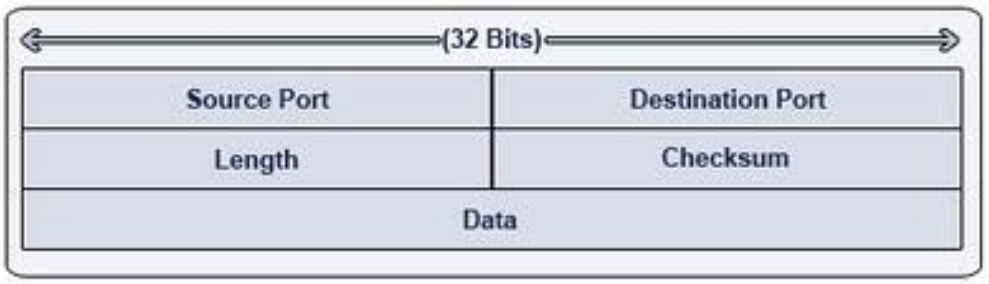
*Slika 6: Primerjava TCP in UDP protokola (*http://networkingtips-tricks.blogspot.com/2010/05/how-transport-layer-works.html, 2014*)*

Ker je TCP povezani protokol, se najprej vzpostavi povezava med odjemalcem in strežnikom. Pri povezavi so določeni odjemalčev naslov IP in vrata (vrata lahko zavzemajo vrednost od 1 do vključno 65535) ter strežnikov naslov IP in vrata, na katerih posluša storitev strežnika. Naslov IP, povezan z določenimi vrati, tvori vtičnico (angl. socket), par odjemalčeve in strežnikove vtičnice tvori povezavo TCP, ki je enolično določena. Glava (header) paketa TCP vsebuje izvorni naslov IP in vrata, ciljni naslov IP in vrata, zaporedno številko paketa, številko potrditve in kontrolne zastavice. Kontrolni zastavici, pomembni za gradnjo požarnega zidu, sta ACK in SYN. Zgradbo TCP segmenta prikazuje slika 7.



*Slika 7: TCP segment (*http://networkingtips-tricks.blogspot.com/2010/05/how-transport-layer-works.html, 2014*)*

UDP (angleško User Datagram Protocol) je nepovezani protokol za prenašanje paketov. Nepovezani pomeni, da odjemalec in strežnik ne vzpostavita povezave, ampak strežnik pošilja pakete odjemalcu in ne preverja, če je odjemalec pakete dobil. Zaradi tega včasih pravijo, da črka "U" pomeni "unreliable" (angl. nezanesljiv). Slika 8 prikazuje polja v UDP datagramu.



*Slika 8: UDP datagram (*http://networkingtips-tricks.blogspot.com/2010/05/how-transport-layer-works.html, 2014*)*

Na tej plasti deluje tudi Network Address Translation (NAT), ki skrbi za spreminjanje lokalnih IP naslovov v zunanje naslove (1 : 1) in Port Adress Translation (PAT), ki skrbi za spreminjanje lokalnih IP naslovov v enega zunanjega, ter spreminjanje izvornih/ponornih vrat.

3.1.5. Plast seje

Skrbi za logično povezovanje aplikacijskih procesov. V okviru TCP/IP arhitekture je to prepuščeno aplikacijam.

Seja pomeni potek dialoga med dvema aplikacijama.

Sejna storitvena pristopna točka (SSPT) omogoča aplikacijskim storitvam dostop do funkcij, ki omogočajo in nadzorujejo logično povezovanje aplikacijskih procesov oddajnika in sprejemnika ter dostop do komunikacijskega sistema. Sejna plast izkorišča storitve transportnega sistema, ki zagotavlja idealen prenosni kanal.

Njena naloga je:

- vzpostavitev, vzdrževanje in prekinitev seje, to je komunikacije med končnimi računalniki;
- - vrste komunikacije:
    - enosmerna (angl. simplex): na eni strani je postaja, ki oddaja sporočilo, na drugi strani ena ali več postaj, ki sporočilo sprejemajo;
    - izmenično dvosmerno (angl. half duplex): postaja lahko sprejema in oddaja podatke, vendar jih lahko istočasno samo oddaja ali samo sprejema;
    - dvosmerno (angl. full duplex): postaja lahko istočasno sprejema in oddaja podatke.

Povezava s transportnim sistemom (odnos med plastjo seje in transportno plastjo):

- vsaka sejna povezava zahteva svojo transportno povezavo, kar pomeni, da po eni transportni povezavi ne moremo vzpostaviti več aplikacijskih dialogov – sej;
- dovoljene so prekinitve ene ali druge povezave (prekine se lahko samo ena);
- multipleksiranje povezav se lahko izvede le na nižjih plasteh (običajno med transportno in omrežno).

Protokoli, ki jih se nahajajo na tej plasti, so:

- Network File System (NFS),
- Structured Query Language (SQL),
- Remote-Procedure Call (RPC),
- X Window System,
- Apple Talk Session Protocol (ASP),
- DNA Session Control Protocol (SCP),
- Real Time Transport Protocol (RTP),
- Session Initiation Protocol (SIP),
- protokoli za avtentikacijo.

3.1.6. Predstavitvena plast

Predstavitvena plast pretvarja podatke med aplikacijsko plastjo in formatom omrežja. Podatki so lahko poslani v različnih formatih preko različnih virov. Tako je predstavitvena plast odgovorna za integracijo vseh formatov v standardno obliko za učinkovito in uspešno komunikacijo.

Predstavitvena plast sledi strukturi podatkovnih programskih shem, razvitih za različne jezike, in v realnem času zagotavlja skladnost, potrebno za komunikacijo med dvema objektoma, kot so plasti, sistemi in omrežja. Format podatkov mora biti sprejemljiv za sosednje plasti, v nasprotnem primeru predstavitvena plast svoje funkcije ne opravlja pravilno (Technopedia, 2014).

Predstavitvena plast je odgovorna za:

- združljivost predstavitve podatkovnih tipov – različno kodirani podatki med seboj niso združljivi in jih je zato treba prevesti v ustrezno obliko;
- združljivost imenovanih kodnih strani – združljivost predstavitve alfanumeričnih znakov (ASCII, EBCDIC);
- stiskanje podatkov (kompresija) – če je kapaciteta transportnega sistema prenizka;
- zaščito vsebine sporočila (enkripcija, dekripcija) – zagotavljanje varnosti poslovanja.

Algoritmi za stiskanje podatkov se delijo na: reverzibilne in nereverzibilne (iz stisnjenih podatkov ni mogoče več rekonstruirati izvornih podatkov).

Na predstavitveni plasti ni posebnih protokolov, vendar naj bi vsi protokoli, ki delujejo na aplikacijski plasti, delovali na vseh zgornjih treh plasteh (seje, predstavitvena, aplikacijska) (Firewall.cx, 2014).

3.1.7. Aplikacijska plast

Pošilja in prevzema toke podatkov od oz. do transportne plasti. Je edina plast, s katero ima uporabnik neposreden stik.

Funkcije aplikacijske plasti določajo storitve, ki jih komunikacijski sistem nudi uporabniku. Najpogostejše storitve so:

- prepoznava komunikacijskega partnerja po imenu ali naslovu;
- določanje trenutne zmožnosti partnerja, ki želi komunicirati;
- vzpostavitev nadzora nad komuniciranjem;
- dogovarjanje o šifrirnih mehanizmih;
- izbiranje vrste dialoga, vključno s postopki njegove vzpostavitve in prekinitve;
- dogovor o odgovornosti za odpravljanje napak;
- prepoznava zahtev pri sintaksi podatkov (znakovni kod, sestavo podatkov in podobno).

Najbolj uporabljeni protokoli aplikacijske plasti so:

- HTTP (Hypertext Transfer Protocol),
- TLS/SSL (Transport Layer Security / Secure Sockets Layer),
- DNS (Domain Name System),
- SMTP (Simple Mail Transfer Protocol),
- POP (Post Office Protocol),
- IMAP (Internet Message Access Protocol),
- NTP (Network Time Protocol),
- Telnet,
- SSH (Secure Shell),
- FTP (File Transfer Protocol),
- SNMP (Simple Network Management Protocol),
- DHCP (Dynamic Host Configuration Protocol).

3.2. Vloga človeka pri zagotavljanju varnosti v računalniškem omrežju

Kakor smo že zapisali, je človek pogosto najšibkejši člen verige. Na spodnjih plasteh OSI modela lahko izvedemo najboljše varnostne rešitve, vendar smo še vedno ranljivi preko zaposlenih.

Že v prejšnjih poglavjih smo ugotovili, da je lahko varnost kršena z izkoriščanjem pomanjkljivosti in slabosti protokolov ter njihovih izvedb na vsaki plasti modela OSI. Obnašanje strojne in programske opreme je ponovljivo. Naprava ali program bo v določenem stanju in z določenim vhodom deloval povsem na enak način, kot

je v preteklosti pod istimi pogoji. Odkrivanje pogojev, ki predstavljajo izpostavljenost varnosti, je v domeni hekerjev.

Seveda ljudje nismo tako procesno programirani in predvidljivi kot stroji, saj se ob istih pogojih ne obnašamo enako. Nekateri ljudje namreč nočejo spoštovati varnostna pravila, medtem ko jih drugi celo kršijo in s tem omogočajo hekerjem, da odkrijejo varnostne pomanjkljivosti.

"Črno-klobučni" heker (black-hat hacker) napada računalnike, ker so v njih shranjeni podatki podjetja. Vendar, ali so lahko takšne informacije dostopne tudi drugje, kjer ni zaščite? Da, v ljudeh. Približno 80 % znanja podjetja naj bi bilo v ljudeh (Greeg, 2006). Ljudje so pomembni, ker:

- so zakladnica informacij,
- so lažje tarče kot računalniki.

Obstaja stereotip, ki pravi, da imajo tehnično podkovani napadalci slabe človeške spretnosti (angl. people skills), vendar to ne velja vedno. Eden najbolj poznanih je Kevin Mitnick. Mitnick je tehnično podkovan, vendar je njegovo tehnično znanje nadgrajeno s spretnostjo manipulacije z ljudmi. Nekaterim se zdijo anonimni napadi na računalnike varni, vendar socialni inženir lažje dobi podatke, ki jih želi, od ljudi.

Podjetja niso edine tarče napadov zaradi pridobivanja informacij. Tatovi identitet zberejo dovolj informacij o neki osebi, da se lahko izdajajo zanj z namenom zlorabe njegove kreditne kartice ali celo naročila nove kreditne kartice ali kredita v njegovem imenu. Kraja identitete se izvaja tako "online" kot "offline".

3.3. Najpogostejši napadi na računalniška omrežja

V nadaljevanju bomo prikazali najpogostejše vrste napadov, ki se dogajajo v računalniških omrežjih.

3.3.1. Kraja podatkov

Med najlažje izvedljive napade spadajo notranji napadi na fizični plasti, saj napadalec že ima dostop do sistema. Ti napadi so postali lažje izvedljivi zaradi izboljšav v elektroniki, ki omogoča težje odkrivanje vohunjenja, prestrezanja in kraje informacij.

Greeg (2006) navaja primer podjetja Sony, katero je na vsako zgoščenko namestilo vohunski program, ki se je namestil na računalnik v primeru kopiranja skladb. Program je zbiral podatke o pesmih in zgoščenkah, ki jih je uporabnik poslušal, ter jih pošiljal podjetju Sony. To je osnovni napad na fizični plasti, medtem ko program, ki se izvaja, teče na aplikacijski plasti.

Druga možnost je kraja podatkov preko USB. Za izvedbo kraje je dovolj že npr. navaden mp3 predvajalnik z možnostjo priklopa preko USB vmesnika. Vse, kar

mora uporabnik storiti, je, priklopiti predvajalnik na USB in prenesti želene datoteke.

V ta namen so bili spisani tudi programi, ki se ob priklopu naprave samodejno zaženejo in poiščejo ter prenesejo želene datoteke, med njimi tudi podatke o uporabniških računih na sistemu (Greeg, 2006).

3.3.2. Napadi na strojno opremo

Ko ima napadalec enkrat fizični dostop do opreme, lahko vpliva na njeno delovanje. Npr. na omrežje namesti razdelilnik (Hub), s pomočjo katerega lahko potem na višjih plasteh prestreza promet.

Poleg samih napadov na varnost vplivajo tudi odpoved strojne opreme in prekinitev napajanja strojne opreme.

3.3.3. Prisluškovanje

Napad se izvaja tako na fizični kot na povezovalni plasti. Na fizični plasti gre za prestrezanje npr. glasovnih klicev s strani nepooblaščene osebe. Kazenski zakonik RS obravnava tovrstno dejanje kot kaznivo, kar je zapisano tudi v 137. členu omenjenega zakonika (Uradni list, 2004):

(1) Kdor neupravičeno s posebnimi napravami prisluškuje pogovoru ali izjavi, ki mu nista namenjeni, ali ju zvočno snema ali kdor takšen pogovor ali takšno izjavo neposredno prenaša tretji osebi ali ji takšen posnetek predvaja ali kako drugače omogoči, da se z njim neposredno seznani, se kaznuje z denarno kaznijo ali z zaporom do enega leta.

(2) Enako se kaznuje, kdor zvočno snema njemu namenjeno zaupno izjavo drugega brez njegove privolitve z namenom, da bi takšno izjavo zlorabil, ali kdor takšno izjavo neposredno prenaša tretji osebi ali ji takšen posnetek predvaja ali ji kako drugače omogoči, da se z njim neposredno seznani.

Načini prisluškovanja na fizični plasti so (Greeg, 2006):

- priklop na telefonsko linijo,
- namestitev prisluškovalne tuljave (coil-tap).

Na povezovalni plasti gre za posledico fizičnega dostopa do opreme. Osnova za veliko število omrežnih napadov je pasivno prisluškovanje (passive sniffing). Običajno mrežne kartice procesirajo pakete, ki so poslani na fizični (v nadaljevanju MAC) naslov mrežne kartice ali naslov za razpršeno oddajanje (v nadaljevanju broadcast naslov). V primeru, da so v omrežju razdelilniki (v nadaljevanju hub), mrežna kartica prejme veliko več paketov in ne samo tiste, ki so namenjene sistemu s to mrežno kartico. Za pasivno prisluškovanje se uporablja program za spremljanje paketov (npr. Wireshark ali tcpdump).

Pasivno prisluškovanje temelji na t. i. promiskuitetnem (angl. promiscuous) načinu mrežne kartice. V tem načinu mrežna kartica posreduje proti operacijskemu sistemu vse pakete in ne samo tiste, ki so namenjeni sistemu. Ta verzija prisluškovanja se je uporabljala v omrežjih s hubi, ker je danes tega vedno manj, pride v poštev aktivno prisluškovanje (angl. active sniffing) (Greeg, 2006).

Aktivno prisluškovanje temelji na vstavljanju (angl. injection) paketov v omrežje, kar povzroči, da je promet, ki naj ne bi bil poslan na naš sistem, poslan na naš sistem. Aktivno prisluškovanje je potrebno, da se obide delitev, ki jo izvajajo stikala (switch). Stikala shranijo svojo ARP (angl. Address Resolution Protocol) tabelo v posebnem delu pomnilnika imenovanega CAM (angl. Content Addressable Mermory), kjer spremljajo, kateri gostitelji (angl. host) so priklopljeni na kateri vmesnik na stikalu (Greeg, 2006).

3.3.4. Napad onemogočanja

Napad onemogočanja (v nadaljevanju DoS) je napad, ki so ga razvili hekerji okoli leta 2000, svoj razcvet je doživel leta 2002, ko so hekerji onesposobili strežnike kot so Amazon.com in Download.com za nekaj ur. Heker pošlje tarči veliko količino podatkov določenega protokola (včasih samo na določena vrata). Heker običajno uporablja protokole UDP, TCP, ICMP, SYN ipd. Po navadi so prvi znaki DoS napada upočasnjeno delovanje računalnika in interneta, rezultati so odklop (angl. disconnect) in včasih tudi samodejen ponoven zagon računalnika (DoS.Wikipedija, 2014). Nadgradnja DoS napadov je distribuiran napad onemogočanja (DDoS), kjer napadalec za napad uporabi več okuženih računalnikov (bot), nad katerimi ima nadzor.

Spodaj je navedenih nekaj DoS napadov na posamezni plasti, od katerih jih bo nekaj opisanih v nadaljevanju (us-cert, 2014):

- na fizični plasti gre lahko za uničenje, obstrukcijo, manipulacijo ali nepravilno delovanje opreme; posledica je, da bo oprema postala neodzivna in bo potrebno izvesti popravilo za povečanje razpoložljivosti;
- na povezovalni plasti se izvaja MAC poplavljanje;
- na omrežni plasti se lahko izvaja ICMP napad;
- na transportni plasti se izvajajo SYN napadi;
- na plasti seje lahko napadalec izkoristi ranljivost Telnet programske opreme na stikalu, kar povzroči nedosegljivost Telnet storitve in posledično onemogoči skrbniku upravljanje stikala;
- na predstavitveni plasti lahko napadalec pošilja popačene (angl. malformed) SSL zahtevke, ki lahko povzročijo, da sistem preneha sprejemati SSL zahtevke ali se ponovno zažene.

3.3.5. ARP napadi

V nadaljevanju bo prestavljenih nekaj ARP napadov, ki se izvajajo na povezovalni plasti.

a) ARP zastrupljanje (angl. ARP poisoning)

Najenostavnejši napad, pri katerem razprševanje ponarejenih paketov ARP prelisiči odjemalce v omrežju. Napadalec preslika svoj MAC naslov v logični naslov (IP naslov) žrtve. Napad je trivialen, saj ARP ne zahteva prijave in slepo odgovarja na vse pakete "ARP-Request". ARP zastrupljanje je eden izmed načinov za izvedbo napada s posrednikom (v nadaljevanju MITM), saj napadalec prepriča žrtev, da je privzeti prehod in tako ves promet v internet poteka čez napadalčev računalnik (Greeg, 2006).

b) ARP/MAC poplavljanje (angl. ARP/MAC flooding)

Napadalec pošlje ogromno okvirjev (angl. frames) z naključnim izvornim MAC in IP naslovom. S tem doseže, da se CAM tabela stikala zapolni in stikalo prične pošiljati promet na vse vmesnike, ki so v istem VLAN-u (angl. Virtual LAN). Prav tako se zapolni CAM tabela sosednjih stikal (Greeg, 2006).

c) ARP sleparjenje (angl. ARP spoofing)

Pri tem napadu gre za povezavo napadalčevega strojnega naslova z enim izmed IP naslovov legitimnega sistema v omrežju. S tem napadalec doseže, da ves promet poteka preko njega. Omogoča izvedbo DoS napadov, kjer več IP naslovov povežejo s fizičnim naslovom legitimnega strežnika, s tem dosežejo, da strežnik dobi preveč prometa, ki ga ne more obdelati (Greeg, 2006).

3.3.6. Preskakovanje med VLAN-i (angl. VLAN hopping)

Namen preskakovanja med VLAN-ni je pridobiti, z napadom gostitelja v nekem VLAN-u, dostop do prometa v drugih VLAN-ih. Napadi se izvajajo na povezovalni plasti OSI modela. Vmesniki na stikalu lahko delujejo v 2 načinih:

- Access/Untagged – prepuščajo samo en VLAN;
- Trunking/Tagged (802.1Q standard) – prepušča enega ali več VLAN-ov.

Če napadalec prepriča stikalo, da vmesnik, na katerega je priključen, spremeni v "trunk" način, lahko prisluškuje prometu na vseh VLAN-ih. Takšen napad se lahko uporabi npr. za krajo uporabniških računov, ki jih lahko uporabi v kasnejših napadih.

3.3.7. Napad na telefonski (angl. Voice) VLAN

Telefonija je v praksi v svojem VLAN-u, ki je označen (angl. tagged). Vmesnik na stikalu pošilja za telefonski VLAN označene pakete, za podatkovni VLAN pa neoznačene. Napadalec iz računalnika pošlje telefonu označen paket. Promet iz računalnika je tako sedaj v telefonskem VLAN-u. Tudi ta napad se izvaja na povezovalni plasti.

3.3.8. DHCP napadi

DHCP (Dynamic Host Configuration Protocol) je omrežni protokol za dinamično nastavitev gostitelja. Narejen je bil z namenom, da omogoči individualnim računalnikom v omrežju, da pridobijo svoje omrežne nastavitve od strežnika (primer je IP naslov in prehod). Namen uporabe DHCP protokola je olajšanje upravljanja omrežja. Glede na to, da DHCP protokol deluje na povezovalni plasti OSI modela, se tudi napadi izvajajo na tej plasti.

Obstajata 2 načina napada:

a) **DHCP stradanje** (angl. DHCP starvation) – deluje s pošiljanjem DHCP zahtevkov s ponarejenim izvornim naslovom. Če napadalec pošlje dovolj zahtevkov, lahko začasno doseže, da DHCP strežnik dodeli vse IP naslove, ki jih ima na voljo. Tako lahko v tem času postavi lažni strežnik, ki odgovarja na zahtevke v omrežju.
Stradanje DHCP je tudi v verziji IPv6 ostalo tveganje, čeprav je na voljo velika količina naslovnega prostora. Ravno to lahko privede do preobremenitve strežnika, saj mora za vsak dodeljen naslov voditi evidenco.

b) **Lažni DHCP strežnik** – lahko ga nevede postavi uporabnik (npr. domači usmerjevalnik) ali napadalec, katerega namen je izvesti MITM napad ali prisluškovanje. V tem napadu namreč napadalec pošlje svoj privzeti prehod in DNS strežnik. Podobno velja tudi za DHCPv6.

3.3.9. Napadi na brezžična omrežja

Danes se pojavlja ogromno brezžičnih omrežij, kar močno olajša in pohitri izgradnjo lokalnega omrežja, saj moramo priklopiti le brezžični usmerjevalnik ali dostopno točko in že imamo zgrajeno lokalno omrežje. Vendar se pozablja na zaščito teh omrežij. Z raznimi prosto dostopnimi programi (npr. Kismet) je možno enostavno prisluškovati nezavarovanim brezžičnim omrežjem.

Tudi če imamo brezžično omrežje zavarovano z ustreznim varnostnim protokolom, smo lahko ranljivi. WEP (Wired Equivalent Privacy) protokol je dokaj enostavno razbiti, saj na vsakih 5000 paketov lahko dobimo znak ali dva ključa. Če napadalec dovolj časa vztraja, lahko razkrije ključ in posledično dešifrira ves promet. Vendar tudi trenutno najmočnejši varnosti pokol za brezžična omrežja, WPA2-PSK (Wi-Fi Protected Access 2 – Pre Shared Key), ni neranljiv. Za to so odgovorni predvsem uporabniki, ki imajo nastavljen šibki PSK in/ali privzeto ime omrežja (v nadaljevanju SSID).

Brezžični telefoni, mobilni telefoni in brezžična omrežna oprema so potencialna nevarnost za podjetja. Za razliko od prisluškovanja, kjer napadalci za namestitev naprave za prisluškovanje potrebujejo fizični dostop, mora biti v tem primeru napadalec samo v dosegu signala.

Čeprav naj bi GSM telefoni veljali za varne, sta leta 2010 Chris Paget in Karten Nohl na konferenci 26CS3 prikazala, kako jim prisluškovati. Sam šifrirni algoritem,

znan pod imenom A5/1, je neodvisnim in akademskim raziskovalcem z razmeroma poceni opremo uspelo razbiti že leta 1999 (Cerar, 2014).

V nadaljevanju bo prikazano nekaj napadov na brezžična omrežja.

Napade na brezžična omrežja lahko v grobem razdelimo na 4 osnovne kategorije (Greeg, 2006):

- prisluškovanje (angl. eavesdropping),
- odprta omrežja (angl. Open Authentication),
- prestrezne dostopne točke (angl. Rogle Access Point),
- napad za zavrnitev storitve (angl. DoS − Denail of Service).

a) Prisluškovanje

V primeru uporabe aplikacij in protokolov, ki ne šifrirajo prometa, so podatki poslani v tekstovni obliki in jih je enostavno prestreči. Najpogostejši so: File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) in Hypertext Transfer Protocol (HTTP).

b) Odprta omrežja

Napadalec se lahko brez težav prijavi na omrežje organizacije, saj dostopne točke ne zahtevajo prijave.

c) Prestrezne dostopne točke

Gre za MITM napad, kjer napadalci postavijo svoje točke v isti prostor, kot so že legitimne točke, in s prijavo uporabnika enostavno prestrezajo ves promet.

d) Napad za zavrnitev storitve

Brezžična omrežja delujejo na enakih frekvencah kot npr. mikrovalovne pečice, brezžični telefoni in je tako možno enostavno motiti signal.

3.3.10. Napadi na IPv4 protokol

IP protokol deluje na omrežni plasti OSI modela, zato se tudi napadi izvajajo na tej plasti.

V nadaljevanju bomo predstavili nekaj najpogostejših napadov na IPv4 protokol.

a) Sleparjenje (angl. spoofing) − Ti napadi so danes v omrežjih IP pogosti. Bistvo pri sleparjenju je spreminjanje izvornega IP naslova ter številke vrat, kar pripomore k anonimnosti napadalca. Ta želi promet prikazati, kot da prihaja z drugega naslova oz. druge aplikacije.

S tovrstnimi napadi dosežejo težjo sledljivost napadov z onemogočanjem izvajanja storitve (DoS), raznimi virusi in črvi. Cilj prirejanja naslova je skrivanje identitete napadalca, ki bi sicer lahko bila zabeležena v dnevniški datoteki (angl. Log File). S tem se izognemo tudi sprejemanju povratnega

prometa s strani žrtve. Takemu napadu bi se zlahka izognili, če bi internetni ponudniki preprečevali promet iz IP naslovov, ki niso v njihovem omrežju.

b) **Fragmentacija (angl. Fragmentation) –** Fragmentacija je postopek razbijanja IP paketov v pakete manjšega velikostnega ranga. Postopek se izvaja zaradi omejitve "maximum transmission unit" (v nadaljevanju MTU), katera določa največjo velikost paketa, ki ga prepuščajo usmerjevalniki na poti do ponora. Tam se fragmenti ponovno združijo. S to metodo se pri verziji IPv4 lahko določa oz. prilagaja MTU velikost paketa vsakega vozlišča. Potrebe po fragmentiranju paketa na poti po IPv4 omrežjih so prizadele predvsem hrbtenične usmerjevalnike. Od njih se zahteva zagotavljanje čim višje propustnosti, ki jo delno omejuje tudi proces fragmentacije s porabo sistemskih sredstev.

Pri IPv6 so z eliminacijo postopka fragmentacije in ponovnega sestavljanja (razen pri izvornem gostitelju) povečane zmogljivosti omrežnih usmerjevalnikov. V okolju IPv6 je fragmentacija na izvoru prilagojena zmogljivosti prenosne poti, po kateri se prenašajo paketi.

Napad se izvaja z namenom, da se zaobide varnostno politiko požarnih zidov. Podatke se dostavi na vrata (angl. port), ki jih sicer požarni zid blokira. Bistvo je v manipulaciji vrednosti polja odmik (angl. fragment offset), ki je del glave fragmenta in določa položaj fragmenta glede na originalni IP paket. V primeru razbitja paketa na dva dela lahko drugemu vrednost dodelimo tako nizko, da namesto združevanja na ciljni strani povozi podatke in del TCP glave predhodnega fragmenta.

IPv6 protokol fragmentacije na poti ne dovoljuje – ta je možna samo pri izvoru podatkov. MTU možnost v ICMPv6 omogoča določanje priporočljive velikosti fragmentov preko sporočil Router Advertisement. Minimalna priporočena velikost znaša 1280 oktetov. Vse kar je manj, se zavrže, razen v primeru, da je paket zadnji v toku podatkov.

c) **Pasivni prstni odtis (angl. Passive Fingerprinting) –** uporabna posebnost IP, TCP, UDP in ICMP za ugotavljanje tipa operacijskega sistema (OS). Za napade se uporabljajo štiri polja znotraj TCP in IP glave (TTL value, DF, TS, Window size).

d) **Skeniranje vrat (angl. Port Scanning)** – preverja se, katera vrata so odprta na sistemu, kar je poleg verzije OS napadalcu podaja dodatne informacije za izvedbo napada.

e) **ICMP napadi**
ICMP kontrolna sporočila se uporabljajo za diagnostiko logičnih napak in omrežja. ICMP ne ponuja avtentikacije in je zaupanja vreden protokol. Napadalci ga uporabljajo za skeniranje in ukane (angl. exlploit) naprav.

Kakor že omenjeno, deluje ICMP na omrežni plasti, kjer se napadi tudi izvajajo.

ICMP zlorabe sistemov so:

- stranska vrata (angl. backdoor) – s pomočjo raznih brezplačnih programov je omogočeno ICMP paketu dodati svoje podatke, ki so videti kot običajen "ping";
- echo napadi – napadalec pošlje poneverjen "ping" paket na "broadcast" naslov, kot izvorni naslov pa je naveden žrtvin naslov. Tako vsi sistemi, ki ne blokirajo "ping", žrtvi pošiljajo "echo" odgovor (v nadaljevanju replay) in porabijo vso pasovno širino;
- skeniranje vrat – napadalec lahko s pomočjo raznih brezplačnih programov (npr. nmap) s pingom preverja, katera vrata so odprta. V echo replay paketku lahko vidimo, ali so neka vrata zaprta ali odprta (Type:3, Code:3);
- preusmeritev prometa;
- prstni odtis OS sistema – napadalec s pomočjo informacije, kateri OS je na žrtvinemu sistemu, ve, katere storitve naj bi tekle na tem strežniku in katere varnostne luknje obstajajo za njih;
- DoS.

3.3.11. Napadi na IPv6 protokol

IPv6 je protokol omrežne plasti, namenjen naslavljanju naprav v omrežju. Je naslednik protokola IPv4 – danes najbolj razširjenega komunikacijskega protokola, ki omogoča delovanje interneta in med seboj povezuje omrežja in naprave. IPv6 v primerjavi z IPv4 omogoča dodatne funkcionalnosti, hkrati pa vsebuje večino funkcionalnosti, ki so bile pri IPv4 razvite v obliki dodatnih protokolov.

V nadaljevanju bomo predstavili nekaj napadov, ki se uporabljajo za zlorabo IPv6 protokola.

a) Napad na IPv6 protokol za raziskovanje soseščine (angl. Neighbor Discovery Protocol)

"Neighbor Discovery Protocol" je nadomestilo za protokole ARP, "ICMP router discover" in ICMP preusmeritvena sporočila iz IPv4. Omogoča razreševanje med-sosedskih odnosov naprav v omrežju. Naprave se na ta način lahko samodejno konfigurirajo, razrešujejo naslove ali iščejo usmerjevalnike. Za komunikacijo se uporablja ICMPv6. ICMP napadi se podobno kot DHCP napadi izvajajo na povezovalni plasti.

"Neighbor Discovery Protocol" (v nadaljevanju NDP) definira 5 tipov sporočil in posledično napade na njih:

- NS – "Neighbor Solicitation" – pošljemo vozlišču v omrežju za ugotavljanje naslovov sosedov in ugotavljanje dosegljivosti IP naslova. Uporablja se tudi za ugotavljanje podvojenih IP naslovov;
- NA – "Neighbor Advertisement" – poslano kot odgovor na NS. Uporablja se tudi za oznanitev spremenjenih naslovov. NS in NA sporočila se izmenjujejo za tvorjenje parov IP naslov – fizični naslov;
- RS – "Router Solicitation" – uporabi se kot zahtevek, da usmerjevalnik pošlje sporočilo tipa RA;

- RA − "Router Advertisement" − usmerjevalniki naznanijo svojo prisotnost in sporočijo parametre, kot so nastavitev omrežne predpone, omejitev skokov …;
- "Redirect" – usmerjevalniki ga uporabljajo za obveščanje gostitelja, da obstaja boljši izbor poti za doseganje ciljnega naslova.

V primeru, da se napadalcu uspe priklopiti v omrežje, lahko s pošiljanjem zlonamernih in odvečnih sporočil doseže:

- gostitelji ga privzamejo kot privzeti usmerjevalnik;
- z oglaševanjem izmišljene predpone omrežja lahko doseže, da paketi nikoli ne dosežejo cilja;
- onemogoči možnost avtomatskega pridobivanja parametrov omrežja (Stateless Address Autoconfiguration − SLACC);
- z dovolj nizko vrednostjo HOP parametra povzroči, da se usmerjanje paketa predčasno konča;
- z dovolj hitrim skeniranjem omrežja doseže, da se zapolni tabela sosedov, ki jo vodi usmerjevalnik ali gostitelj (DoS). Pri IPv6 veljajo priporočila, da je v enem podomrežju na voljo 2^{64} IP naslovov.

b) IPv6 "multicast"

Preko oddajanja sporočil večim prejemnikom (v nadaljevanju multicast), lahko napadalec dokaj hitro izvede napad s poizvedovanjem na lokalno omrežje. Preprosto izvede "ping" na "multicast" naslov FF02 ::1, ki vrne naslove vseh dosegljivih naprav. Poleg tega lahko s pomočjo skript programa *nmap* razkrije skoraj vse naprave v IPv6 omrežju in jih "prisili", da preko Stateless Autoconfiguration (SLAAC) ustvarijo nove (začasne) IPv6 naslove. Ustrezna "multicast Listener Discovery" sporočila od žrtev, ki so poslana preko multicasta, razkrijejo oznako (ID) svojega vmesnika.

c) ICMPv6 napadi

ICMPv6 igra ključno vlogo pri pravilni uporabi IPv6 protokola. Za enostavno uporabo IPv6 protokola so potrebna predvsem sporočila za odkrivanje soseda (angl. Neighbor Discovery), kot so oglaševanje usmerjevalnika (angl. Router Advertisements − RAS) in povpraševanje/oglaševanje sosedov (angl. Neighbor Solicitation/Advertisements − NS/NA).

1) Poneverjanje Router Advertisement sporočila (angl. Router Advertisement Spoofing)

Kadar napadalec pošlje poneverjeno Router Advertisement sporočilo znotraj podomrežja, bodo vsa IPv6 vozlišča takoj spremenila svoje usmerjevalne tabele in shranile napadalca kot enega od privzetih usmerjevalnikov. Če bodo poslali promet proti internetu, se bo uporabljal novi privzeti usmerjevalnik. To vodi do situacije, v katerih lahko napadalec v celoti vidi (in celo spremeni) ves odhodni promet iz vozlišč IPv6 do interneta, to je MITM napad.

2) Poplava Router Advertisement sporočil (angl. Router Advertisement Flooding)

Napadalec lahko pošlje tudi več tisoč RAS sporočil, ki takoj onemogočijo vse računalnike Microsoft Windows, saj so popolnoma preobremenjeni z veliko količino SLAAC procesov. Ta hrošč je znan že več let, vendar ga še vedno izkoriščajo. To pomeni: če ima napadalec dostop do lokalnega omrežja in stikalo ne preprečuje pošiljanja poneverjenih RAS sporočil, bodo vsa Windows okolja postala neodzivna.

3) Poneverjanje "Neighbour Discovery" sporočil (angl. Neighbour Discovery Spoofing)

Kadar napadalec ponaredi nekatera "Neighbor Discovery" sporočila, lahko izvrši MITM napad. S poneverjenimi "Neighbour Discovery" sporočili kot odgovor na "Neighbour Solicitation" sporočila od žrtev, preusmeri ves IPv6 promet preko svoje usmerjevalne instance v isto podomrežje.

4) Zaznavanje podvojenih naslovov (angl. Duplicate Address Detection)

DoS napad je izveden, če napadalec odgovori na vsa sporočila "Duplicate Address Detection" (DAD) iz novega IPv6 vozlišča (IPv6 naslov še ni dodeljen).Vozlišče vedno verjame, da je ta naslov že v uporabi in tako nikoli ne bo dobil prostega IPv6 naslova. Posledično ne bo mogel dostopati do omrežja. IPv6 naslov lahko pridobi šele, ko napadalec ustavi napad.

3.3.12. Napadi na usmerjevalnik in usmerjanje

Usmerjanje igra pomembno vlogo na omrežni plasti OSI modela, saj omogoča povezavo lokalnega omrežja z zunanjim. Na tej plasti najdemo 2 usmerjevalna protokola (IGMP in OSPF), medtem ko se drugi nahajajo na aplikacijski plasti. Napade lahko razdelimo v dve kategoriji (Greeg, 2006):

- hit-and-run napadi – težko jih je zaznati in izolirati. Napadalec vstavi enega ali več slabih paketov in povzroči trajne škodljive učinke;
- vztrajne (angl. persistent) napade – napadalec mora neprestano ustavljati škodljive pakete, da bi povzročil občutno škodo.

Pri usmerjanju prometa se uporablja tudi usmerjanje glede na izvorni naslov. Napadalec lahko to izkoristi na način, da pošlje poneverjen paket z legitimnim izvornim IP naslovom. Izvorno usmerjanje usmeri na svoj naslov in pošlje paket žrtvi. Ker žrtev misli, da je paket prišel iz legitimnega sistema, ga sprejme. Tako se ves promet pošilja napadalcu in nikoli ne doseže legitimnega cilja.

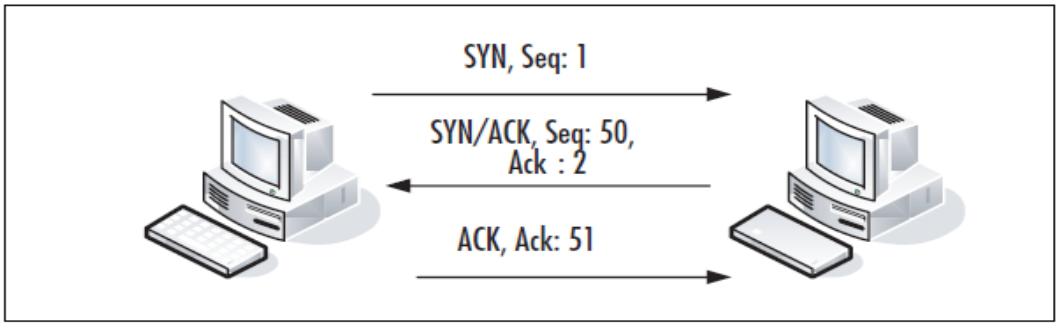
3.3.13. SYN napad

Z uporabo legitimnih TCP funkcij lahko napadalec, ki upravlja z majhnim številom gostiteljev, kontrolira in izvaja DoS napade, ki lahko popolnoma zasedejo pasovno širino organizacije, drugače obremenijo ali zasedejo vire tarče (npr. porabi razpoložljiva vrata na strežniku, zato ta postane nedosegljiv).

V 3-stranskem rokovanju (angl. three-way handshake), ki ga prikazuje slika 9, so na strani odjemalca izbrana izvorna vrata (angl. Source Port) za novo povezavo, ki je odprta na določena vrata na strežniku. Pri multipleksiranju TCP povezav spletni brskalnik odpre več povezav na spletni strežnik, da hitreje prikaže slike na spletni strani. Vendar več odprtih sej močno obremeni tako strežnik kot odjemalca. Ker napadalci želijo zapolniti vire na strežniku in ne na odjemalcu, pošljejo surov SYN paket, ki ima kot izvorni naslov nastavljen neuporabljen naslov proti strežniku. Če odjemalec ne ve, da je poslal SYN paket, se 3-stransko rokovanje ne bo izvedlo in ne bo zasedel virov na odjemalcu. Glede na to, da se 3-stransko rokovanje izvaja na plasti seje, se tudi SYN napadi izvajajo na tej plasti.

3.3.14. Kraja/ugrabitev seje (Session Hijacking)

Kakor že omenjeno, je TCP povezani protokol, pri katerem se najprej vzpostavi povezava med odjemalcem in strežnikom. Za to je poskrbljeno s pomočjo 3-stranskega rokovanja, katerega namen je sinhronizacija sekvenčnih številk (angl. sequence numbers) med odjemalcem in strežnikom za čas povezave. Ko so sekvenčne številke sinhronizirane, se prenos podatkov lahko prične. Slika 9 prikazuje potek 3-stranskega rokovanja.



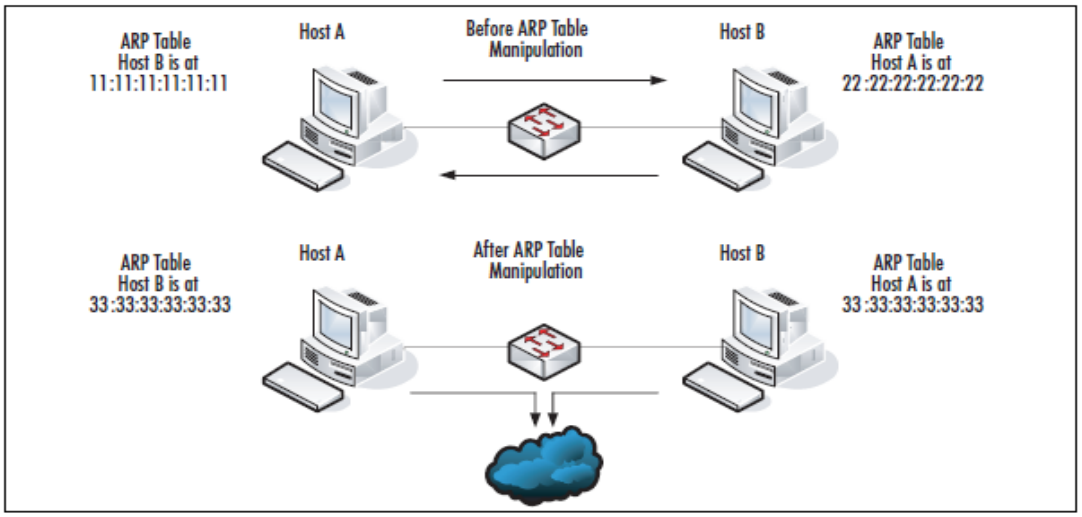
Slika 9: Sekvenčne številke med vzpostavljanjem seje (Greeg, 2006)

Sekvenčna številka odjemalca se poveča za 1 za vsak bajt poslanega podatka. Ko strežnik uspešno prejme podatke, vrne odjemalcu ACK paket s potrditveno številko (angl. acknowledgement number), katere vrednost je enaka naslednji pričakovani vrednosti sekvenčne številke. Kakor že omenjeno, se 3-stransko rokovanje izvaja na plasti seje, zato se tudi SYN napadi izvajajo na tej plasti.

Namen napada je pridobiti dostop do seje. Uspešna kraja seje omogoča prekinitev seje med strežnikom in odjemalcem in nato neopazno vzpostavi komunikacijo nazaj.

Ker usmerjevalniki večinoma blokirajo ICMP "redirect" pakete, napadalci ne morejo uporabiti MITM napada s pomočjo ICMP "redirect" paketa, zato uporabijo ARP poneverjanje, s čimer preusmerijo promet žrtve preko svoje naprave. Tako lahko analizirajo promet in predvidijo naslednjo sekvenčno številko. Napadalcu mora uspeti prepričati še prehod, da ima gostitelj nedosegljiv fizični naslov (v nadaljevanju MAC), in gostitelja, da ima prehod napadalčev MAC naslov. V tem primeru gostitelj ne bo prejel ACK paketa, kar bo preprečilo ARP poplavo. Primer

ARP poneverjanja prikazuje slika 10. Ko je enkrat promet tako strežnika kot gostitelja preusmerjen, lahko napadalec vrine neomejeno število podatkov. ARP poneverjanje se izvaja na povezovalni plasti.



Slika 10: ARP tabela pred in po napadu (Greeg, 2006)

Kraja seje se lahko izvaja tudi na aplikacijski plasti. V tem primeru mora imeti napadalec dostop (fizični, virusi/črvi, naiven uporabnik, XSS) do t. i. "session_id-ja", ki ga napadalec uporabi za dostop (Kozak, 2014). Piškotki so besedilne datoteke, shranjene v uporabnikovem računalniku, v katerih spletne strani hranijo določene informacije o uporabniku. Pogosto se uporabljajo tudi kot identifikatorji seje. Pri kraji piškotkov napadalec uporabi predmet "JavaScript document.cookie", s katerim pridobi podatke, shranjene v piškotku in tako lahko prevzame identiteto uporabnika na strani, ki je piškotek izdala (Strosar, 2014).

3.3.15. DNS zastrupljanje (Domain Name System Poisoning)

DNS zastrupljanje omogoča napadalcu, da prepriča DNS strežnik in se predstavi kot gostitelj na poljubnem IP naslovu. Vendar je napad težko izvesti, saj napadalec potrebuje identifikacijsko polje velikosti 2 bajta, ki ga vsebuje vsaka DNS poizvedba. Tovrstni napad je mogoč, ker se uporablja UDP, ki nima vzpostavitve seje in je zato hitrejši. Izvaja se na plasti seje.

3.3.16. NetBIOS napadi

NetBIOS (Network Basic Input/Output System) sam po sebi ni protokol. Je vmesnik za programiranje aplikacij (angl. application programming interface – API), ki zagotavlja bistvene omrežne funkcije, katere sistem potrebuje. Danes se NetBIOS večinoma uporablja preko TCP/IP protokola, vendar lahko teče tudi preko IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange) protokola. NetBIOS določa ogrodje, ki omogoča dvema ali več gostiteljem, da delijo objekte, ki se nahajajo na enem izmed teh gostiteljev. V povezavi s SMB (Server Message Block) zagotavlja dve pomembni storitvi, deljenje datotek in tiskalnikov (file and printer

sharing). Storitev NetBios se izvaja na plasti seje, na kateri se tudi izvajajo napadi.
Če NetBIOS ni primerno zaščiten, omogoča napadalcu lahek dostop do informacij o omrežjih in uporabnikih. V tem primeru gre za napad z zbiranjem (eangl. numeration attack). Druga možnost je, da bi lahko napadalec pridobil dostop do datotečnega sistema z izkoriščanjem ranljivosti administrativnih omrežnih diskov (administrative shares) v nekaterih operacijskih sistemih Windows. Obstaja tudi priložnost za DoS napade preko NetBIOS.

Ko napadalec dobi informacijo o odprtih vratih, začne z zbiranjem informacij, kaj točno je na voljo. Z napadom poizkuša pridobiti informacije o uporabniških imenih, skupinah in imenih skupnih map (angl. share names). Ko to pridobi, gre lahko še globlje in lahko v primeru, da sistem ni ustrezno zaščiten, pridobi še naslednje podatke:

- uporabniške račune,
- nastavitve skupin,
- članstvo v skupinah,
- nastavitve aplikacij,
- pasice storitev (angl. service banners),
- podatke o nastavitvah revizije (angl. audit setting),
- nastavitve ostalih servisov.

3.3.17. Vohljanje šifriranega prometa (Sniffing Encrypted Traffic)

Šifriranje prometa se izvaja na predstavitveni plasti, zato se tudi napadi izvajajo na tej plasti.

Čeprav so podatki zaščiteni, lahko napadalec izkoristi implementacije samega algoritma za kodiranje vsebine v ASCII znakovni nabor. Npr. organizacija uporablja Base64 algoritem in to razkrije v HTML izvorni kodi. Napadalec, ki prestreže podatke, te enostavno dešifrira.

Nekatere organizacije za zaščito gesel uporabljajo MD5 zgoščevalno funkcijo, ki za poljuben čistopis vrne 128-biten prstni odtis. Na ta način izpostavljene datoteke ne bodo razkrivale čistopisa gesel. Vendar, ker ima MD5 težave s kolizijo (Sotirov, Stevens, Appelbaum, idr., 2014), se priporoča uporaba SHA-1 z 256-bitno zgoščevalno funkcijo. Tudi SHA-1 ni imun na napade. Ravno tako kot MD5 je tudi SHA-1 občutljiv na napade s slovarjem (angl. dictionary attack) in z "grobo silo" (angl. brute force attack). Ti napadi se zanašajo na informacijo, katera funkcija je bila uporabljena za zaščito podatkov, in se opirajo na vhodne podatke ter primerjavo rezultatov z znanim prstnim odtisom. Če se rezultat ujema s ciljnim prstnim odtisom, je prava vrednost zaščitenih podatkov verjetno razkrita.

3.3.18. SQL vrinjenje (SQL Injection)

Glede na to, da se aplikacije izvajajo na aplikacijski plasti, se tudi napadi, povezani z aplikacijami, izvajajo na tej plasti.

Spletne aplikacije za shranjevanje in črpanje podatkov uporabljajo podatkovne baze. Gre za relacijske baze, ki za poizvedbeni jezik uporabljajo SQL. Včasih bo skripta izvedla poizvedbo v podatkovno bazo s pomočjo vnosa s spletne strani, ne da bi prej preverila, ali vhod vsebuje katerega od ubežnih znakov (angl. escape characters). Z ubežnik znakom ločilo spremenimo v navaden znak. Tipično \', kjer je \ ubežni znak, ' ločilo. Če vhod vsebuje ločila, ki spremenijo sintaktični pomen poizvedbe, govorimo o SQL vrivanju.

Primer prijave na spletno stran:

```
query = "SELECT * FROM users WHERE username = '{$_POST['user']}' AND password ='{$_POST['pass']}' ";
```

Ta poizvedba v podatkovni bazi preveri uporabniško ime in geslo ter v primeru, da vrne rezultat, je vneseno uporabniško ime in geslo pravilno.
V primeru, da nekdo uporabi uporabniško ime "bob", namesto gesla vpišemo del SQL stavka (' **OR '1'='1**'), ki spremeni prvotni SQL ukaz, in poizvedba se spremeni v:

```
"SELECT * FROM users WHERE username = 'bob' AND password = ' ' OR '1'='1'";
```

V tem primeru aplikacija ne preveri, ali se geslo v podatkovni bazi ujema s podanim geslom, ampak v vsakem primeru vrne podatke o uporabniku z ID1 (običajno je to skrbnik) in ga prijavi. Na tak način je možno iz podatkovne baze dobiti tudi kakšne občutljive podatke.

3.3.19. Vrinjenje kode (Code Injection)

Tudi v tem primeru so to napadi na aplikacijski plasti.

Podobno kot v primeru SQL vrinjenja, tudi tukaj velja, da uporabniško podani nizi niso preverjeni za ubežne znake, preden so poslani ukazom kot argument. Primer PHP skripta, ki sprejme niz s spletne strani in ga posreduje orodju *nslookup*, je naslednji:

```
<form action="nslookup.php" method="POST">
Hostname: <input name="hostname" type="text">
<input type="submit" value="Lookup">
</form>
<?php
system("nslookup {$_POST['hostname']}");
?>
```

V primeru, da napadalec vpiše v polje "hostname" vrednost www.google.com; **ls / -la**, bo rezultat izvedbe izpis skrbniške mape (angl. root directory). Na takšen način lahko napadalec s svoje spletne strani prenese škodljiv skript in ga zažene na žrtvinem strežniku (Greeg, 2006). Npr:

www.google.com;wget http://attackersite/backdoor.pl;perl backdoor.pl

3.3.20. XSS napad (Cross-Site Scripting – XSS)

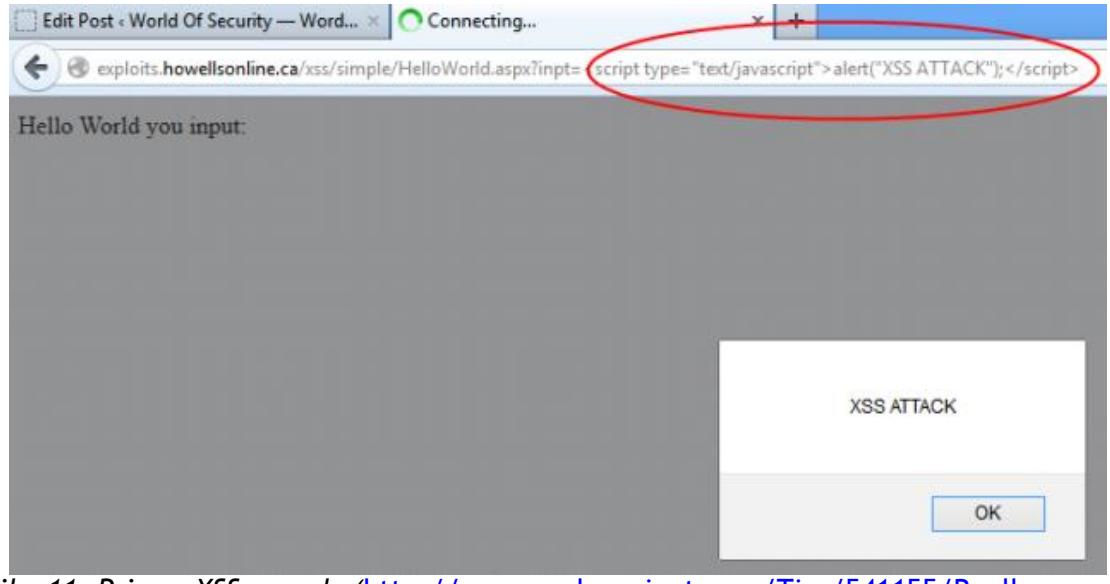
XSS napadi se izvajajo na aplikacijski plasti, saj gre za napad na aplikacije.

Predstavlja napad na spletno stran z vrinjenjem zlonamerne kode, napisane v skriptnem programskem jeziku. Omogoča napadalcu vrinjenje kode ali HTML-ja na spletno stran, ki bo izvedena v brskalniku obiskovalca, ko bo naključni uporabnik obiskal spletno stran. Ti napadi ciljajo na uporabnika in ne na samo spletno stran ter se pojavijo, kadar spletna stran pravilno ne počisti vhodnih podatkov, preden jih uporabi na izhodu.

V polje na spletni strani vpišemo:

<script type="text/javascript">alert("XSS ATTACK");</script>

in dobimo naslednje pojavno okno, kot je prikazano na sliki 11.



Slika 11: Primer XSS napada (http://www.codeproject.com/Tips/541155/Really-Simple-XSS-and-a-Solution, junij 2014)

3.3.21. Napad z DNS odbojem (DNS reflection, DNS amplification)

Je napad na omrežni in transportni plasti OSI modela.

Je zelo star način poplavljanja žrtve s prometom, vendar je v lanskem letu postal zopet aktualen. Ideja je preprosta: napadalec pošlje vprašanje DNS strežniku, ponaredi svoj izvorni naslov in vstavi žrtvinega, zato DNS strežnik odgovor pošlje žrtvi. Če napadalec želi ta enostavni trik spremeniti v napad, morata biti izpolnjena dva pogoja (Si-cert, 2014):

- pakete mora pošiljati iz omrežja ponudnika, ki omogoča potvarjanje naslovov in
- najti mora dovolj uslužnih DNS strežnikov, ki so pripravljeni odgovarjati komur koli na internetu (ang. open resolvers).

Ta napad je postal aktualen zaradi velikega števila uslužnih DNS strežnikov in uvedbe DNSSEC (Domain Name System Security Extensions). DNS odgovor je tipične velikosti manj kot 512 bajtov, medtem ko DNSSEC sporočila lahko dosežejo velikost tudi do 4096 bajtov. V primeru, da napadalec najde dovolj uslužnih DNS strežnikov, je DoS napad dokaj hitro uspešen. S tem povzroči težave tudi lastnikom uslužnih DNS strežnikov, ki imajo šibko povezavo, saj se jim povezava v smeri proti internetu hitro zapolni.

Podoben napad se izvaja tudi z uporabo NTP strežnikov.

3.3.22. "Heartbleed" ranljivost

Tudi v tem primeru se napad izvaja na aplikacijski plasti. Gre za resno ranljivost v priljubljeni OpenSSL kriptografski knjižnici programske opreme, ki je bila odkrita aprila 2014. Pomanjkljivost omogoča krajo podatkov, ki so v normalnih razmerah zaščiteni s šifriranjem SSL/TLS. Ranljivost obstaja od decembra 2011, ko je bila predstavljena verzija 1.0.1 knjižnice in vse do verzije 1.0.1f. Ranljivost je bila odpravljena v verziji 1.0.1g, ki je bila izdana 7. aprila 2014. Poleg verzije 1.0.1g nista ranljivi verziji 1.0.0 branch in 0.9.8 branch (heartbleed, 2014).

Heartbleed napaka omogoča vsakomur na internetu, da prebere del spomina na sistemih, ki jih varujejo ranljive različice programske opreme OpenSSL. To ogroža tajne ključe, ki se uporabljajo za identifikacijo ponudnikov storitev in šifriranje prometa, imena in gesla uporabnikov ter dejanske vsebine. Napadalcem omogoča prisluškovanje komunikacijam, krajo podatkov neposredno od storitev in uporabnikov ter se izdajati kot storitev in uporabnik.

3.3.23. Socialni inženiring

Socialni inženiring je umetnost prevare, ki ima v človeški civilizaciji dolgo tradicijo. Po svoji naravi pomeni predvsem pridobivanje koristi z zlorabo zaupanja posameznika oz. z manipulacijo. V zgodovini je najbolj znana Odisejeva prevara oz. njegov trojanski konj. Tega so Trojanci potegnili v mesto, ponoči pa so iz njegovega trebuha skočili grški vojaki in skozi vrata v mesto spustili svojo vojsko. Ukana ne bi uspela, če Grki ne bi dobro poznali Trojancev: kakšni so, kaj želijo in kako se bodo na konja odzvali. Prvi sodobni oz. tehnološki socialni heker je bil Kevin Mitnick, ki je s pomočjo socialnega inženiringa prišel do zaupnih poslovnih podatkov najrazličnejših podjetij. Znano je njegovo stališče, da je veliko enostavnejše z besedami in dejanji pretentati zaposlenega v izdajo osebnega geslo za vstop v sistem, kot se truditi z vdorom vanj (Moj Mikro, 2012).
V nadaljevanju bo predstavljeno nekaj najpogostejših napadov s pomočjo socialnega inženiringa.

a) Zvabljanje/Ribarjenje (anlg. Phishing)

S tem imenom poimenujemo krajo podatkov, ki storilcu omogočijo dostop do spletnih storitev v našem imenu in v skrajnem primeru tudi krajo našega denarja. V običajnem scenariju nas skuša storilec z elektronskim sporočilom zvabiti na lažno stran banke ali spletne storitve. Običajno pod pretvezo, da se moramo zaradi preverjanja podatkov ali dodatnih ugodnosti prijaviti in "preveriti podatke". Če na tej lažni strani vpišemo geslo za dostop, se le-to posreduje storilcu (Si-cert, 2014).

Čeprav je zvabljanje v osnovi namenjeno kraji podatkov za dostop do e-bančništva, imajo vrednost tudi drugi podatki, ki se nam na prvi pogled morda ne zdijo vredni stroge zaščite. Najbolj tipično je uporabniško ime in geslo za dostop do poštnega predala. Velika večina omrežnih storitev od nas zahteva registracijo, kjer si izberemo ime (večinoma lahko kar uporabimo svoj elektronski naslov) in določimo geslo za dostop do storitve. V primeru, da geslo pozabimo, nam spletno mesto na dani elektronski naslov pošlje spletno povezavo za nastavitev novega gesla. Kdor ima dostop do našega poštnega predala, lahko v našem imenu dostopa tudi do storitev, pri katerih smo elektronski naslov predala navedli pri registraciji (Si-cert, 2014).

b) Prevare na spletnih socialnih omrežjih

V spletnih socialnih omrežjih je v današnjem času zlonamerna koda običajen pojav. Mladi in odrasli dnevno množično uporabljajo spletna socialna omrežja in nanje nalagajo veliko podatkov. To je tudi obdobje, ko so spletne prevare v vzponu, s tem pa tudi zlorabe podatkov. Spletna socialna omrežja so v zadnjih letih postala zelo priljubljena, ker omogočajo, da ljudje spoznavajo osebe s podobnimi interesi. Poleg vseh ugodnosti in prednosti, ki jih ponujajo spletna socialna omrežja, je tudi veliko slabosti, kot so grožnje zasebnosti uporabnikov ter zlorabe osebnih podatkov v različne namene (Murn, 2014).

Uporabniki spletnih socialnih omrežij z neverjetno lahkotnostjo posredujejo svoje podatke, kar spretno izkoriščajo spletni prevaranti, in sicer za pridobivanje in nato za zlorabo pridobljenih podatkov. Istočasno je poznavanje značilnosti, navad in načina komunikacije uporabnikov pomembno tudi z vidika informacijske varnosti ter osveščanja o nevarnostih, ki prežijo na spletnih socialnih omrežjih, tako na posameznike kot na podjetja (Murn, 2014).

c) Neželena elektronska pošta (SPAM)

V splošnem lahko za neželeno elektronsko sporočilo smatramo vsako sporočilo, ki je poslano večjemu številu naslovnikov z namenom vsiljevanja vsebine, ki se je naslovniki sami ne bi odločili prejemati. V veliki večini primerov gre za oglaševanje plačljivih storitev ali izdelkov. Običajno se z neželeno elektronsko pošto oglašujejo izdelki ali storitve dvomljive kvalitete, velikokrat pa gre za goljufije. Tak tipičen primer je nigerijska prevara.
Zakaj "spam" ni zaželen (Si-cert, 2014):

- “spam” utaplja koristno komunikacijo;
- večino stroškov nosi prejemnik;

- kraja resursov in nepooblaščena uporaba tujih računalnikov;
- pošiljatelj "spama" vas morda želi zavesti ali ogoljufati;
- "spam" je lahko nevaren.

d) Spletne goljufije

Hitra in enostavna spletna komunikacija tudi goljufom omogoča celotno paleto "prijemov". Naj navedemo nekaj primerov.

Prijateljeva prošnja za pomoč

Po elektronski pošti se vam javi prijatelj ali znanec in vas prosi za pomoč. Na hitro opiše, kako so mu na potovanju po Afriki ukradli denar in vse dokumente. Sedaj nujno potrebuje denar, da si bo lahko kupil hrano in se vrnil domov.

Sporočila seveda ni poslal vaš prijatelj, ampak nekdo, ki mu je ukradel geslo za dostop do brezplačnega poštnega predala (kot sta npr. hotmail.com ali gmail.com). Ukradeno geslo mu omogoči, da sporočila pošlje samo osebam, s katerimi se vaš prijatelj tudi sicer dopisuje (Varni na internetu, 2014).

Nigerijske prevare in spletni nakupi

V t. i. nigerijski prevari želi goljuf prepričati žrtev, da ji lahko ponudi dobro plačilo za prenos velike vsote denarja preko žrtvinega bančnega računa. Za izvedbo transakcije si izmisli sorazmerno nizek strošek, ki ga mora žrtev najprej plačati, da se lahko transakcija izvede. Goljuf nato niza še druge stroške enega za drugim, dokler žrtev ne spregleda prevare. Zlorabe, ki smo jim priča v zadnjem obdobju, pa so nadgrajene z nekaterimi dodatki, ki skušajo povečati navidezno verodostojnost goljufa (Si-cert, 2014).

Žrtev najdejo s spletnim oglasom, npr. na bolha.com. Tam bodoča žrtev oglašuje, da želi prodati npr. mobilni telefon. Goljuf se predstavi kot možni kupec in pri tem navede, da je rezident evropske države, vendar kupuje telefon za sorodnika v Nigeriji. Sporočila so včasih tudi prevedena v slovenščino s pomočjo Google Translate, kar je iz vsebine jasno opazno (Si-cert, 2014).

Pri plačilu naj bi posredoval sistem PayPal, kot zaupanja vreden sistem plačevanja preko omrežja. Žrtev naj pošlje paket in posreduje njegovo identifikacijsko številko na PayPal, ki potem sprosti plačilo. Pri tem goljuf podtakne lažna elektronska sporočila in zahteva v imenu PayPala dodatne kavcije za izvedbo transakcije. V nekem primeru je žrtev dobila tudi sporočila, ki naj bi prišla s carinske službe v Nigeriji, seveda pa je šlo še za dodaten gradnik goljufije (Si-cert, 2014).

e) Gledanje čez ramo (angl. shoulder surfing)

V računalniški varnosti se gledanje čez ramo nanaša na uporabo tehnik neposrednega opazovanja, kot je gledanje nekomu čez ramo z namenom pridobiti informacije. To se običajno uporablja za pridobitev gesla, PIN-a, varnostne kode, in podobnih podatkov (Shoulder surfing. Wikipedija, 2014).

f) Brskanje po smeteh (angl. Dumpster diving)

Gre za prebiranje fizičnih odpadkov, ki so jih odvrgla podjetja ali posamezniki. Ti odpadki imajo lahko neko uporabno vrednost za prebiralca. Privedejo ga lahko do informacij, ki bi jih uporabili za ogrozitev omrežja ali identitete. Če žrtev zavrže bančne izpiske, izpiske kreditih kartic ali druge občutljive podatke brez pravega razreza, lahko napadalec pridobi informacije o žrtvi (Dumpster Diving.Abaut.com, 2014).

"Dumpster diving" lahko vodi tudi v "Information diving". Gre za povrnitev tehničnih podatkov, včasih zaupne ali tajne narave iz zavrženih materialov. V zadnjem času gre predvsem za medije za shranjevanje podatkov na odsluženih računalnikih. Iskani so večinoma obnovljivi podatki, ki so ostali na trdih diskih. Osebe, zadolžene za odpis računalniške opreme, običajno zanemarjajo brisanje trdih diskov. Tako lahko napadalec prekopira programsko opremo, s čimer pridobi dostop tudi do bolj občutljivih podatkov, shranjenih na njih (npr. številka kreditne kartice) (Information diving. Wikipedija, 2014).

g) Spletni iskalniki

Socialni inženiring velikokrat poteka po principu izrabe že obstoječih informacij o posamezniku za pridobitev še več in bolj ključnih podatkov. Glede na to, da se skoraj o vsakem izmed nas na internetu pojavljajo določeni podatki, socialni inženir zlahka pridobi podatke o naši preteklosti (o naših hobijih, obiskovanih šolah, profesionalnem življenju in ostalih aktivnostih). Nemalokrat se zgodi celo, da so na internetu objavljeni določeni osebni podatki (v obliki seznamov, tabel ...) pomotoma, saj za velikimi strežniki in računalniškimi ekrani seveda sedijo ljudje, uredniki spletnih strani, ki lahko objavijo na internetu nekaj, česar pravzaprav niso nameravali (IP RS(a), 2014).

h) Socialni inženiring preko telefona

Izvedba socialnega inženiringa s pomočjo telefonskega klica je glede na svojo učinkovitost precej enostavna. Napadalec pokliče ciljno osebo z namenom, da od nje pridobi določene podatke. Pogosto so to administratorska prijavna imena in gesla. Tovrstnim napadom so podvrženi zlasti razni asistenti, tajnice in drugi zaposleni v sprejemnih pisarnah. Prav ti ljudje so namreč navadno slabše poučeni o varnostni politiki in morajo biti ustrežljivi in prijazni do vsakega klicatelja. Torej sprejemajo klic za klicem, ne razmišljajo o posledicah, to pa predstavlja veliko varnostno luknjo. Takšen napad se najpogosteje izvede s telefonske naprave, pri kateri ni potrebna nobena avtentikacija storilca (IP RS(a), 2014).

i) Vishing

Vishing je novejši poltehnični pristop socialnega inženiringa, ki izkorišča telefonske sisteme vrste VoIP (Voice over IP). Tudi ta izraz je kombinacija dveh besed, in sicer “voice”, torej glas, in “phishing”, zvabljanje. Vishing se uporablja predvsem za krajo identitete in drugih zaupnih podatkov (npr. podatki o kreditnih karticah). Pri izvedbi klica napadalec skrije pravo številko in jo zamenja s številko, ki jo žrtev pozna ali ji zaupa (npr. operaterja). Tehniko je mogoče uporabiti v navezi z zvabljanjem tako, da je v elektronski pošti navedena številka namesto spletne povezave. Napad se izvede ob pomoči vnaprej posnetega govora, ki

uporabnika opozori, da je z njegovim računom nekaj narobe. Nato ga ta posnetek vodi skozi procese, ki na koncu pripeljejo do želenega razkritja zaupnih informacij (IP RS(a), 2014).

j) Napad s pomočjo nosilcev podatkov

Male nosilce podatkov odlikuje praktičnost, so lahki in prenosni, hkrati glede na svojo velikost sprejmejo veliko količino podatkov. Ravno zaradi njihove popularnosti in vsesplošne uporabnosti lahko hitro postanejo način, kako izrabiti nepazljivost žrtve.

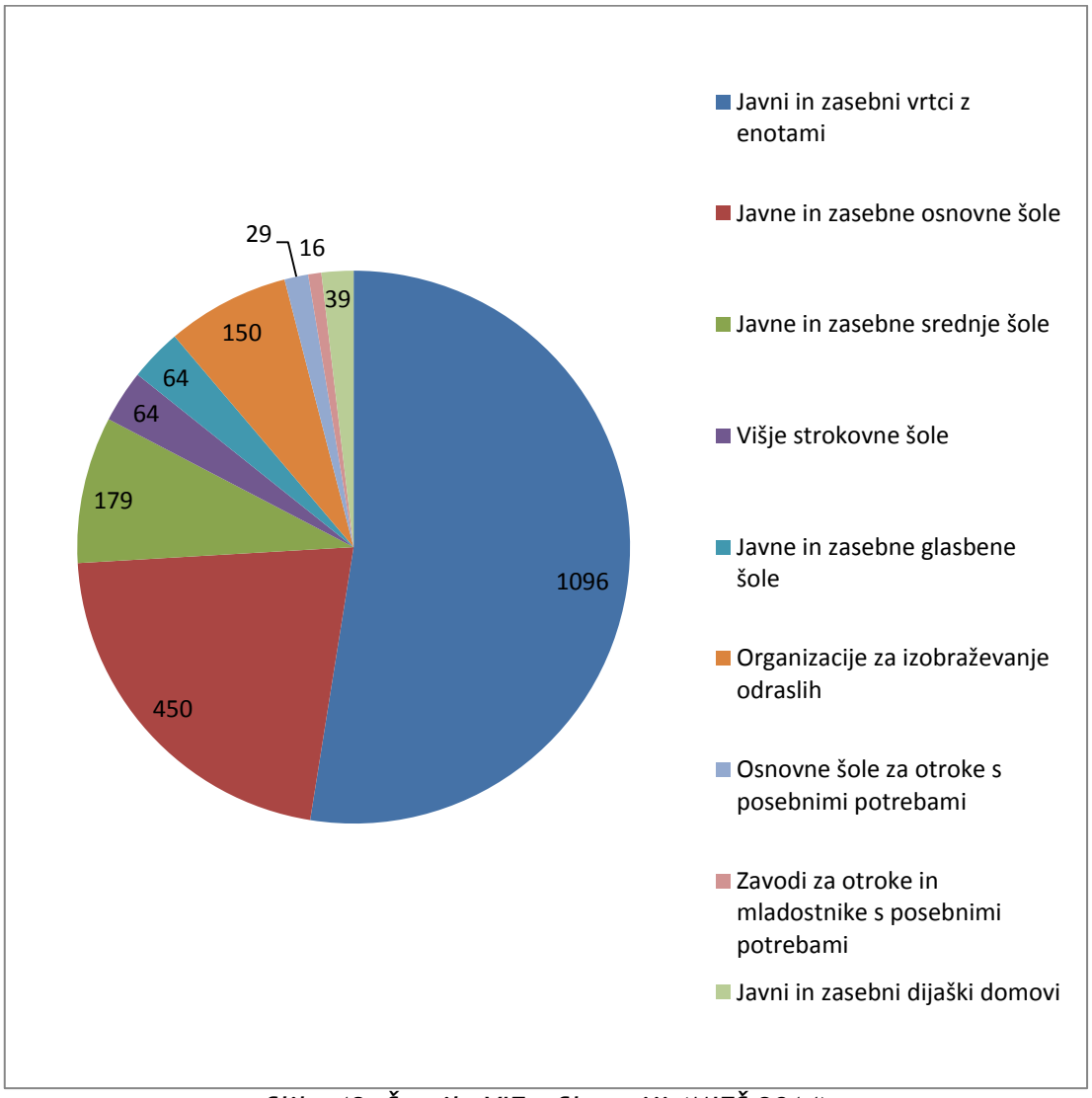
Napad s pomočjo USB ključka se navadno izvede tako, da napadalec ključek s škodljivo programsko kodo pusti na javnem kraju, kjer čaka na žrtev. Ker smo ljudje po naravi zvedavi, ključek nekdo pobere in ga pogosto brez pomisleka vtakne v računalnik. Ob tem se na računalniku zažene program, ki z računalnika pobere vsa shranjena gesla in jih pošlje na elektronski naslov napadalca. Lahko se celo zgodi, da se s ključka samodejno namesti trojanski konj ali podobna škodljiva programska oprema.

4. ZAGOTAVLJANJE VARNOSTI RAČUNALNIŠKIH OMREŽIJ V VIZ

V nadaljevanju bomo predstavili, kakšno je stanje varnosti računalniških sistemov VIZ v Sloveniji. Podali bomo rezultate ankete o varnosti računalniških omrežij na VIZ, ki so jo izpolnili skrbniki sistemov v slovenskih VIZ. Navedli bomo tudi nekaj primerov dobrih praks iz tujine.

4.1. Stanje v Sloveniji

V Sloveniji je bilo v šolskem letu 2013/2014 registriranih 2084 VIZ (MIZŠ, 2014). Slika 12 prikazuje število zavodov glede na vrsto.



Slika 12: Število VIZ v Sloveniji (MIZŠ 2014)

4.1.1. Vloga posameznih državnih organizacij

a) Arnes

Kakor že omenjeno, je Arnes javni zavod, ki zagotavlja omrežne storitve organizacijam s področja raziskovanja, izobraževanja in kulture, omogoča njihovo povezovanje in medsebojno sodelovanje ter sodelovanje s sorodnimi organizacijami v tujini. Zaradi nenehnih sprememb tehnologije se Arnes sproti prilagaja potrebam svojih uporabnikov in jim dolgoročno želi zagotoviti enake možnosti sodelovanja v enotnem evropskem prostoru. Pogoj za to je tesno povezana omrežna infrastruktura z enotnimi tehnološkimi in varnostnimi standardi ter ustrezne storitve, ki jih na celotnem evropskem območju vzpostavljajo in vzdržujejo nacionalne izobraževalne in raziskovalne mreže.

V omrežje ARNES je povezanih več kot 1000 slovenskih organizacij, storitve Arnesa na tak način uporablja blizu 200 000 ljudi. Mednarodna povezljivost z izobraževalnimi in raziskovalnimi omrežji drugih držav je zagotovljena preko več deset gigabitnega omrežja GÉANT, ki ga sofinancira Evropska komisija. Na ta način lahko uporabniki sodelujejo pri mednarodnih projektih, ki zahtevajo hitre in zanesljive informacijsko-komunikacijske povezave, stabilne videokonferenčne prenose ter prenos velike količine podatkov.

Poleg same povezljivosti imajo VIZ, tudi tisti, ki niso povezani v omrežje ARNES, na voljo kup storitev, ki jih lahko koristijo brezplačno. Storitve, ki jih omogoča Arnes, so:

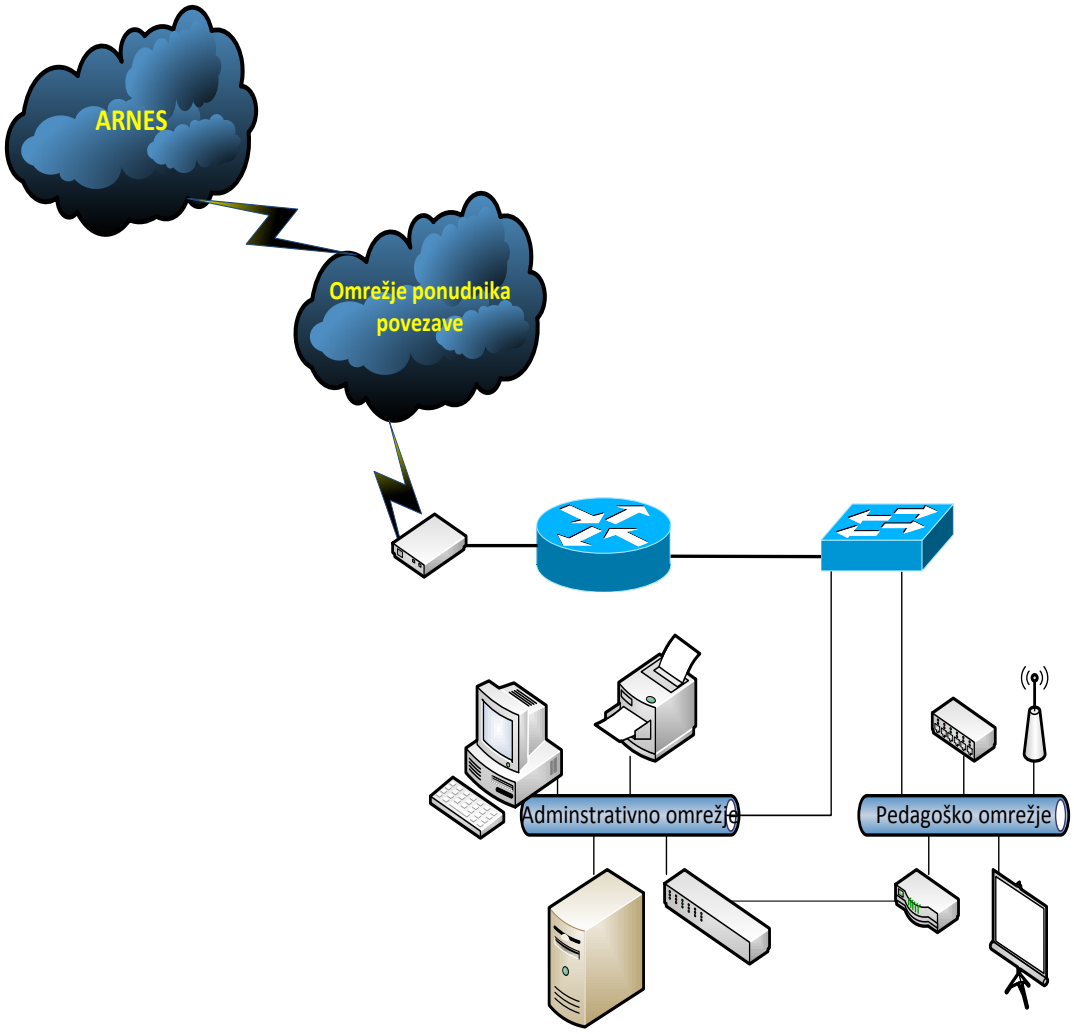
- elektronska pošta s protivirusno zaščito,
- dinamično gostovanje spletnih strani,
- gostovanje virtualnih strežnikov,
- označevanje nezaželene elektronske pošte,
- gostovanje spletnih strani na CMS sistemu Wordpress,
- analiza obiska spletnih strani,
- registracija in upravljanje domen,
- digitalna strežniška potrdila (Comodo CA Limited),
- možnost uporabe gruč,
- spletne videokonference,
- videokonference visoke ločljivosti,
- možnost prenosov videa v živo,
- zelo hiter prenos zvoka in slike prek interneta (LOw LAtency audio visual streaming system – LOLA).

Tistim, ki so povezani v omrežje ARNES, omogoča še:

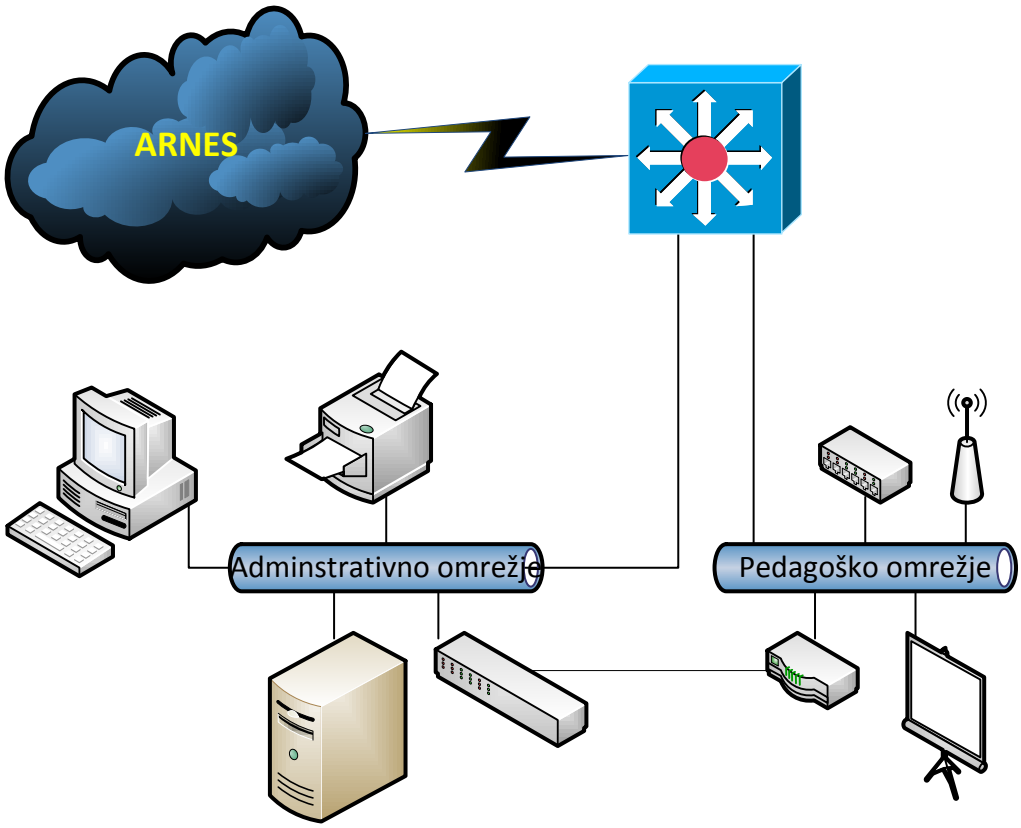
- upravljanje usmerjevalnika in stikala (CPE),
- prioriteto prometa (QOS),
- filtriranje prometa proti omrežju zavoda,
- registracijo javnih IP naslovov.

Izmed vseh VIZ, jih je v omrežje ARNES povezanih 863. Ti se povezujejo preko tehnologij: xDSL, FTTH, Wifi ali neosvetljenih optičnih vlaken.

Sliki 13 in 14 prikazujeta omrežje VIZ, ki je povezano v omrežje ARNES. Na slikah vidimo najpogostejše elemente (PC, stikalo, hub, tiskalnik, strežnik, dostopna točka, interaktivna tabla …), ki jih najdemo v njihovem omrežju. Slika 13 prikazuje povezavo v omrežje ARNES preko enega izmed ponudnikov povezave. Pri tem načinu povezave je največkrat uporabljen Cisco usmerjevalnik in Cisco stikalo (v nadaljevanju L2 stikalo). Slika 14 prikazuje povezavo (optično) direktno do vozlišča ARNES. Pri takšnem načinu povezave je največkrat uporabljeno Cisco stikalo, ki omogoča tudi protokole in storitve omrežne plasti (v nadaljevanju L3 stikalo), saj omogoča, da je hitrost omejena samo s hitrostjo vmesnika (angl. line Fate). V tem primeru usmerjevalnik in L2 stikalo ali L3 stikalo upravlja Arnes. Na usmerjevalniku ali L3 je izvedeno filtriranje prometa s pomočjo filtrov (Acess Control List – ACL) glede na želje zavoda in zagotavljanje kakovosti storitve (Quality of Service – QOS). Na samem stikalu je izvedena ločitev omrežja na vsaj 2 omrežji (administrativni in pedagoški del). Pri L3 stikalu (v nadaljevanju usmerjevalnik) se to že izvaja s pomočjo tega stikala. Glede na želje zavoda jih je možno nastaviti tudi več.



Slika 13: Omrežje VIZ, povezano v omrežje ARNES preko enega izmed ponudnikov povezave.



Slika 14: Omrežje VIZ, povezano neposredno v omrežje ARNES.

Kakor smo že omenili, lahko okrnjeno, vendar v osnovi podobno, funkcijo kot požarna pregrada opravlja tudi usmerjevalnik prometa, s katerim se šola povezuje v omrežje ARNES in internet. Usmerjevalnik prometa lahko nadzoruje in filtrira internetni promet na podlagi informacij, ki so kot dopolnilo podatkov shranjene v paketih, katere usmerjevalnik prenaša za šolsko omrežje. Usmerjevalnik lahko filtrira na podlagi naslova, od koder promet prihaja, naslova, kamor je promet namenjen, tipa prometa (protokola, internetnega servisa oz. storitve) in še nekaterih drugih podatkov. Vendar ne more nadzorovati vsebine prometa, količine prenesenih podatkov, trajanja, imena uporabnika ipd. Z usmerjevalnikom, ki ima nameščeno le osnovno programsko opremo, tudi ni mogoče zgraditi navideznih privatnih omrežij (angl. VPN), omogočiti avtentikacije uporabnikov, ki dostopajo do šolskih sistemov, šifrirati prometa itd.

Usmerjevalnik prometa je že del šolskega omrežja in je pod nadzorom in upravljanjem tehničnega osebja Arnesa. Zato je to, kljub okrnjeni funkcionalnosti v primerjavi z običajno protipožarno pregrado, za šolo pogosto cenovno najbolj ugodna in dostopna rešitev.

Drugi element v omrežju, je stikalo, na katerem se izvaja ločitev omrežja s pomočjo navideznih lanov (VLAN).

Uporabniki lokalnega računalniškega omrežja šole so v večini primerov razdeljeni v vsaj dve skupini:

- administracijo, vodstvo in učitelje,
- učence.

Vsebina podatkov, s katerimi razpolagajo člani prve t. i. administrativne skupine, je s stališča varnosti bolj občutljiva in zahteva višjo stopnjo varovanja. Dostop do teh podatkov je iz pedagoške skupine zato omejen in nadzorovan. Pedagoški del omrežja je na stikalu ločen od administrativnega, saj se le na ta način lahko kontrolira promet med omrežjema. Napravam v pedagoškem delu omrežja je tudi preprečeno prisluškovanje (angl.sniffing) prometu, ki poteka na administrativnem delu omrežja.

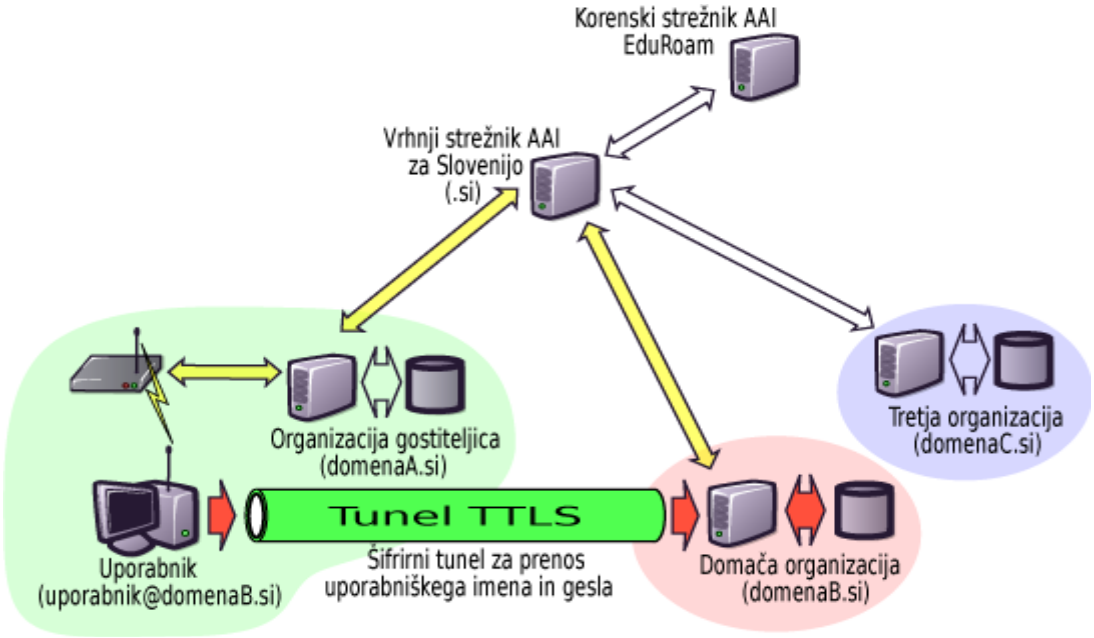
Ker na VIZ niso samo računalniki, pač pa tudi strežniki, je potrebno ščititi tudi te. Strežniki so računalniški sistemi, ki so dostopni širšemu krogu uporabnikov. Običajno so ti sistemi dosegljivi z interneta. Na VIZ so to običajno: imenski strežnik (DNS), strežnik za elektronsko pošto (SMTP, POP3, IMAP), WWW, FTP, DNS, DHCP strežnik … Dostop do teh storitev z interneta, drugih segmentov lokalnega omrežja (npr. iz pedagoškega dela, če se strežnik nahaja v administrativnem delu omrežja) in iz lokalnega omrežja, v katerem se strežnik nahaja, se omejuje skladno z opisom internetnega prometa določene storitve.

V preteklosti Arnes na ISDN povezavah ni upravljal usmerjevalnika, zato so se ob preklopu na xDSL tehnologijo postavili filtri za osnovne storitve, kot so: DNS, NTP, SMTP, POP3, IMAP, HTTP, HTTPS.

O tem so bili VIZ obveščeni v dokumentaciji, ki so jo prejeli poleg nove komunikacijske opreme, ki jo upravlja Arnes. Koliko so si nasvete in navodila prebrali, se vidi v tem, da imajo nekateri VIZ še vedno nastavljene privzete nastavitve. Vendar Arnes ne določa varnostne politike na VIZ, temveč o tem samo opozarja zavode, dokler ne pride do kakšnega varnostnega incidenta.

Arnes nudi tudi podporo pri vzpostavitvi brezžičnega omrežja Eduroam (education roaming). Eduroam je mednarodna federacija brezžičnih omrežij za uporabnike iz izobraževalne in raziskovalne sfere. Študenti, učenci, pedagogi, raziskovalci in drugi lahko uporabljajo vsako brezžično omrežje Eduroam, v Sloveniji ali tujini. Za uporabo je potrebno le odpreti prenosnik in to ne glede na lokacijo: na domači ustanovi ali na primer na Univerzi v Edinburgu (Eduroam.si 2014).

Na sliki 15 je prikazan potek prijave uporabnika v omrežje Eduroam.



Slika 15: Potek prijave uporabnika v omrežje Eduroam (Arnes AAI 2014)

Vidimo lahko napredno uporabo WPA-2 Enterprise protokola, ki kot dodatek za avtentikacijo uporabnikov uporablja Radius strežnik.

VIZ imajo na Arnesu omogočeno tudi gostovanje elektronske pošte z uporabo lastne domene, kjer se tako izvajajo virusna preverjanja in označevanje neželene elektronske pošte. Tudi v primeru, da imajo VIZ postavljen lastni poštni strežnik, lahko preusmerijo svoje MX DNS zapise na Arnesove strežnike, ki prejeto elektronsko pošto pregledajo, ustrezno označijo glede na vsebino (oznaka je vidna v glavi elektronske pošte) in dostavijo na strežnike VIZ. Njihovi strežniki se potem "odločijo", kaj bodo naredili s prejeto pošto. Prednosti te rešitve so predvsem v tem, da je bitka z neželeno elektronsko pošto stalno opravilo, ki zahteva precej dela. Velikokrat se izkaže, da včerajšnji prijemi za zaznavo neželene elektronske pošte danes ne delujejo več. Arnesovi strokovnjaki s sodelovanjem zunanjih sodelavcev iz Instituta Jožefa Stefana proaktivno spremljajo delovanje poštnih strežnikov in ukrepajo glede na trende pri pošiljanju neželene elektronske pošte. Poleg označevanja neželene elektronske pošte članicam ponuja tudi možnost podpisovanja poslane elektronske pošte DKIM (DomainKeys Identified Mail), ki poveča verjetnost, da se bo poslana elektronska pošta res pojavila v nabiralniku prejemnika in ne bo končala v njihovi mapi za neželeno elektronsko pošto.

V okviru Arnesa deluje tudi SI-CERT (Slovenian Computer Emergency Response Team), ki je nacionalni odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij. Opravlja koordinacijo razreševanja incidentov, tehnično svetovanje ob vdorih, računalniških okužbah in drugih zlorabah ter izdaja opozorila za upravitelje omrežij in širšo javnost o trenutnih grožnjah na elektronskih omrežjih. SI-CERT samostojno izvaja nacionalni program ozaveščanja "Varni na internetu" in sodeluje v projektu SAFE-SI (Si-cert, 2014).

SI-CERT na svoji spletni strani redno obvešča o novih ranljivostih in nevarnostih. Preko spletne strani je možno oddati tudi prijavo varnostnega incidenta.

Pod okriljem SI-CERT-a pa se izvaja tudi projekt "Varni na internetu", čigar namen je (Varni na internetu, 2014):

- dvigniti stopnjo zavedanja slovenskih spletnih uporabnikov o različnih nevarnostih, katerim so izpostavljeni na spletu;
- informirati o varni uporabi spletnega bančništva in varnem spletnem nakupovanju;
- informirati o različnih oblikah spletnih goljufij in ponuditi praktične rešitve, kako se zavarovati;
- informirati o varstvu osebne identitete.

Namenjen je najširši slovenski javnosti, poseben sklop vsebin pa je namenjen malim podjetjem, obrtnikom in samostojnim podjetnikom. Na svojem portalu s primeri in zabavnimi video spoti prikažejo varnostna tveganja na spletu in navodila, kako se pred njimi zaščititi.

b) Projekt SAFE-SI

Projekt Center za varnejši internet SAFE.SI izvajajo Univerza v Ljubljani, Fakulteta za družbene vede, Arnes, Zveza prijateljev mladine Slovenije in Zavod MISSS (Mladinsko informativno svetovalno središče Slovenije), financirata ga Generalni direktorat Connect pri Evropski komisiji in Ministrstvo za izobraževanje, znanost in šport.

Safe.si je točka ozaveščanja o varni rabi interneta in novih tehnologij, katere namen je ozaveščanje ciljnih skupin otrok, najstnikov, staršev, učiteljev in socialnih delavcev preko različnih "online" in "offline" aktivnosti, izobraževanj, delavnic, gradiv, promocijskih in medijskih kampanj o tem, kako varno in odgovorno uporabljati internet in mobilne naprave (Safe.si, 2014).

Poleg točke ozaveščanja v okviru projekta Safe.si se izvajata še storitvi Tom in Spletno oko. Pri prvi gre za svetovalno linijo za težave na spletu Tom telefon 116 111, na kateri med 12. in 20. uro vsak dan svetovalci odgovarjajo na vprašanja, dileme in rešujejo zagate, povezane z uporabo interneta. Storitev je na voljo za otroke, mlade in njihove starše. S februarjem 2013 je z delovanjem pričela tudi TOM klepetalnica http://www.e-tom.si/, kjer lahko otroci, mladostniki ter njihovi starši nasvete in pomoč dobijo preko spletnega klepeta. Med letoma 2012 in 2013 so obravnavali 234 vprašanj, ki so se nanašala na vprašanja varne rabe interneta. Tukaj je šlo predvsem za vprašaja na temo potencialno škodljivih vsebin in vsebin vrstniškega nasilja preko spleta (Safe.si, 2014).

Storitev Spletno oko nudi anonimno spletno prijavo nezakonitih spletnih vsebin – posnetkov spolne zlorabe otrok (otroška pornografija) in sovražnega govora. Če na spletu naletite na tovrstne vsebine, jih lahko prijavite na www.spletno-oko.si. Sodelovanje podobnih točk v Evropi se je izkazalo za učinkovit ukrep v boju za zmanjšanje nezakonitih vsebin na internetu. V letu 2012 so prejeli 4707 prijav sovražnega govora in 1127 prijav spolnih zlorab otrok. Medtem ko večina prijav sovražnega govora ne ustreza kriterijem za potencialno kaznivost (le 1,5 %), je skorajda za eno četrtino (24 %) prijav posnetkov spolnih zlorab otrok ugotovljeno, da posedujejo znake kaznivih dejanj (Safe-si, 2014).

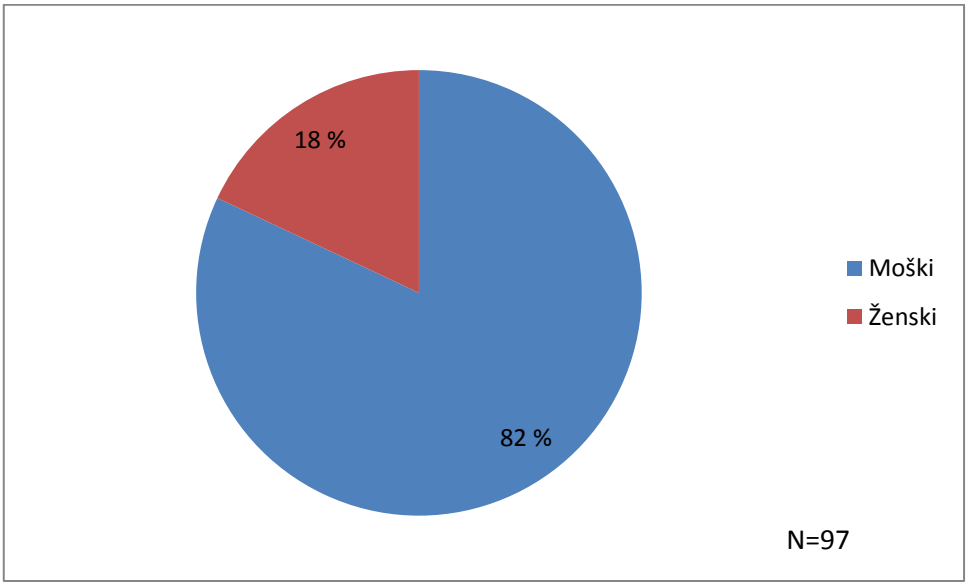
V okviru Safe.si poteka tudi program Varnejši internet. Uporaba interneta in drugih komunikacijskih tehnologij, kot so mobilne naprave, v Evropski uniji še vedno zelo narašča in ponuja vsem državljanom velike priložnosti (udeležba, interaktivnost in ustvarjalnost). Vendar tveganja za otroke in zloraba tehnologij še vedno obstajajo, zaradi spreminjajočih se tehnologij in socialnega vedenja pa nenehno nastajajo nova tveganja in zlorabe. Cilji programa so (Safe-si, 2014):

- povečanje ozaveščenosti javnosti: omogočanje mladim, njihovim staršem in učiteljem, da lahko pri uporabi interneta sprejemajo odgovorne odločitve s pomočjo nasvetov o tem, kako biti previden na spletu;
- zagotoviti omrežje kontaktnih točk, dosegljivih preko spletne strani ali na telefonski številki in pri katerih je mogoče prijaviti nezakonite in škodljive vsebine in obnašanje, zlasti otroško pornografijo, spletno zapeljevanje otrok (angl. grooming) in ustrahovanje na spletu (anlg. cyberbullying);
- pospeševanje pobude za samoregulativo na tem področju in vključevanje otrok v ustvarjanje varnejšega spletnega okolja;
- vzpostavitev baze znanja o novih trendih pri uporabi spletnih tehnologij in njihovih posledicah za življenje otrok, pri čemer bodo na evropski ravni združena tehnična, psihološka in sociološka strokovna znanja in izkušnje.

4.1.2. Analiza obstoječega stanja v slovenskih VIZ

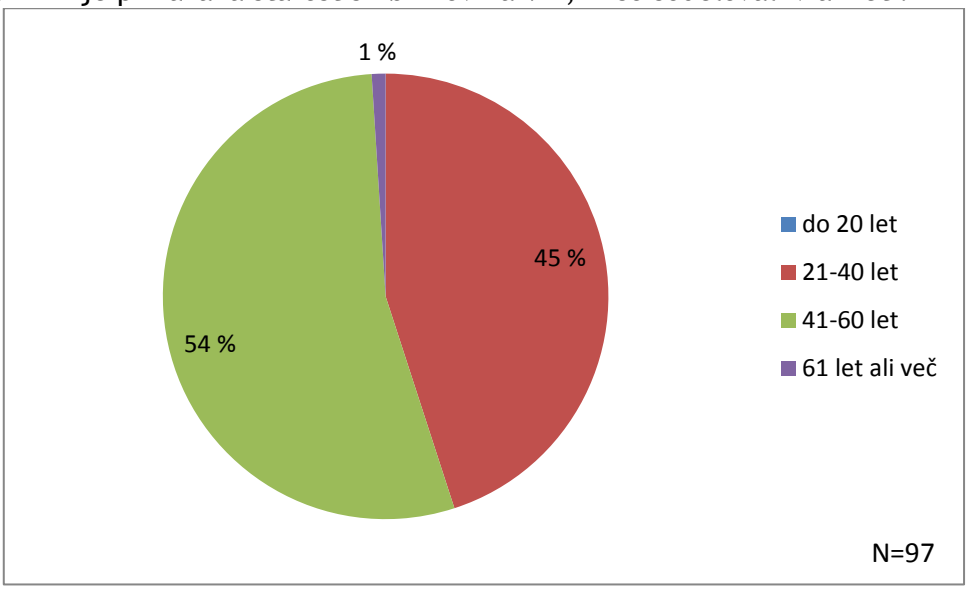
V magistrskem delu raziskujemo, kako na slovenskih VIZ skrbijo za varnost računalniških omrežij. V ta namen smo pripravili spletni vprašalnik (Priloga 1), ki je bil izdelan s spletnim orodjem 1ka (www.1ka.si). V raziskavi opazujemo odnos entitete VIZ do varnosti računalniških omrežij. V imenu VIZ je vprašalnik izpolnjevala oseba, ki je na VIZ skrbnik IKT. Vprašalnik smo preko spletne pošte poslali na kontaktne e-naslove 100 VIZ v Sloveniji, poleg tega pa je bila povezava do spletnega vprašalnika objavljena na portalu Slovenskega izobraževalnega omrežja (www.sio.si). E-naslove smo pridobili s strani Ministrstva za izobraževanje, znanost in šport. Vprašalnik so začeli izpolnjevati na 135 VIZ, zaključili pa v 97 primerih.

Slika 16 prikazuje odstotek moški in ženskih sodelujočih v anketi glede na vrsto VIZ.



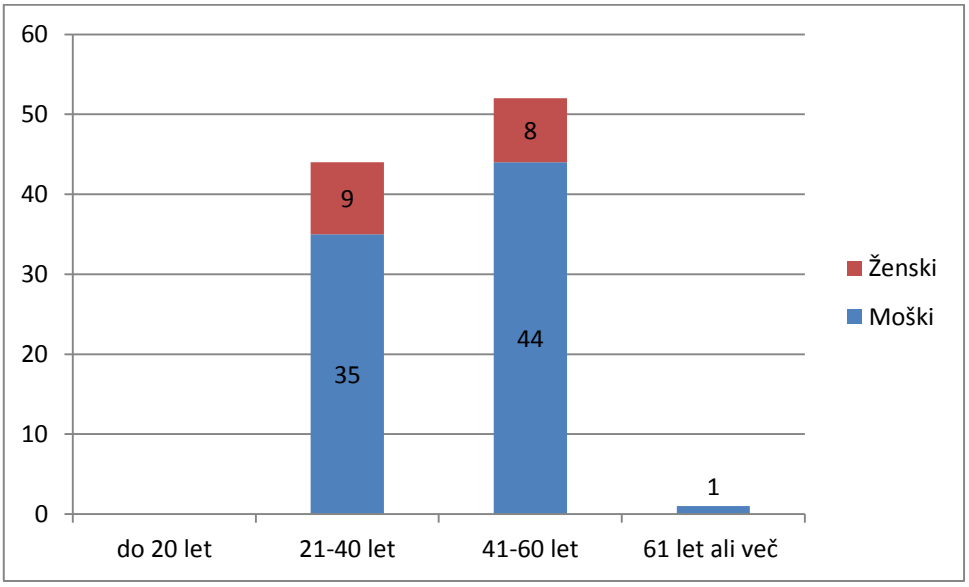
Slika 16: Odgovor na vprašanje 1: Spol

Na sliki 17 je prikazana starost skrbnikov na VIZ, ki so sodelovali v anketi.



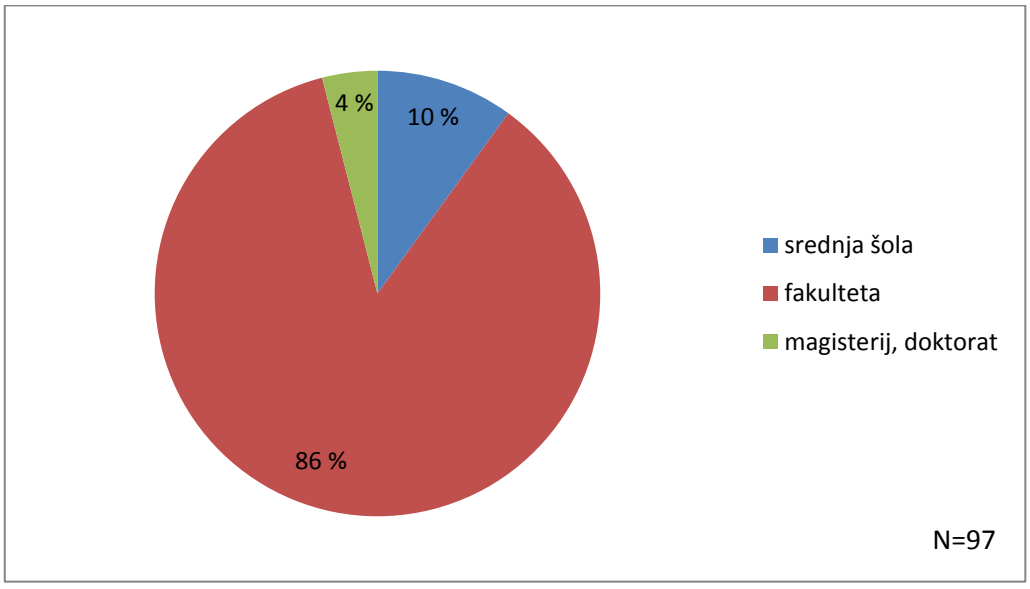
Slika 17: Odgovor na vprašanje 2: V katero starostno skupino spadate?

Anketa je pokazala, da je večina anketiranih skrbnikov informacijskega sistema na VIZ v starostni skupini med 41 in 60 let (slika 17). S slike 18 je razvidno, da največ anketiranih moških skrbnikov spada v starostno skupino med 41 in 60 let, medtem ko je žensk največ v skupini med 21 in 40 let.



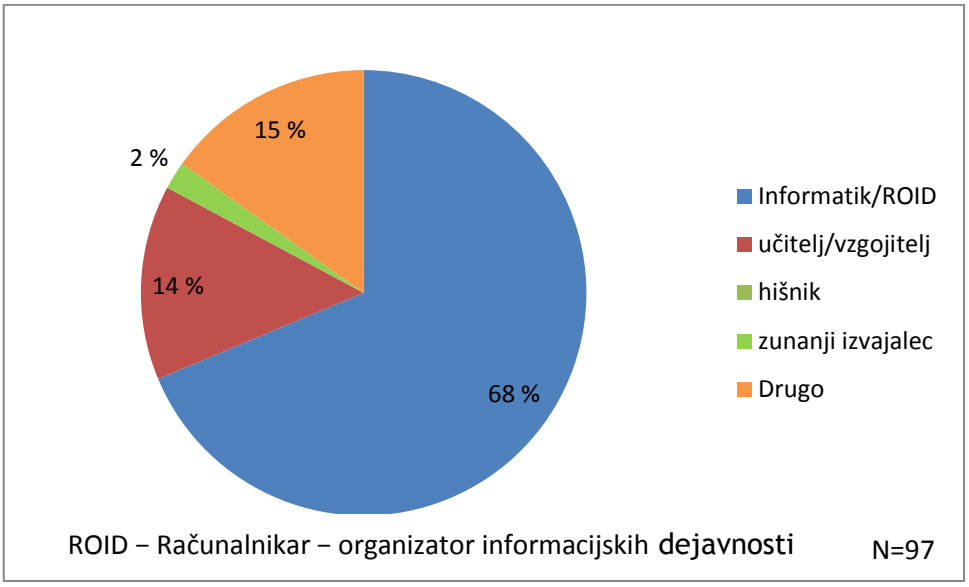
Slika 18: Starostna struktura skrbnikov glede na spol na VIZ

V nadaljevanju je sledilo vprašanje o stopnji izobrazbe, katerega odgovore prikazuje slika 19. Izkazalo se je, da ima večina (86 %) fakultetno izobrazbo, medtem ko imajo magisterij ali doktorat samo 4 %, srednjo šolo pa 10 %.



Slika 19: Odgovor na vprašanje 3: Kakšna je vaša stopnja izobrazbe?

S slike 20 je razvidno, da je delovno mesto večine skrbnikov (68 %), ki so sodelovali v anketi, informatik. Ta rezultat je presenetljiv, glede na to, da sistematizacija delovnega mesta skrbnik informacijskega sistema na VIZ ni urejena.

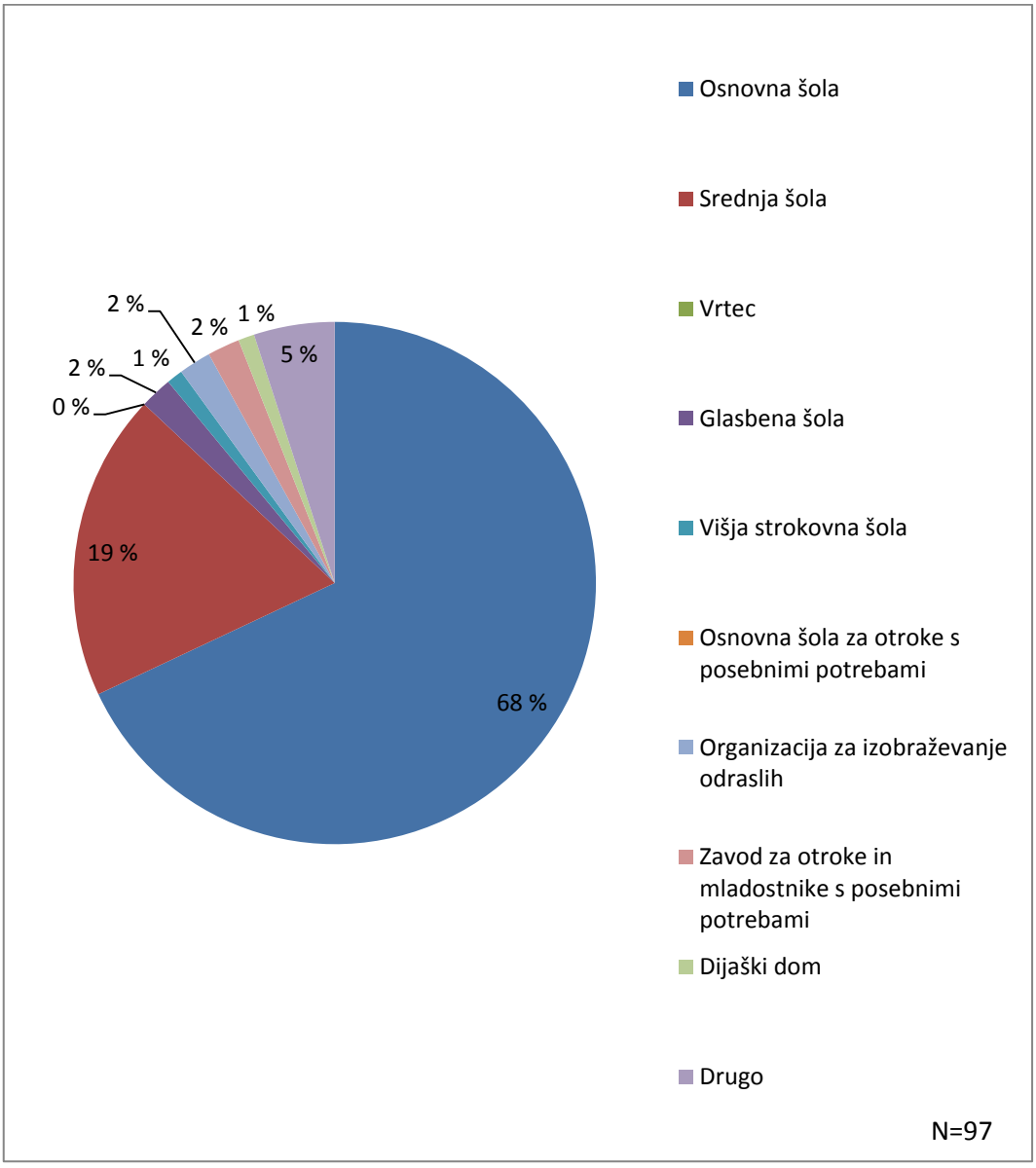


Slika 20: Odgovor na vprašanje 4: Kakšno je vaše delovno mesto?

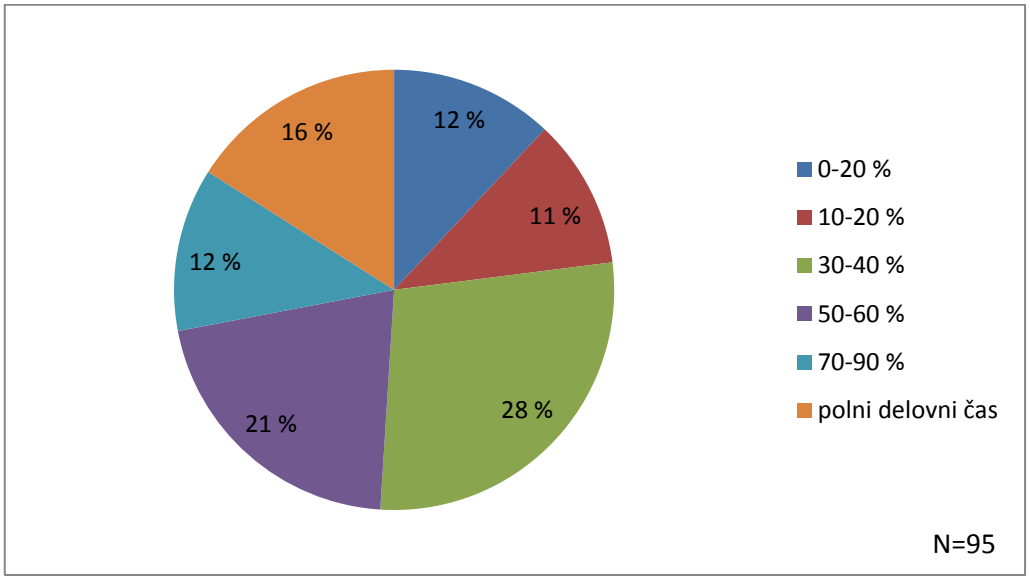
Kot drugo (15 %) so sodelujoči v anketi navedli naslednja delovna mesta: vzdrževalec računalniške mreže, učiteljica in roid, vzdrževalec učne tehnologije, roid in učitelj, ROID in učiteljica računalništva, učitelj in roid, organizator izobraževanja, ikt vzdrževalec, ravnatelj, predavatelj, asistent z doktoratom, pomočnica ravnatelja.

Večina (68 %) v anketi sodelujočih skrbnikov je zaposlenih na osnovnih šolah, kar prikazuje tudi slika 21.

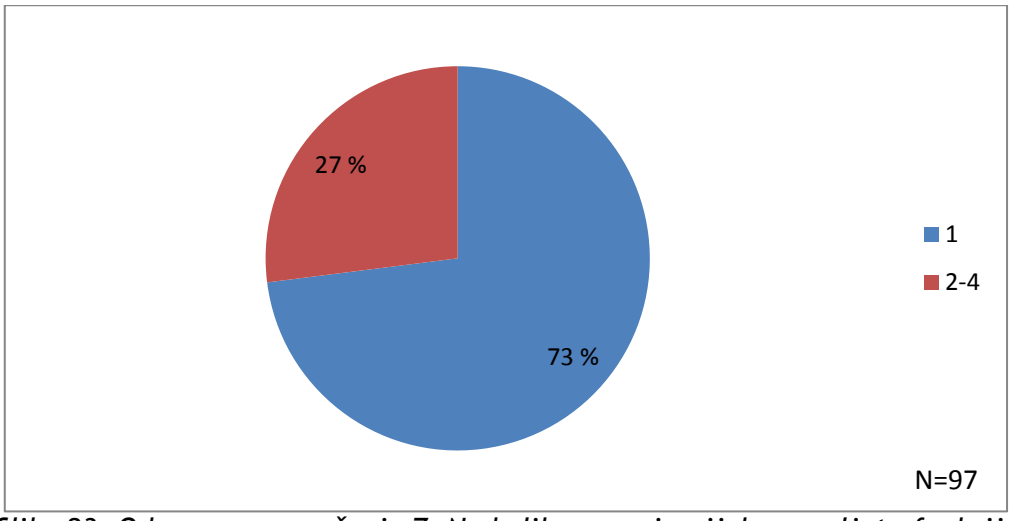
Večina skrbnikov, ki so sodelovali v raziskavi, opravlja to delo samo kot dopolnilno dejavnost. Samo 16 % skrbnikov, ki so sodelovali v raziskavi, opravlja to delo za polni delovni čas, večinoma to delo predstavlja 30–40 % njihovega delovnega časa (slika 22). Večina, 73 %, opravlja delo na enem VIZ (slika 23). Slika 24 prikazuje delež zaposlitve anketiranega skrbnika glede na tip VIZ. Največ zaposlenih za polni delovni čas je tako na anketiranih srednjim šolah, nekaj pa jih je še na anketiranih osnovnih šolah in drugi VIZ.



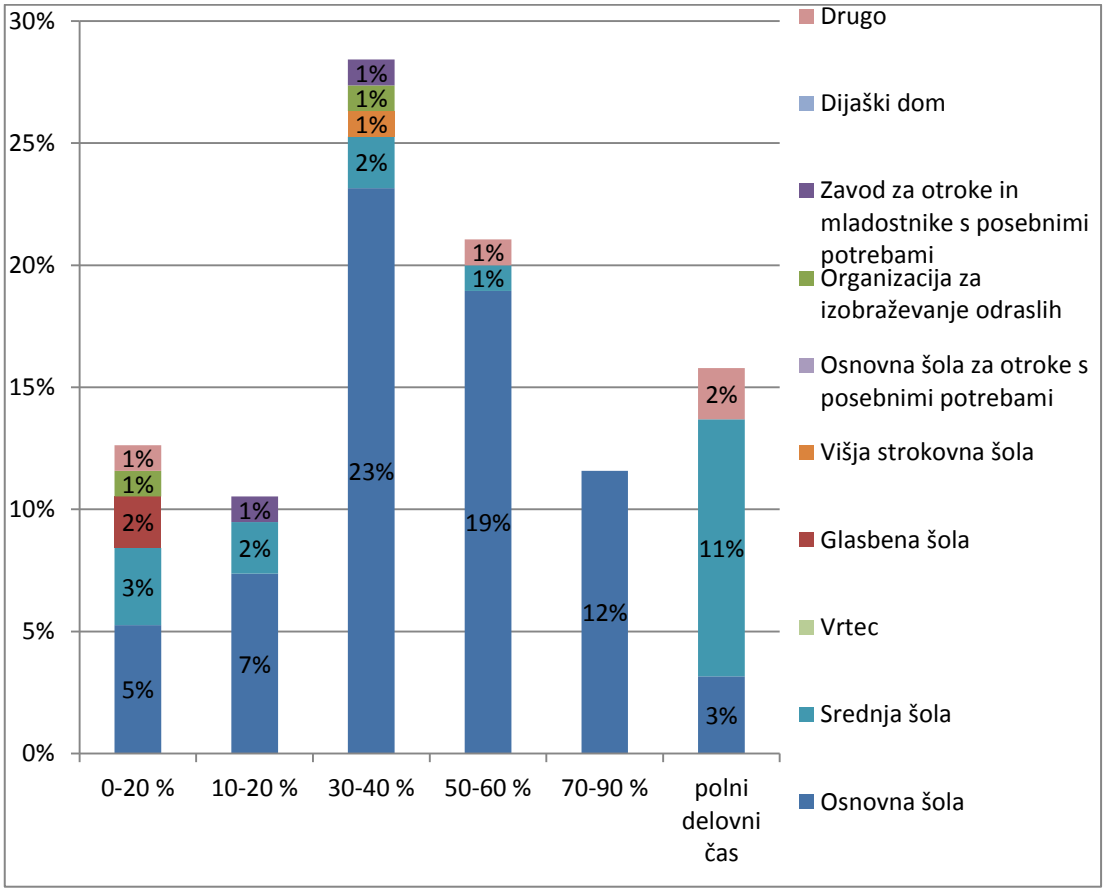
Slika 21: Odgovor na vprašanje 5: Tip organizacije, kjer ste zaposleni?



Slika 22: Odgovor na vprašanje 6: Koliko % delovnega časa ste zaposleni kot skrbnik informacijskega sistema (računalnikar)?

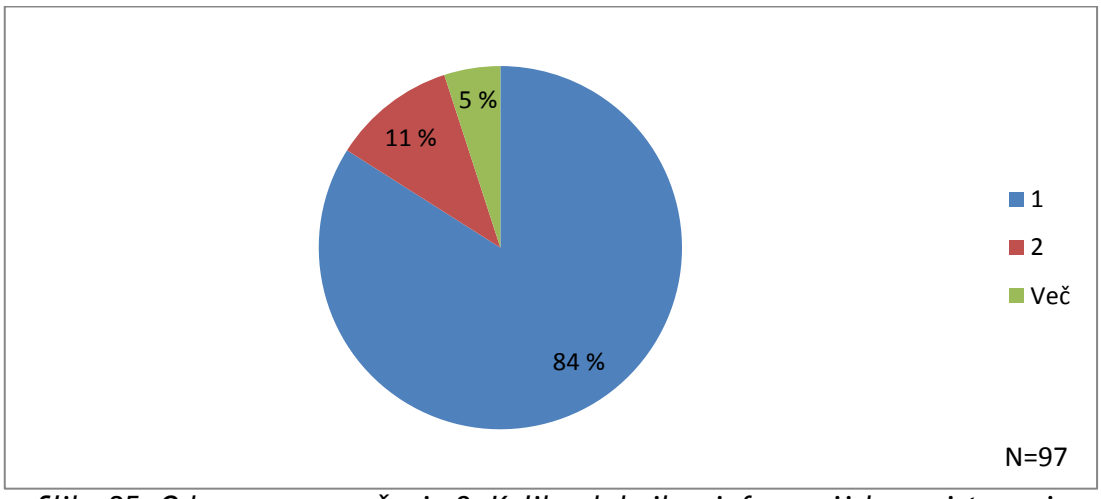


Slika 23: Odgovor na vprašanje 7: Na koliko organizacijah opravljate funkcijo skrbnika sistema?



Slika 24: Delež zaposlitve kot skrbnik računalniške sistema glede na tip VIZ

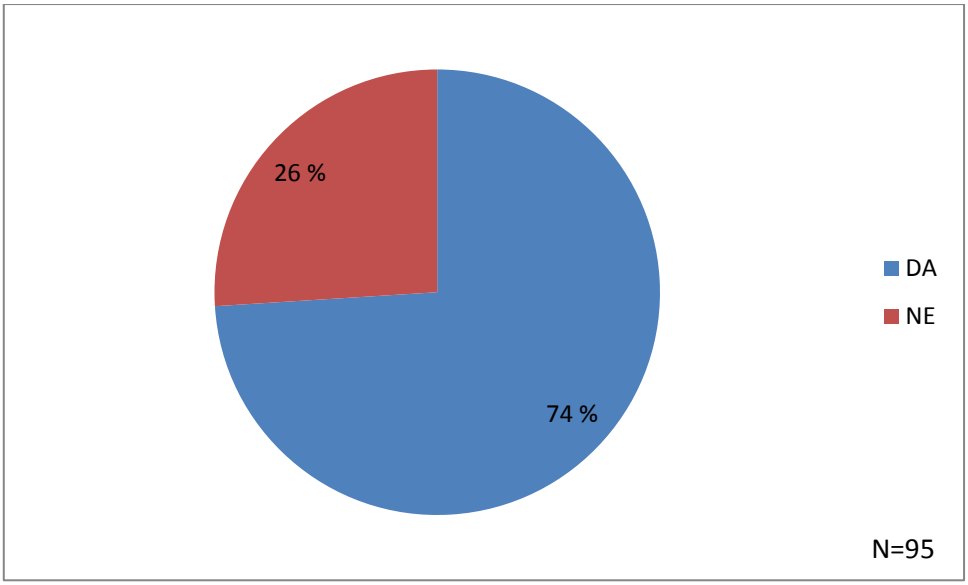
Slika 25 prikazuje, da imajo VIZ, ki so sodelovali v anketi, le enega skrbnika informacijskega sistema.



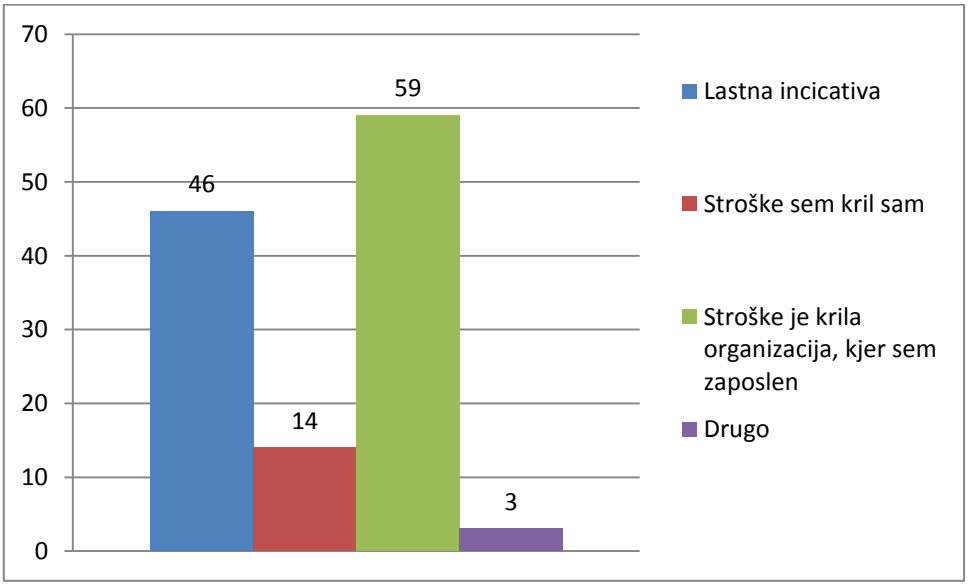
Slika 25: Odgovor na vprašanje 8: Koliko skrbnikov informacijskega sistema je zaposlenih na vaši organizaciji?

Anketa je pokazala, da so se anketiranci izobraževali s področja informacijskih tehnologij in/ali zagotavljanja informacijske varnosti. Slika 26 prikazuje, da se jih je 74 % odstotkov izobraževalo v času, odkar jim je bila zaupana vloga skrbnika

informacijskega sistema. Velika večina se je za izobraževanje odločila samo-iniciativno. Pri tem jih je podpiralo tudi vodstvo, saj jim je krilo stroške izobraževanja (slika 27).



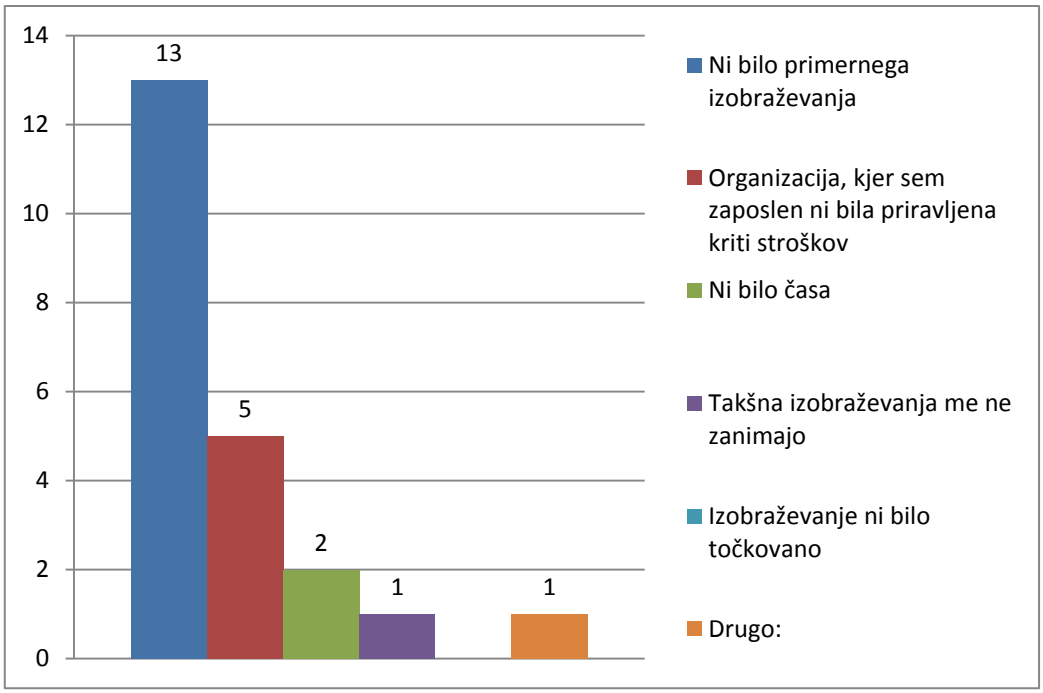
Slika 26: Odgovor na vprašanje 9: Ali ste se v času, odkar vam je bila zaupana vloga skrbnika informacijskega sistema, izobraževali na temo informacijskih tehnologij in/ali zagotavljanja informacijske varnosti?



Slika 27: Odgovor na vprašanje 10: Ali ste se izobraževanja udeležili na lastno iniciativo in/ali stroške ali je za to poskrbela organizacija, kjer ste zaposleni? (Možnih več odgovorov)

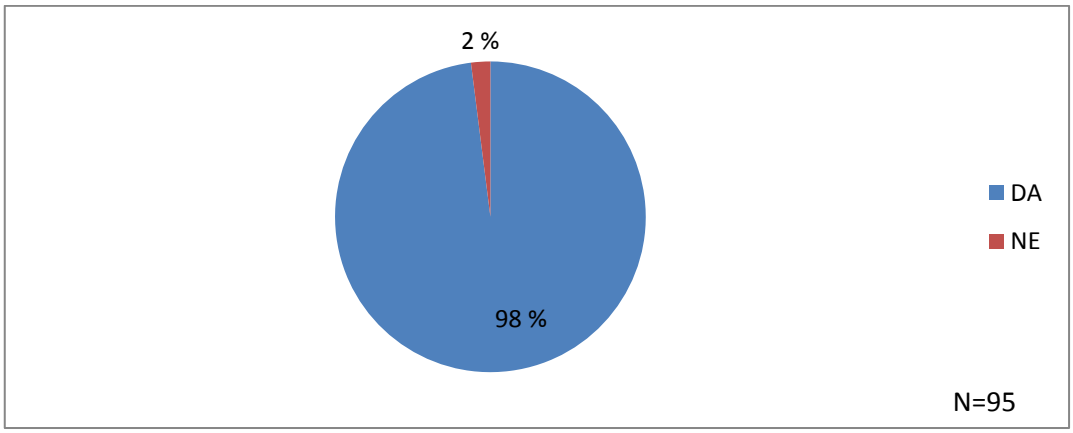
Kot drugo se je eden izmed skrbnikov, sodelujočih v raziskavi, poleg izobraževanja, ki mu ga je kril VIZ, udeležil izobraževanja v lastni režiji. Medtem ko je eden navedel, da se je udeležil brezplačnega izobraževanja.

Slika 28 prikazuje, zakaj se skrbniki, ki so sodelovali v raziskavi, niso udeležili izobraževanja.



Slika 28: Odgovor na vprašanje 11: Zakaj se izobraževanja niste udeležili? (Možnih več odgovorov)

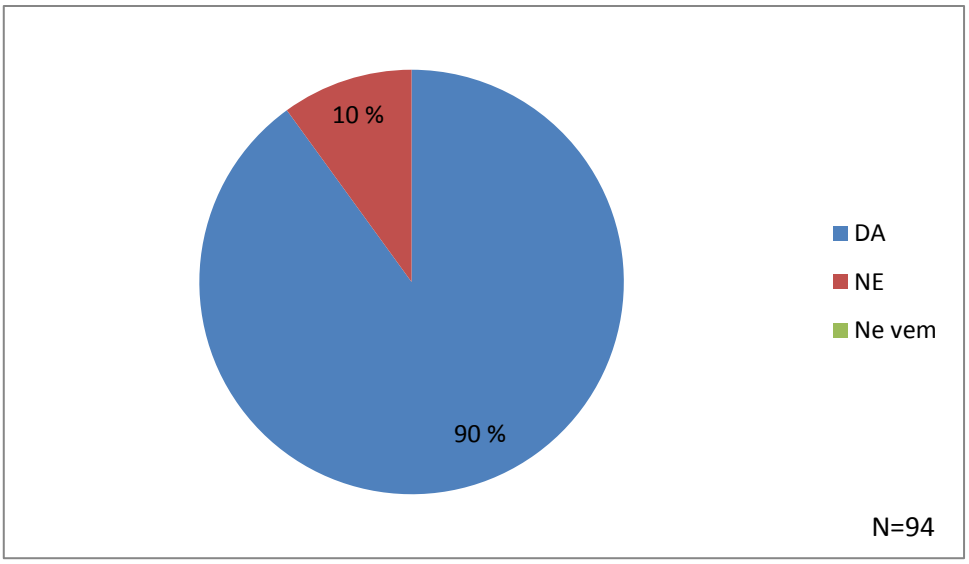
Med drugim je eden izmed anketirancev navedel, da mu ni bilo ponujeno.
Slika 29 prikazuje, da se je velika večina anketirancev pripravljena izobraževanja udeležiti, čeprav za to niso nagrajeni. Kar 98 % jih je odgovorilo, da so se izobraževanja pripravljeni udeležiti, čeprav le-to ni točkovano.



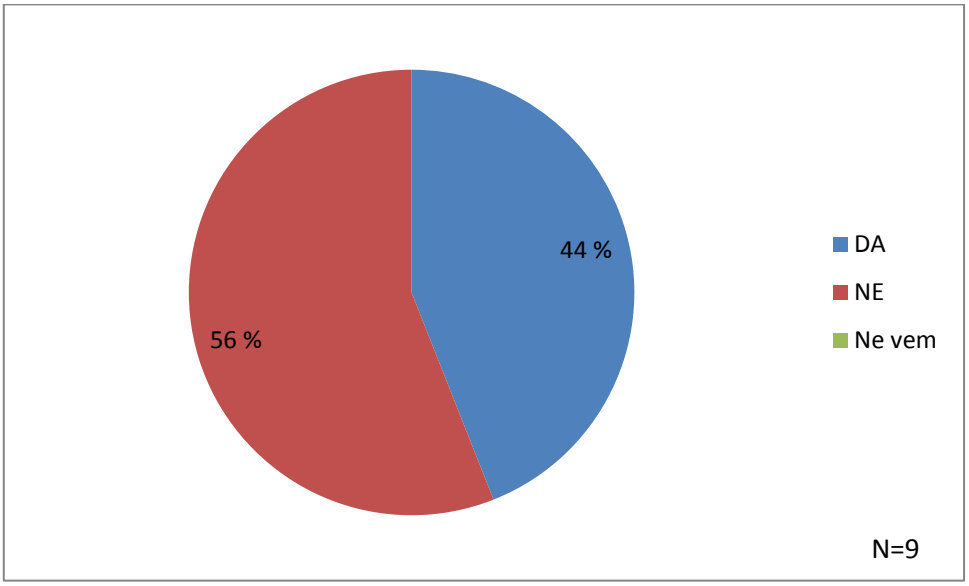
Slika 29: Odgovor na vprašanje 12: Ali bi se izobraževanja na temo informacijskih tehnologij udeležili, čeprav le-to ne bi bilo točkovano?

Sledila so vprašanja o omrežju na VIZ. Slika 30 prikazuje, da ima večina VIZ, ki so sodelovali v raziskavi, povezavo v omrežje ARNES, kjer je omrežje tudi ločeno na administrativni in pedagoški del. Na vprašanje 14 so odgovarjali tisti, ki so pri

vprašanju 13 izbrali, da nimajo povezave v omrežje ARNES. Slika 31 prikazuje, da večina tistih (55 %), ki nimajo povezave v omrežje ARNES, te ločitve nima.

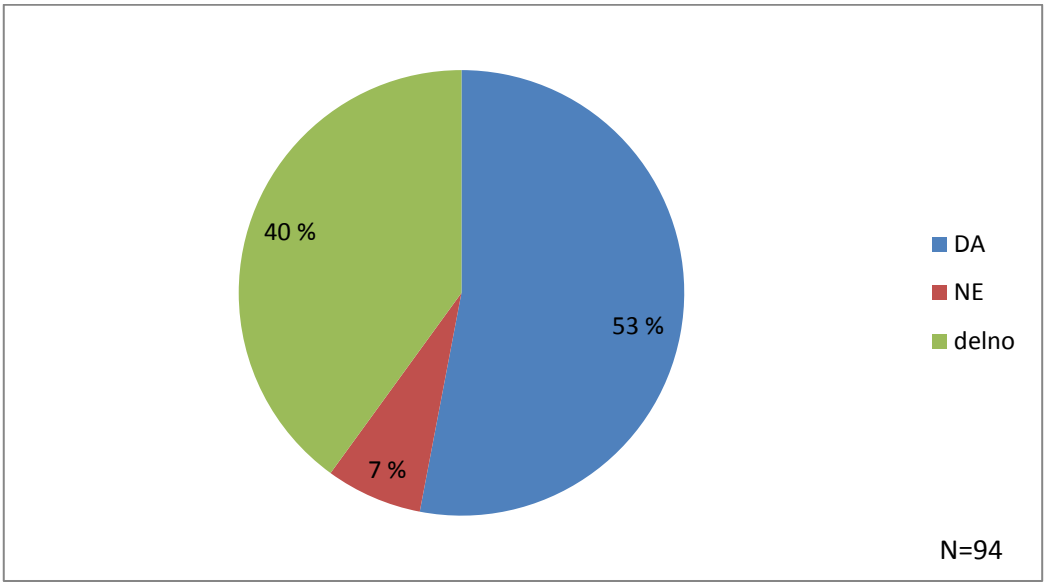


Slika 30: Odgovor na vprašanje 13: Ali je omrežje, za katerega skrbite, povezano v omrežje ARNES?



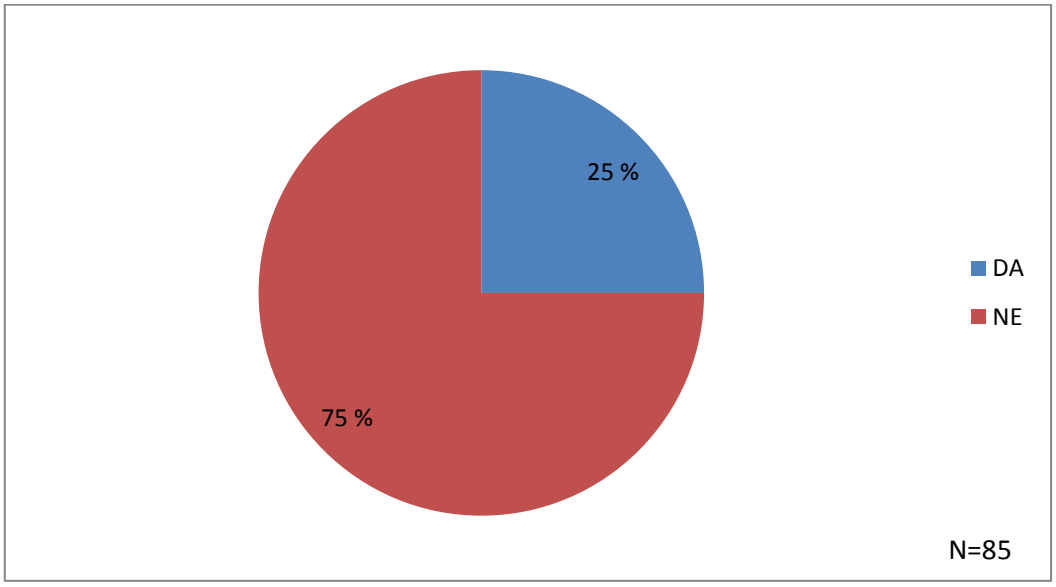
Slika 31: Odgovor na vprašanje 14: Ali je omrežje, za katerega skrbite, ločeno na pedagoški in administrativni del?

Izkazalo se je, da anektirani VIZ vsaj delno vodijo dokumentacijo o omrežju (stanje filtrov, dodeljeni in porabljeni IP naslovi, skica omrežja ...), kar prikazuje tudi slika 32.

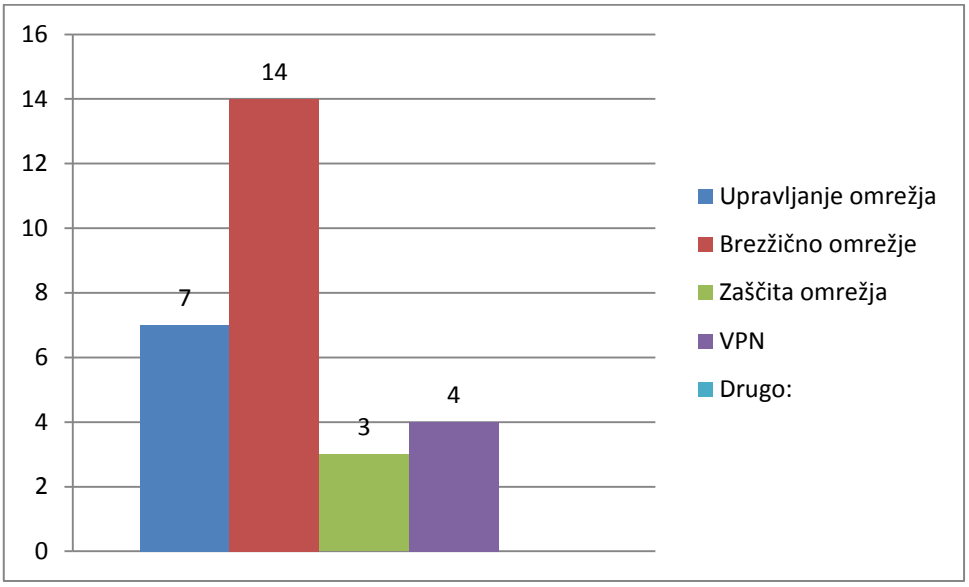


Slika 32: Odgovor na vprašanje 15: Vodite dokumentacijo o omrežju na vaši organizaciji (stanje filtrov, dodeljeni in porabljeni IP naslovi, skica omrežja ...)?

Slika 33 prikazuje, da ima 25 % anketiranih VIZ za usmerjevalnikom, ki ga upravlja Arnes, postavljen še svoj usmerjevalnik, katerega funkcija je na 14 VIZ zagotavljanje brezžičnega omrežja (slika 34). Preostale funkcije so prikazane na sliki 34. Na vprašanje 17 so odgovarjali samo anketiranci, ki so pri vprašanju 16 odgovorili DA.

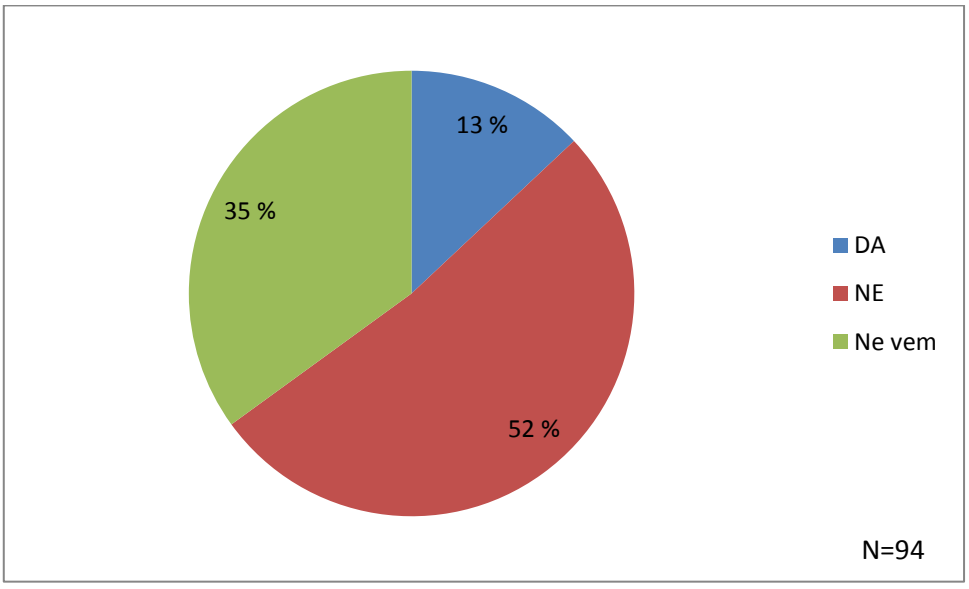


Slika 33: Odgovor na vprašanje 16: Imate za usmerjevalnikom, ki ga upravlja Arnes, postavljen še svoj usmerjevalnik?

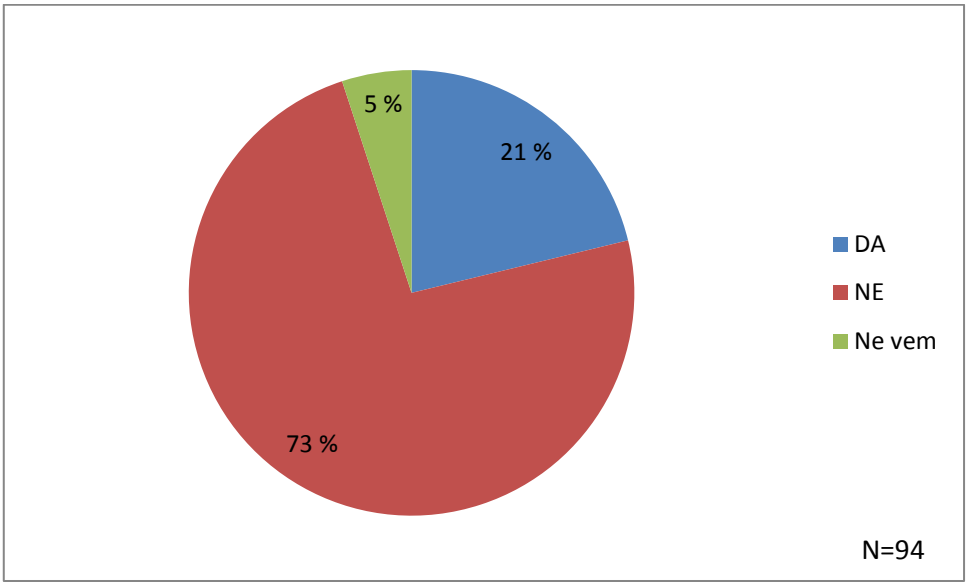


Slika 34: Odgovor na vprašanje 17: Kakšna je funkcija tega usmerjevalnika? (Možnih več odgovorov)

13 % VIZ uporablja NAT/PAT (slika 35), 21 % jih ima, poleg zaščite na usmerjevalniku, ki ga upravlja Arnes, postavljen še lastni požarni zid (slika 36).

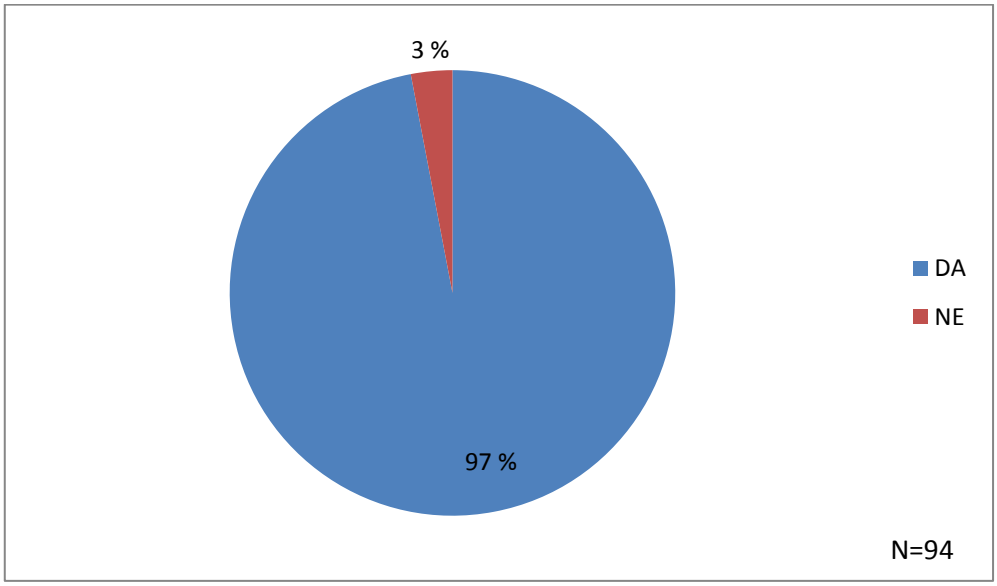


Slika 35: Odgovor na vprašanje 18: Uporabljate NAT/PAT?



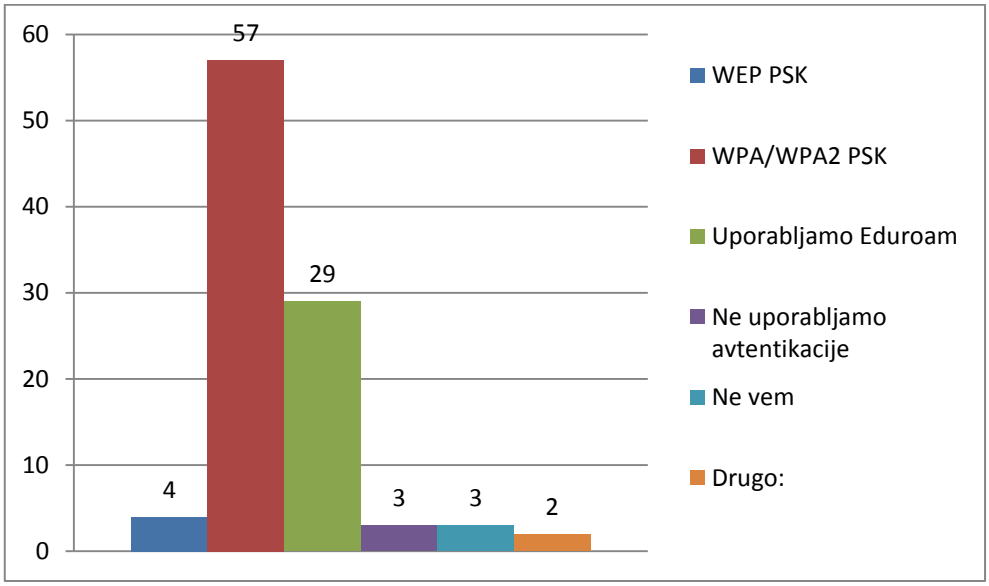
Slika 36: Odgovor na vprašanje19: Imate postavljen svoj požarni zid (poleg zaščite na usmerjevalniku)?

Na VIZ poleg osebnih računalnikov, ki so fizično povezani v računalniško omrežje, uporabljajo še prenosnike, ki so večinoma povezani preko brezžičnega omrežja, tiskalnike, interaktivne table, razne oglasne televizije, sisteme za nadzor proizvodnje električne energije iz sončnih elektrarn idr. S slike 37 je razvidno, da ima 97 % anketiranih VIZ postavljeno brezžično omrežje.



Slika 37: Odgovor na vprašanje 20: Imate v organizaciji vzpostavljeno brezžično omrežje?

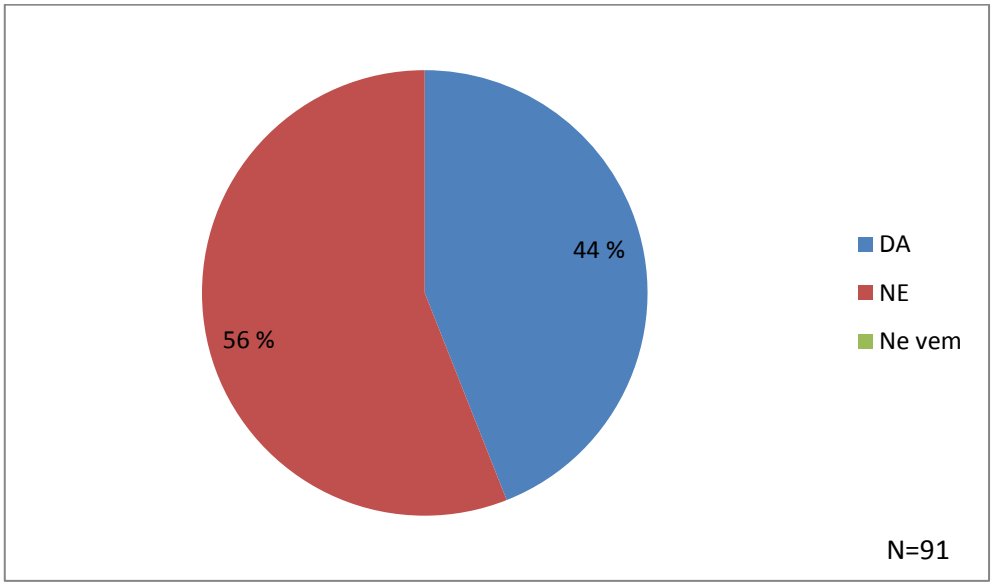
Slika 38 prikazuje Wifi varnostne protokole, ki jih anketirani VIZ na teh omrežjih uporabljajo.



Slika 38: Odgovor na vprašanje 21: Kakšno avtentikacijo za brezžično omrežje uporabljate? (Možnih je več odgovorov)

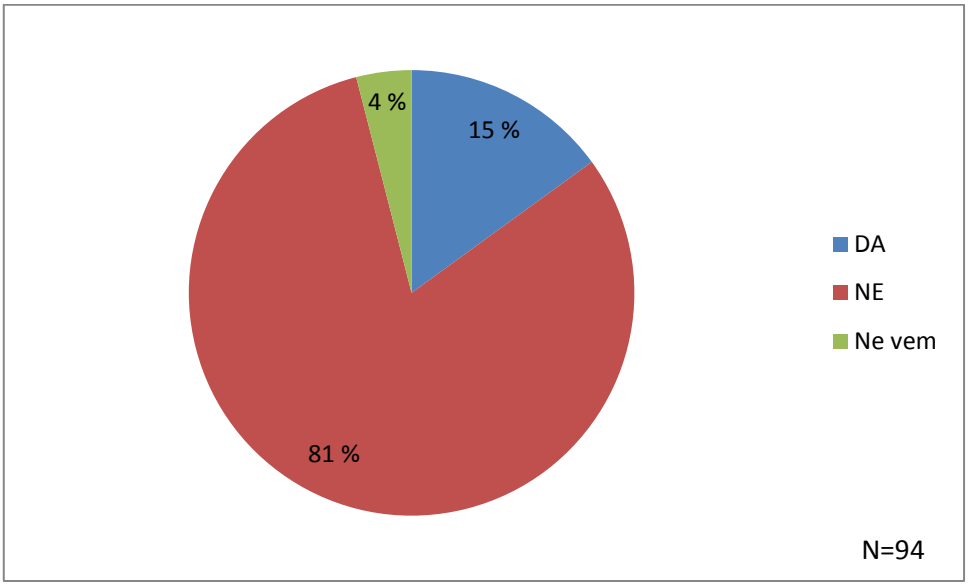
Eden izmed anketirancev je navedel, da pripravljajo omrežje Eduroam, in drug, da uporabljajo mono wall.

Slika 39 prikazuje, da ima skoraj polovica sodelujočih VIZ brezžično omrežje za goste v ločenem podomrežju.

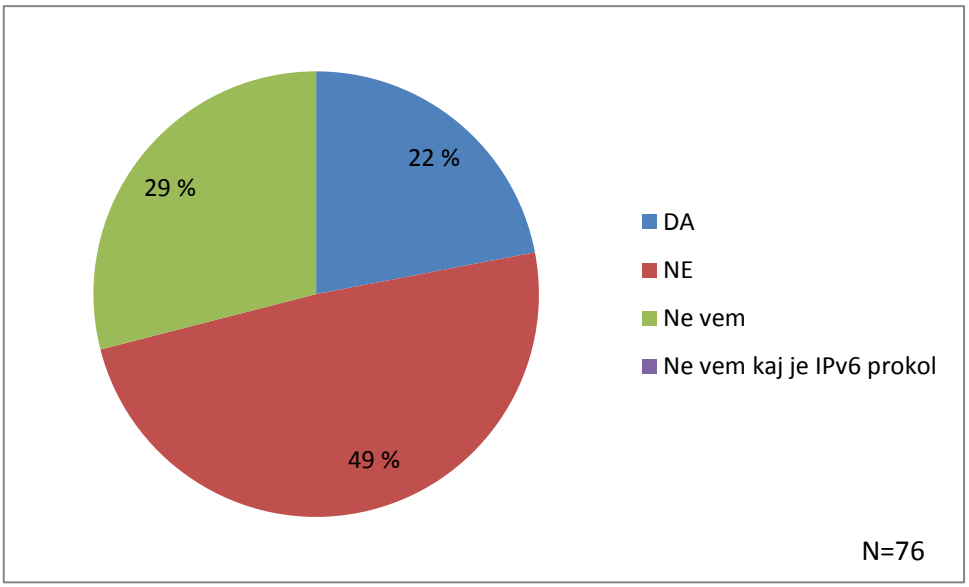


Slika 39: Odgovor na vprašanje 22: Imate brezžično omrežje za goste v ločenem podomrežju?

Sledili sta dve vprašanji o IPv6 protokolu, katerega uporablja 15 % anketiranih VIZ (slika 40), čeprav ima večina VIZ, povezanih v omrežje ARNES, možnost uporabe IPv6 protokola. Slika 41 prikazuje, ali imajo tisti, ki uporabljajo IPv6 protokol, izklopljene translacijske mehanizme (Terredo, 6 to 4 …).

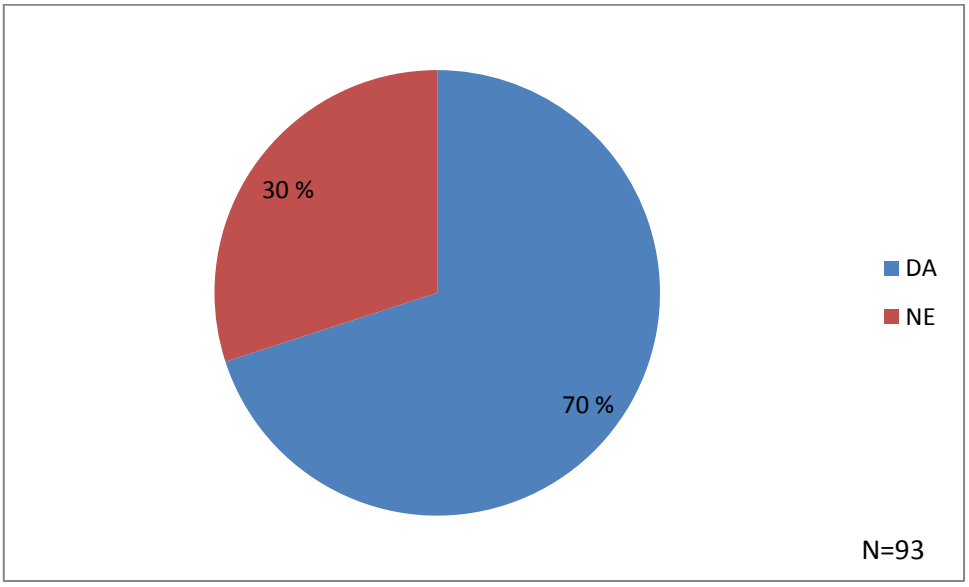


Slika 40: Odgovor na vprašanje 23: Uporabljate IPv6 protokol?



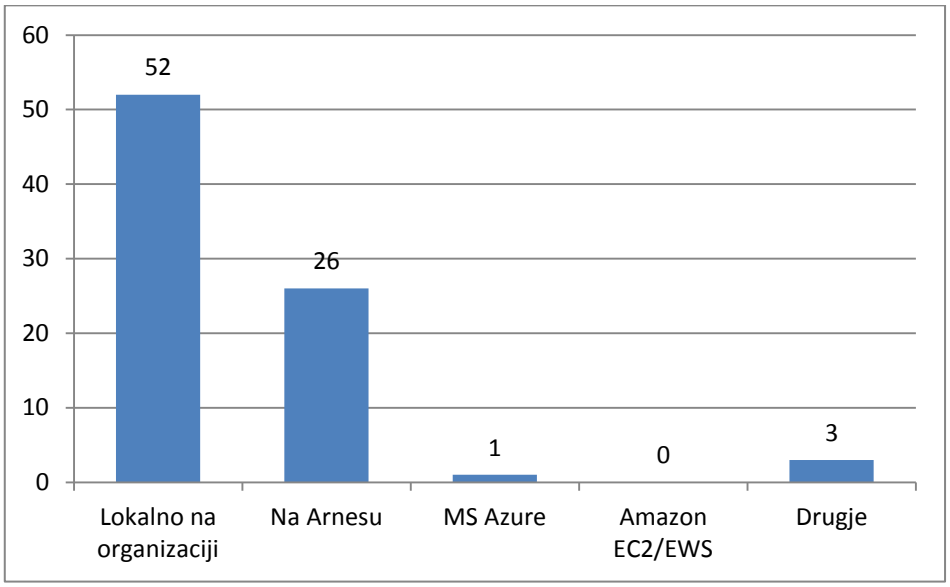
Slika 41: Odgovor na vprašanje 24: Imate na operacijskih sistemih Windows Vista in novejših izklopljene IPv6 translacijske mehanizme?

V nadaljevanju so anketiranci odgovarjali na vprašanja o strežnikih. Kar 70 % anketiranih VIZ ima postavljen strežnik (slika 42).



Slika 42: Odgovor na vprašanje 16: Ima vaša organizacija postavljen strežnik?

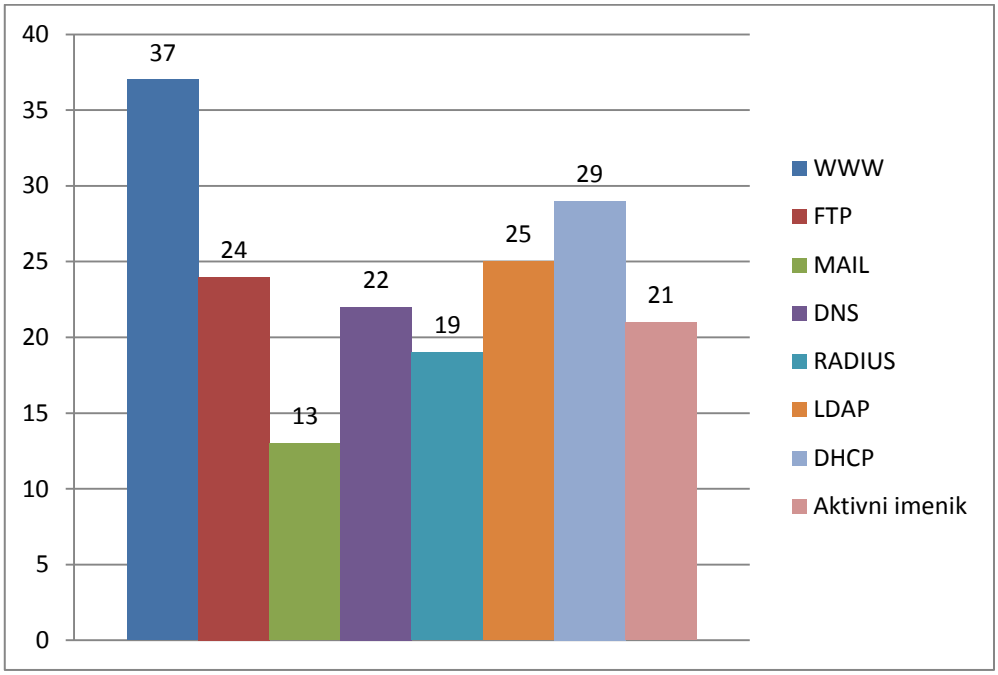
Slika 43 prikazuje, da imajo anketirani VIZ strežnik običajno postavljen kar v svojem omrežju.



Slika 43: Kje ima vaša organizacija postavljen strežnik? (Možnih več odgovorov)

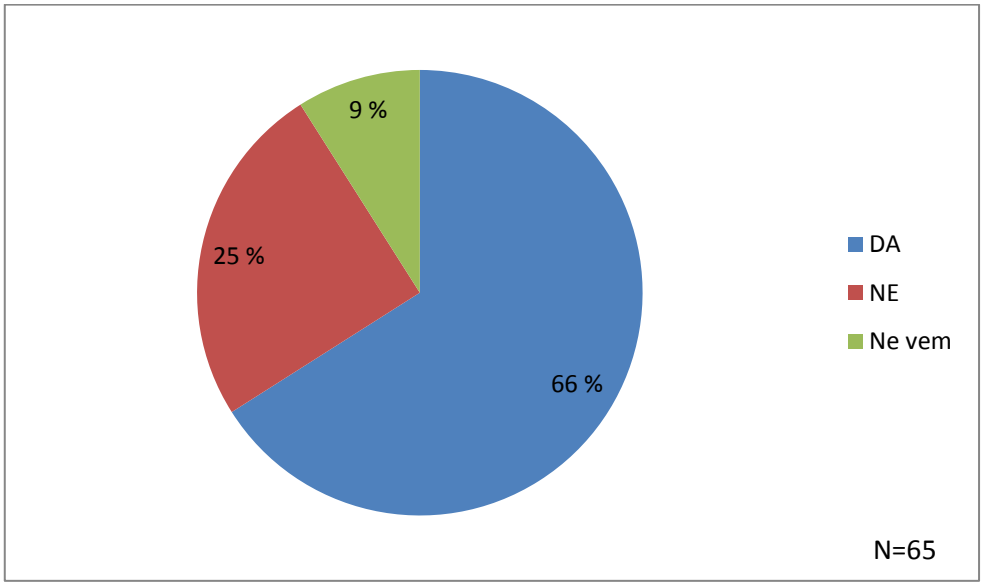
V nasprotju z vsemi, ki imajo strežnik postavljen na VIZ, je eden izmed anketirancev odgovoril, da imajo strežnik postavljen samo za potrebe administracije, 2 od anketiranih VIZ pa imata strežnik postavljen v okviru kampusa.

Slika 44 prikazuje storitve, ki tečejo na teh strežnikih. Večinoma na teh strežnikih tečejo storitve WWW strežnika.



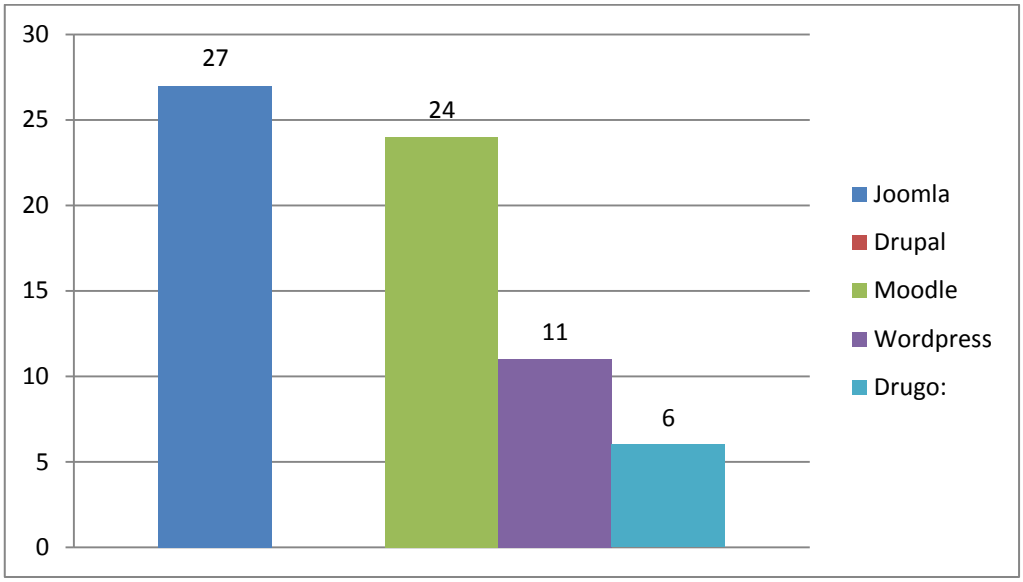
Slika 44: Odgovor na vprašanje 27: Na strežniku tečejo naslednje storitve (Možnih več odgovorov)

Na VIZ veliko uporabljajo tudi sisteme za upravljanje vsebin (CMS), saj je na vprašanje, ali uporabljate sistem za upravljanje z vsebinami, kar 66 % anketirancev odgovorilo z DA, 9 % jih ne ve, preostalih 25 % jih ne uporablja (slika 45).



Slika 45: Odgovor na vprašanje 28: Uporabljate sistem za upravljanje z vsebinami (CMS)?

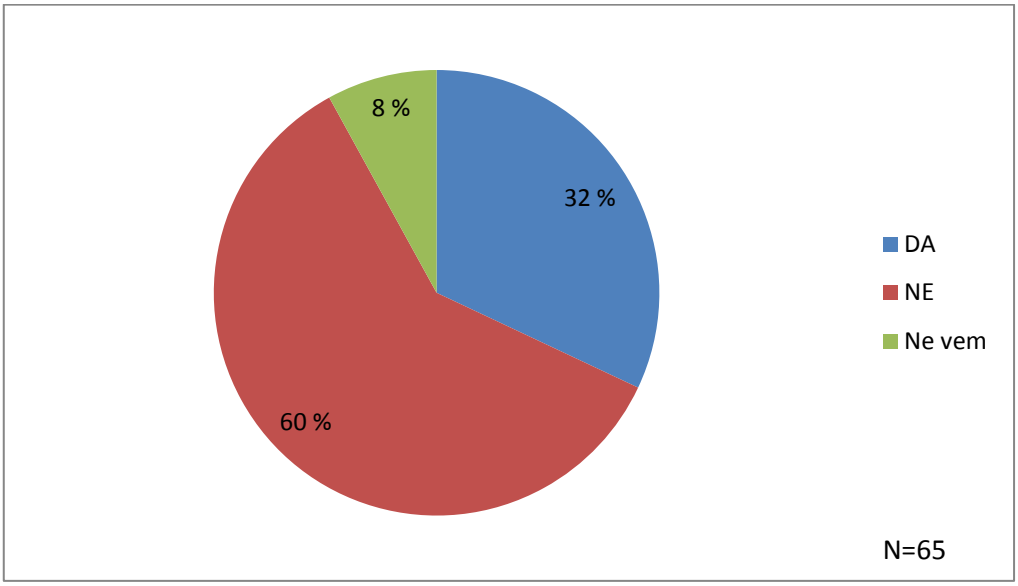
Slika 46 prikazuje, da sta med sistemi za upravljanje z vsebinami običajno v uporabi Joomla in Moodle.



Slika 46: Odgovor na vprašanje 29: Kateri strežnika za upravljanje vsebin (CMS) uporabljate? (Možnih več odgovorov)

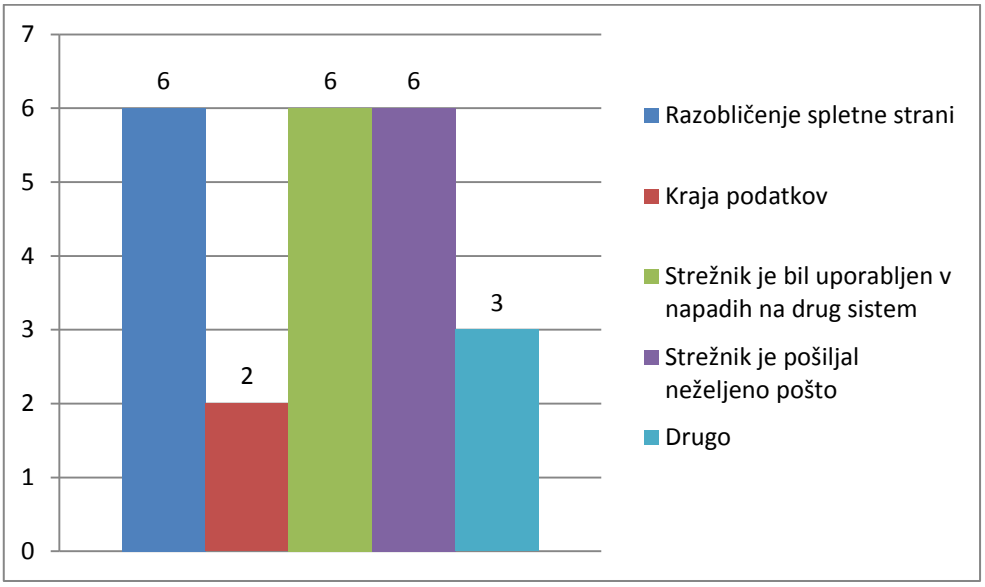
Kot drugo so navedli: cmsmadesimple, myportal, sharepoint, typo3 neos – uvajamo, concrete5.

Sledila so vprašanja o varnosti na aplikacijski plasti. Vdor v strežnik je imelo že 32 % anketiranih VIZ, 8 % jih ne ve, preostali vdora še niso zabeležili (slika 47).



Slika 47: Odgovor na vprašanje 30: Ali ste že imeli vdor v sistem (strežnik)?

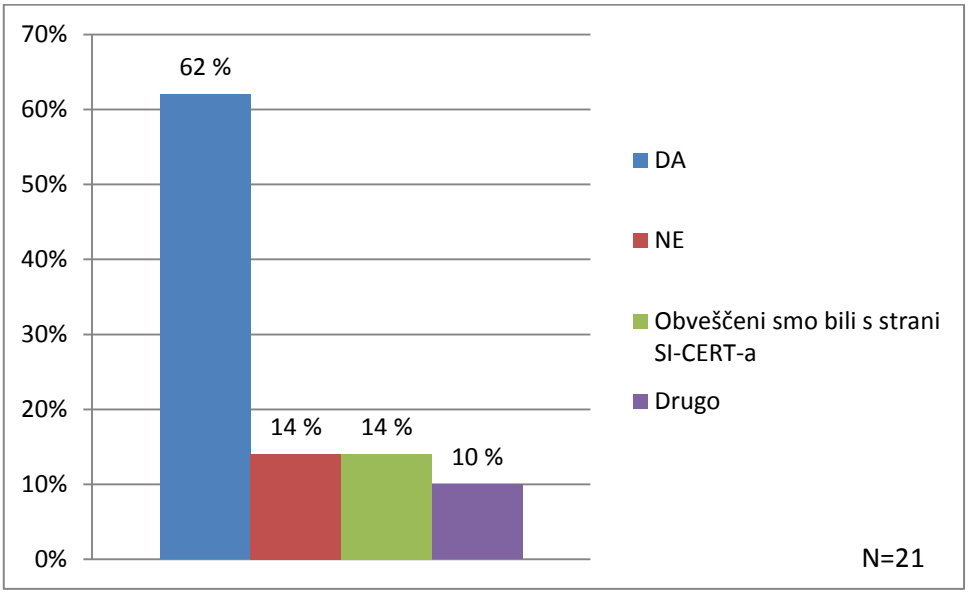
Slika 48 prikazuje posledice vdora na anketiranih VIZ. Večinoma je bila posledica razobličenje spletne strani ali pa je bil strežnik uporabljen v napadih na druge sisteme.



Slika 48: Odgovor na vprašanje 31: Kaj je bila posledica vdora? (Možnih več odgovorov)

Kot drugo so navedli: uporabili so ga za igralniški strežnik, arhiviranje piratskih filmov, se ne spomnim točno in nič opaznega.

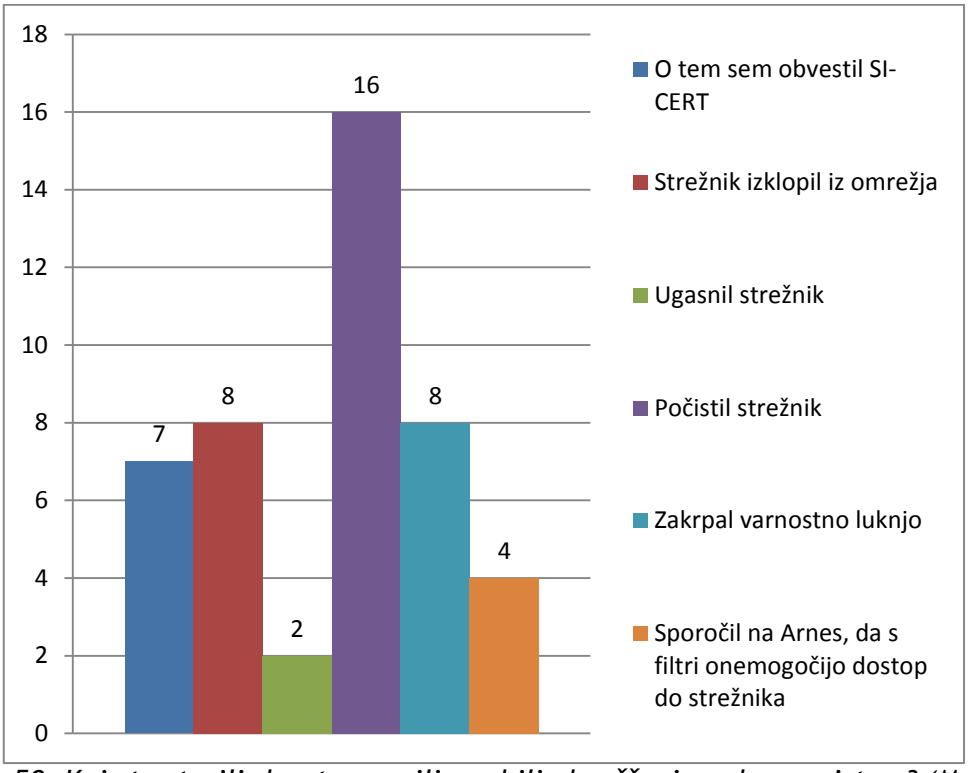
Slika 49 prikazuje, ali so vdor zaznali sami oz. jih je kdo o tem obvestil. Kar v 62 % anketiranih VIZ so vdor zaznali sami.



Slika 49: Odgovor na vprašanje 32: Ste vdor v sistem zaznali sami?

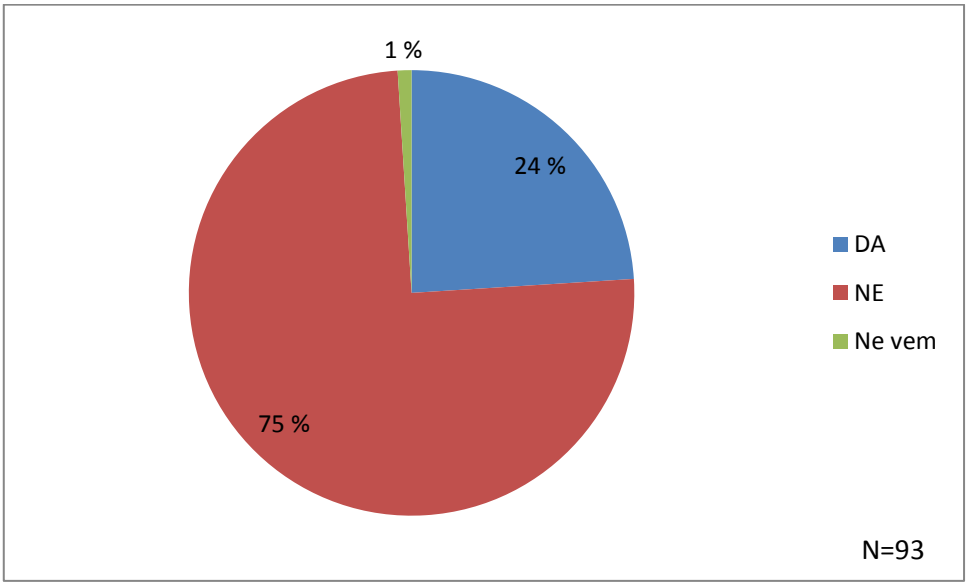
Kot drugo so navedli: enkrat sam, drugič ne, s pomočjo Advant-a.

Slika 50 prikazuje odgovore na vprašanje, kaj ste storili, ko ste opazili oz. bili obveščeni o vdoru v sistem. Kar 16 anketiranih skrbnikov, ki so ogovorili na vprašanje, je med drugim s strežnika odstranilo škodljivo kodo.

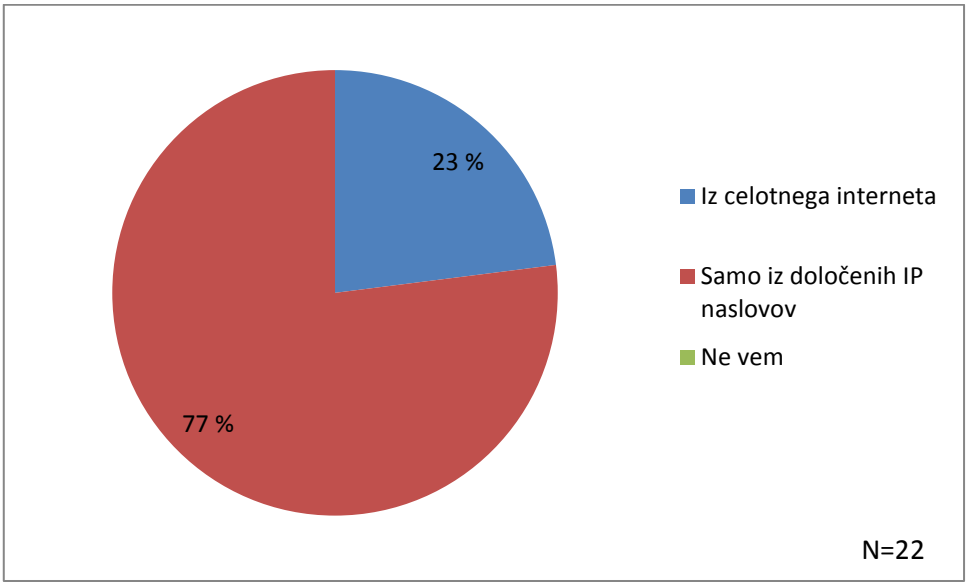


Slika 50: Kaj ste storili, ko ste opazili oz. bili obveščeni o vdoru v sistem? (Možnih več odgovorov)

V nadaljevanju je anketa pokazala, da na večini anketiranih VIZ ne uporabljajo oddaljenega dostopa do službenih računalnikov. Namreč kar 75 % jih je odgovorilo, da ne (slika 51). Tisti, ki to uporabljajo (24 %), imajo večinoma (77 %) dostop omejen samo iz določenih IP naslovov (slika 52).

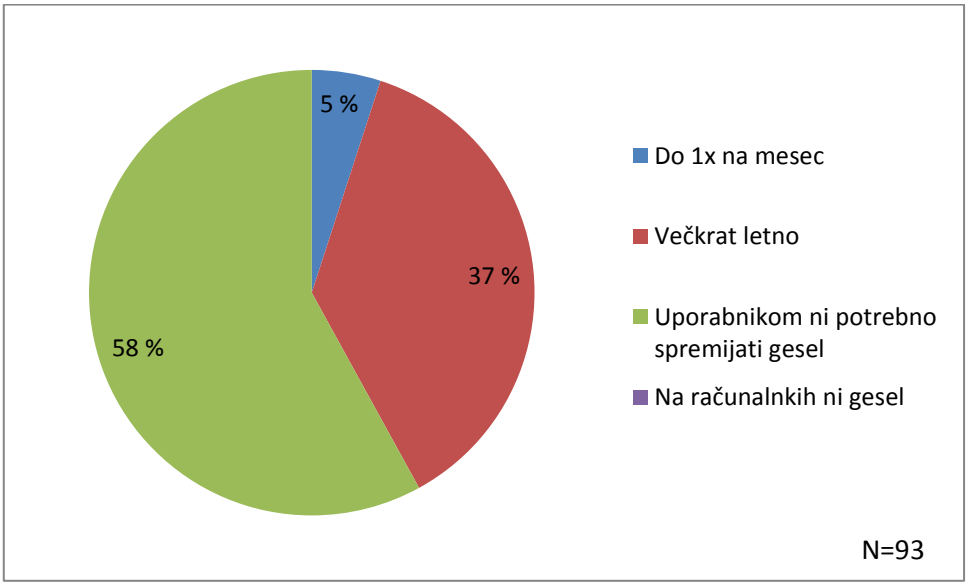


Slika 51: Odgovor na vprašanje 34: Ali zaposleni uporabljajo za dostop do službenih računalnikov oddaljeno namizje (RDP)?



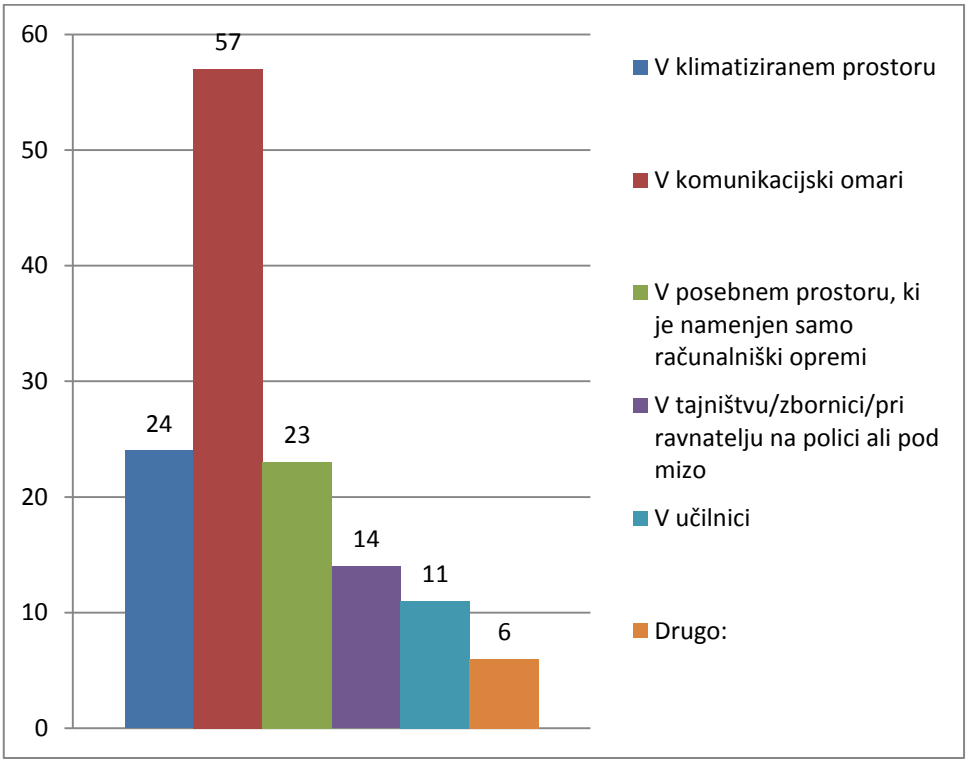
Slika 52: Odgovor na vprašanje 35: Imate omogočen dostop do službenih računalnikov preko oddaljenega namizja (RDP)?

Slika 53 prikazuje, kako pogosto so uporabniki na anketiranih VIZ primorani zamenjati svoje geslo. Anketa je pokazala, da na več kot polovici (59 %) anketiranih VIZ uporabnikom sploh ni potrebno spreminjati gesel na službenih računalnikih.



Slika 53: Odgovor na vprašanje 36: Kakšen je časovni razpon zamenjave osebnih gesel na službenih računalnikih?

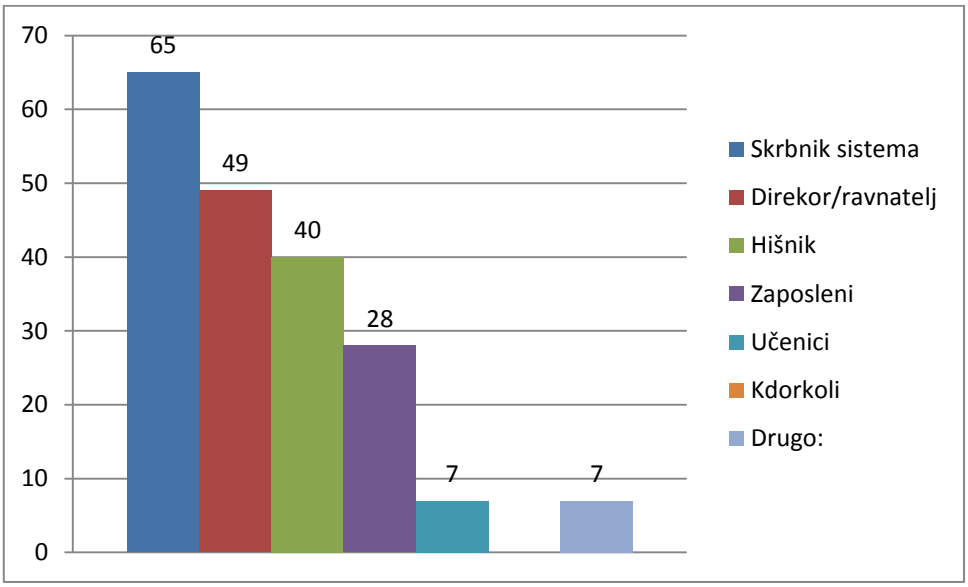
Anketiranci so odgovarjali tudi o fizični varnosti informacijskega sistema. Slika 54 prikazuje, v kakšnem prostoru na anketiranih VIZ hranijo opremo. Večina anketiranih VIZ je odgovorila, da gre to za poseben in klimatiziran prostor, ki je namenjen samo računalniški opremi.



Slika 54: Odgovor na vprašanje 37: Kje se nahaja komunikacijska oprema?(Možnih več odgovorov)

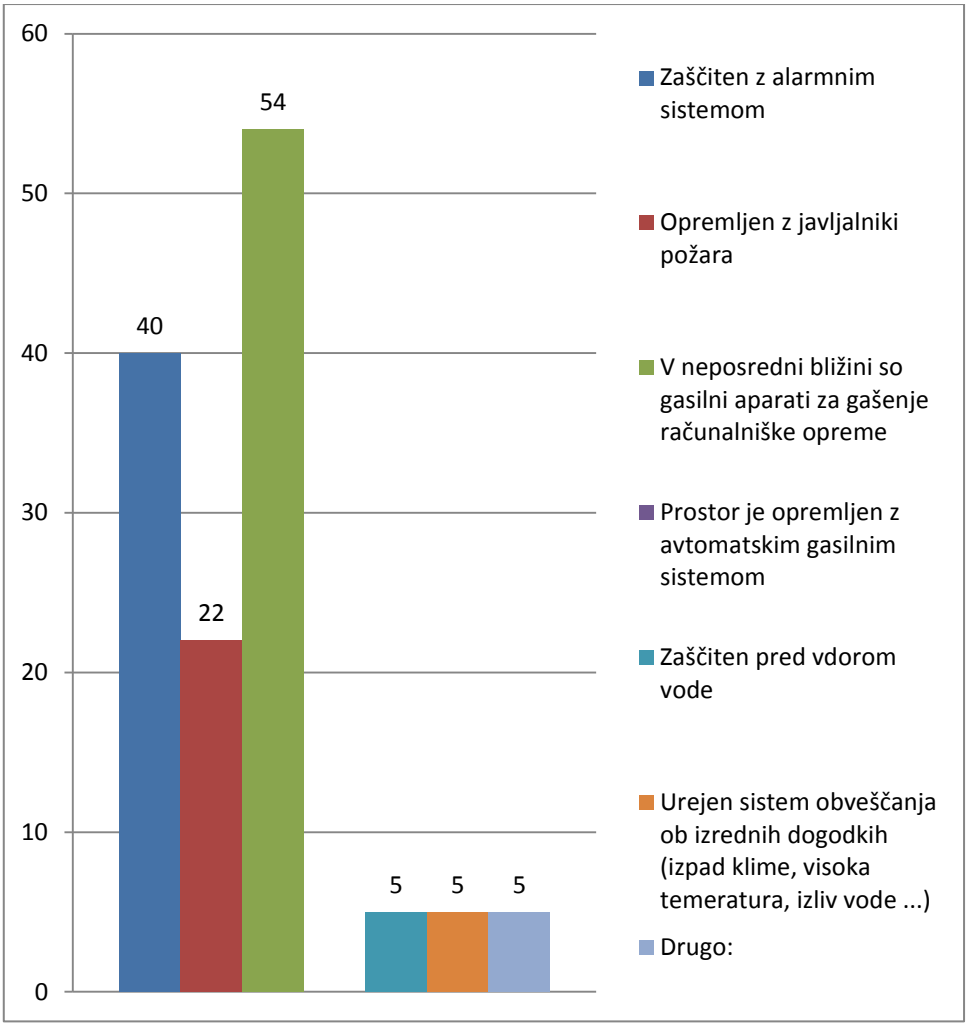
Kot drugo so navedli: večnamenska soba, knjižnica, kabinet, računalniška učilnica, v nočni sobi.

Slika 55 prikazuje, da imata v večini anketiranih VIZ dostop do tega prostora skrbnik informacijskega sistema in direktor/ravnatelj.



Slika 55: Odgovor na vprašanje 38: Kdo ima dostop do prostora, kjer se nahaja komunikacijska oprema? (Možnih več odgovorov)

Kot drugo so navedli: knjižničarka, tajnica, še en učitelj, zunanji sodelavci, delno le ravnateljica in informatik, drugi del je v računalniški učilnici v zaklenjeni kom. omarici, vzdrževalec, IKT vzdrževalec.

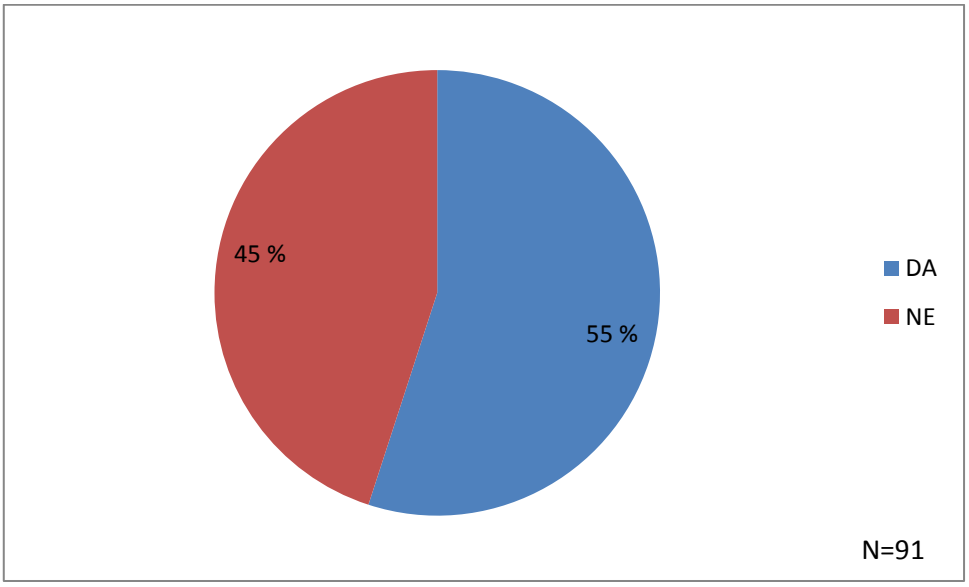


Slika 56: Odgovor na vprašanje 39: Prostor, kje se hrani komunikacijska oprema, je? (Možnih več odgovorov)

S slike 56 je razvidno, da imajo na anketiranih VIZ prostor večinoma zaščiten z alarmnim sistemom in opremljenega z javljalniki požara, v bližini imajo tudi gasilni aparati za gašenje računalniške opreme.

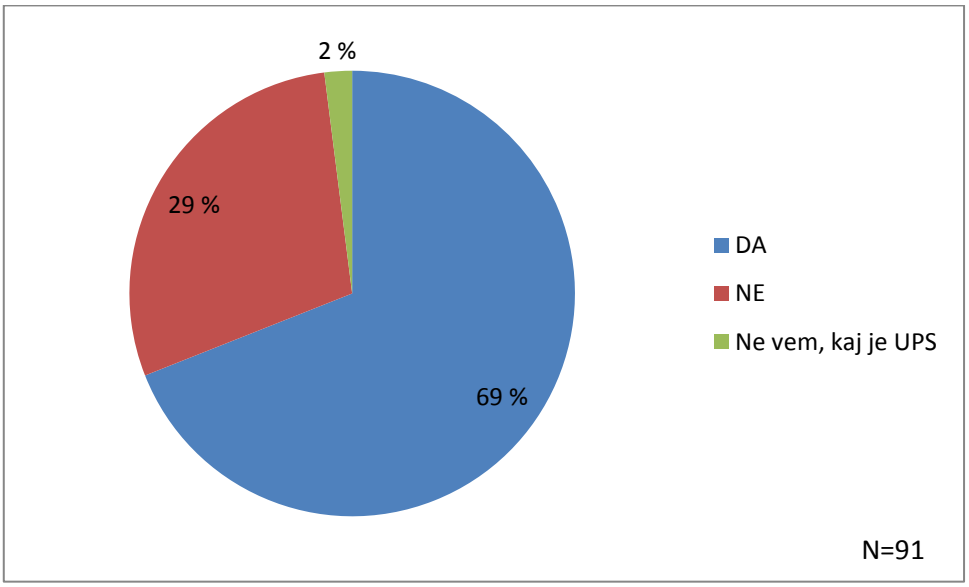
Kot drugo sta dva skrbnika navedla, da nimajo nič od tega, eden pa, da nimajo posebne opreme.

Po VIZ, ki so sodelovali v anketi, se obiskovalci v 55 % lahko prosto gibljejo, v preostalih 45 % ne (slika 57).



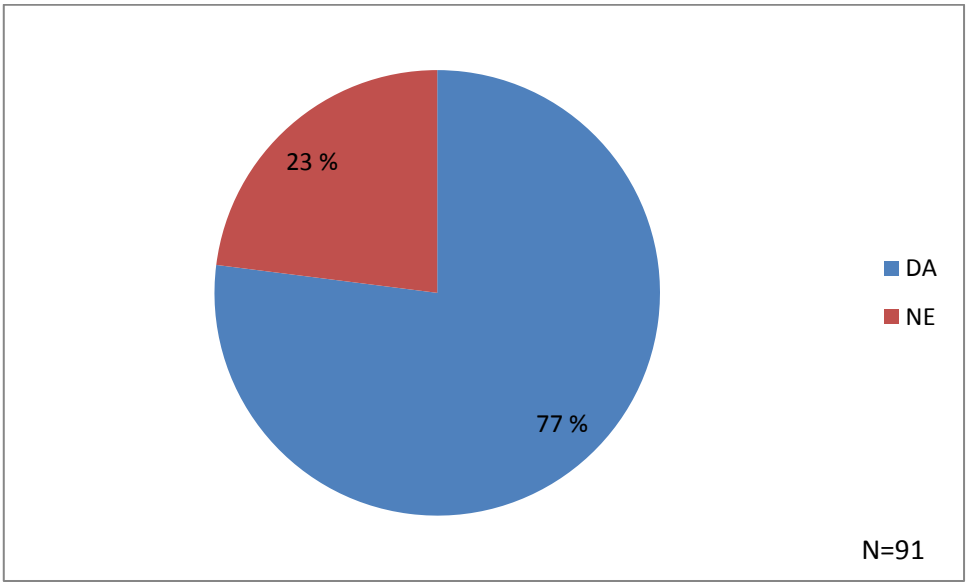
Slika 57: Odgovor na vprašanje 40: Ali se obiskovalci lahko prosto gibajo po stavbi organizacije?

V večini anketiranih VIZ (69 %) uporabljajo UPS, 2 anketiranca pa ne vesta, kaj je to UPS (slika 58).



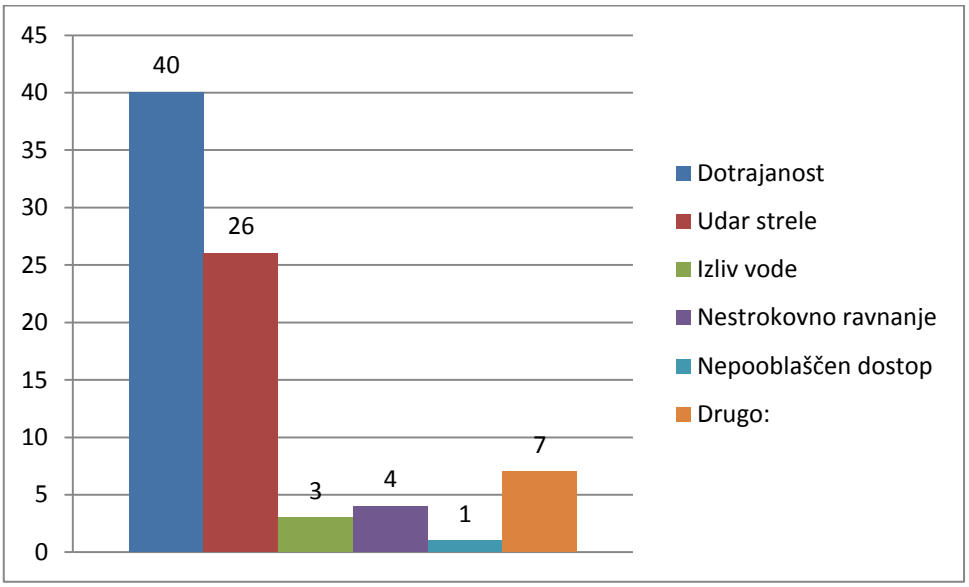
Slika 58: Odgovor na vprašanje 41: Ali za zagotavljanje nemotenega delovanja električnih naprav in uravnavanje napetostnih nihanj uporabljate UPS?

Slika 59 prikazuje, da so imeli na 77 % anketiranih VIZ že okvaro komunikacijske opreme.



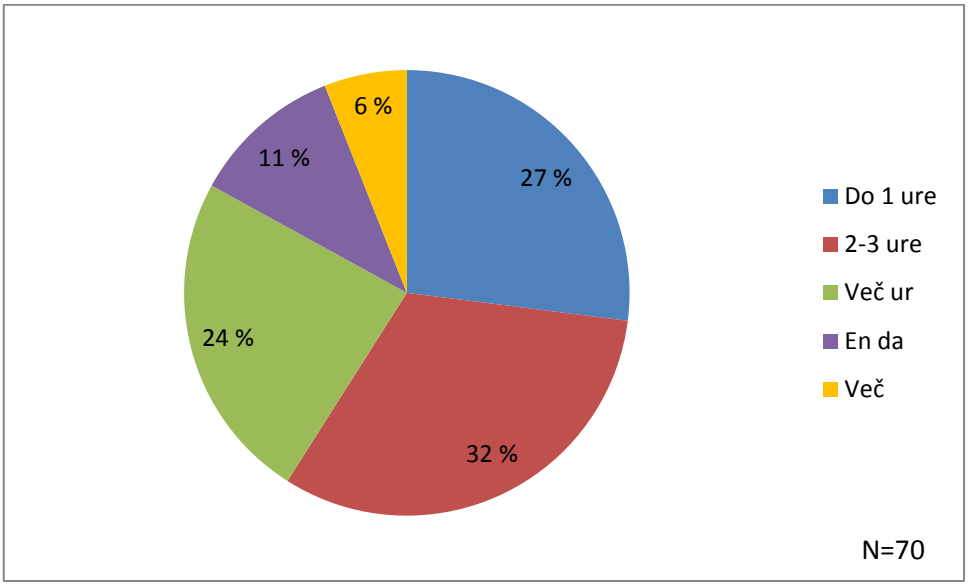
Slika 59: Odgovor na vprašanje 42: Ali ste že imeli okvaro komunikacijske opreme?

S slike 60 je razvidno, da je v večini primerov šlo za dotrajanost, kot drugo so navedli: nihanje el. napetosti, serijska napaka Telsey mrežnih stikal, napaka na opremi, težko reči, enostavno ni več delovalo (napaka na zunanji povezavi, najverjetneje vlaga), izklopi in vklopi elektrike.

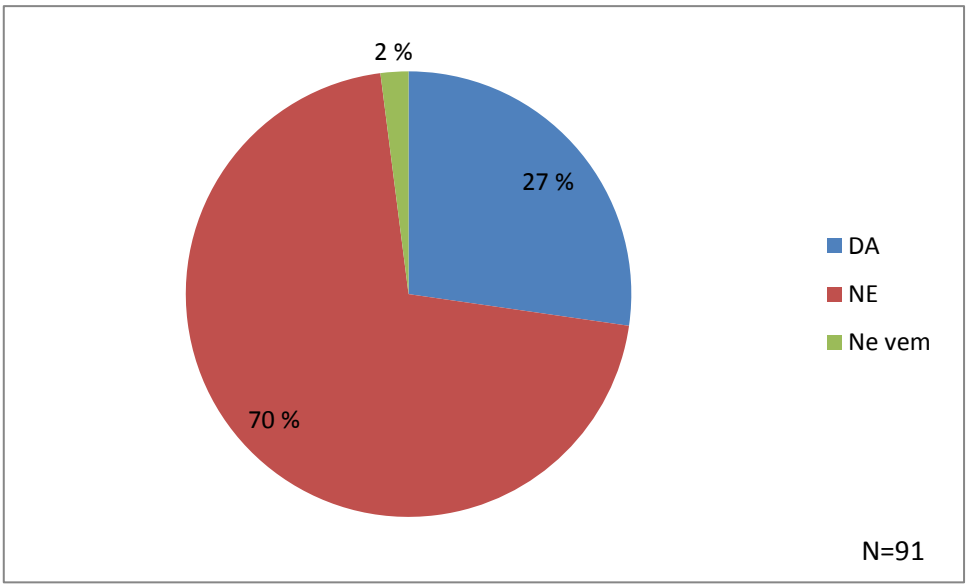


Slika 60: Odgovor na vprašanje 43: Kaj je bil vzrok okvare? (Možnih več odgovorov)

Povprečni izpad na anketiranih VIZ je v večini primerov trajal 2–3 ure, v 41 % pa celo več (slika 61). Težava je tudi v tem, da kar 70 % VIZ nima urejenega vzdrževanja za opremo (slika 62).

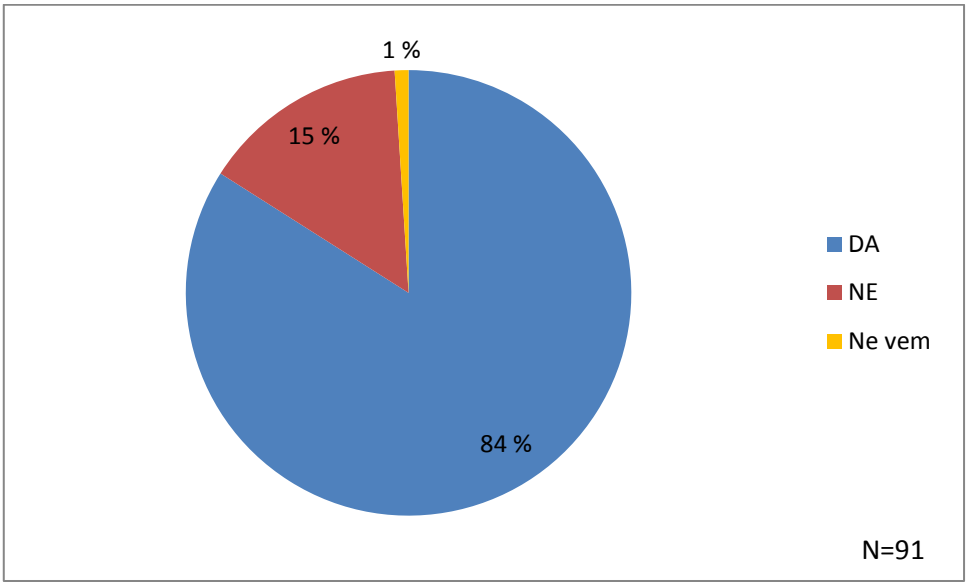


Slika 61: Odgovor na vprašanje 44: Koliko časa je trajal povprečni izpad?

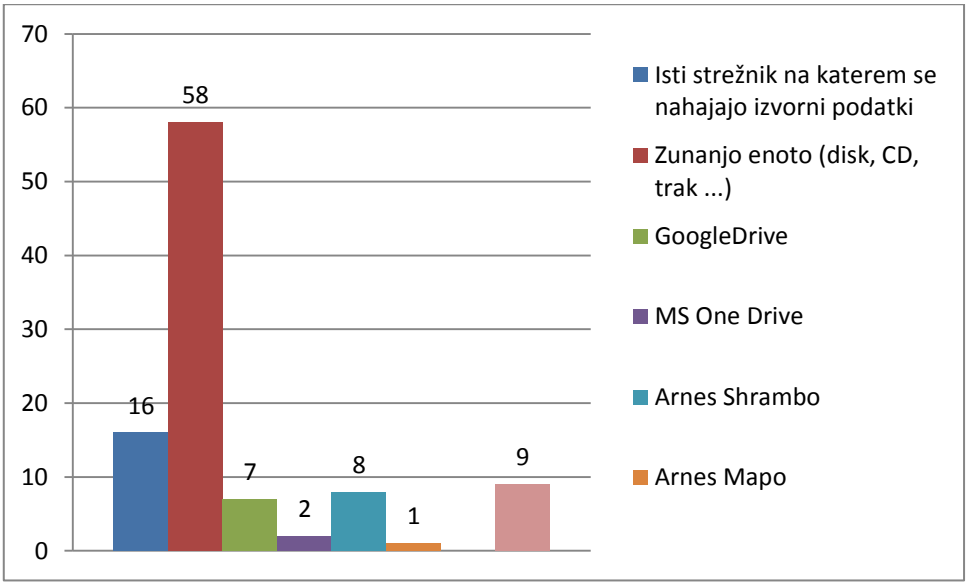


Slika 62: Odgovor na vprašanje 45: Imate za vzdrževanje strojne opreme urejeno vzdrževalno pogodbo?

Na VIZ, ki so sodelovali v anketi, se zavedajo pomembnosti svojih podatkov, saj ima v 84 % urejeno varnostno kopiranje ključnih podatkov (slika 63). S slike 64 je razvidno, da gre običajno za kopiranje na zunanjo enoto.



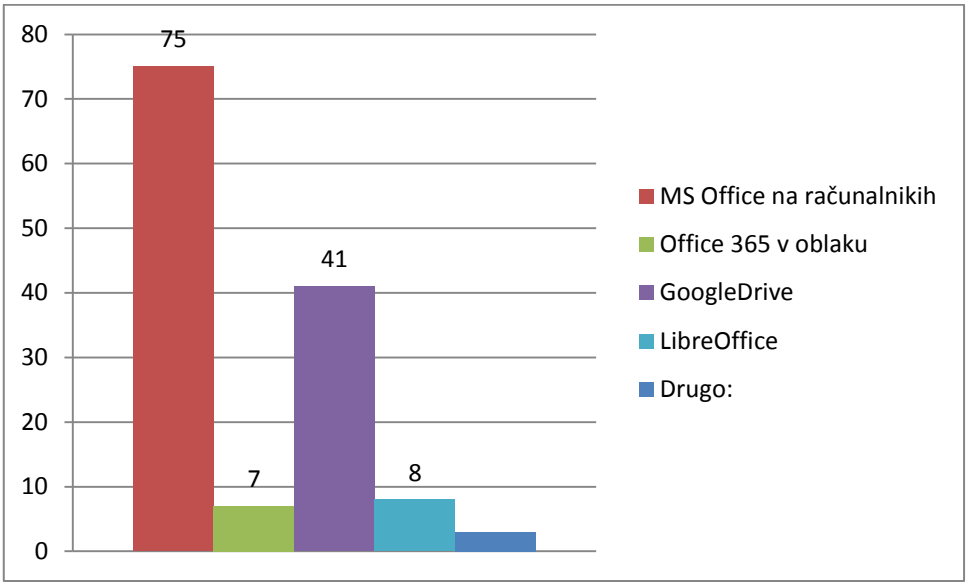
Slika 63: Odgovor na vprašanje 46: Imate urejeno varnostno kopiranje ključnih podatkov?



Slika 64: Odgovor na vprašanje 47: Kaj uporabljate za hranjenje varnostnih kopij? (Možnih več odgovorov)

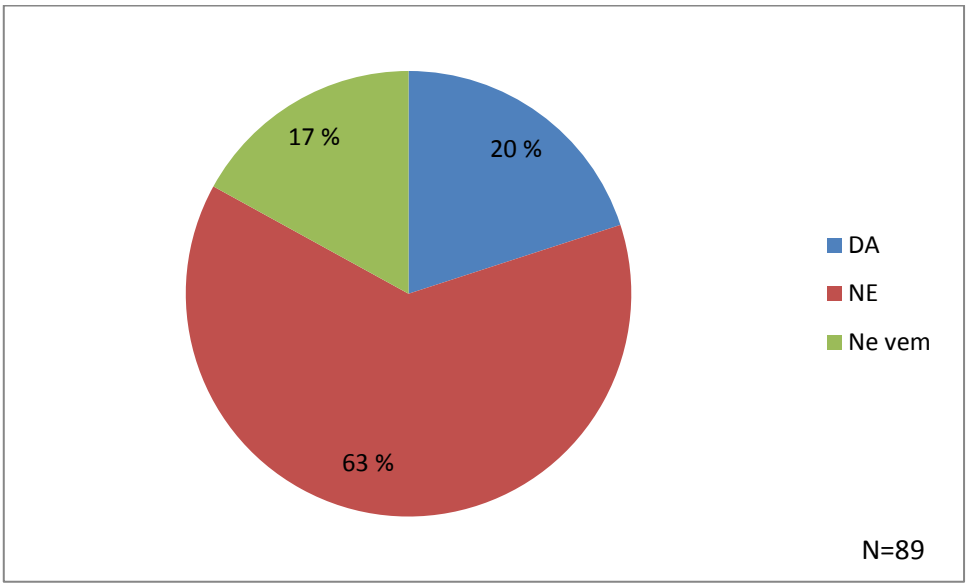
Kot drugo so navedli: nas, Dropbox, istor, wualla, samba strežnik, replikacijo na sekundarni strežnik.

Pri urejanje dokumentov v oblaku 41 anketiranih VIZ uporablja tudi GoogleDrive, 7 Office 365 (slika 65), kar se bo z uvedbo brezplačnih licenc še povečalo. Preostale storitve, ki jih na anketiranih VIZ uporabljajo, prikazuje slika 65.



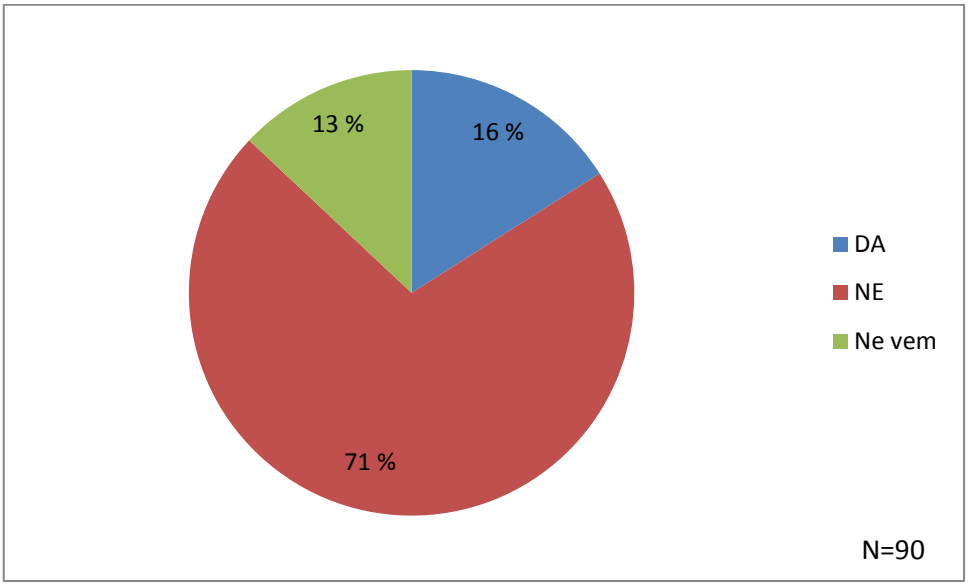
Slika 65: Odgovor na vprašanje 48: Kateri program/storitev uporabljate za delo z dokumenti?

Pričakovano je bilo, da na VIZ nimajo dokumentiranih IT varnostnih priporočil. Kar 63 % anketiranih VIZ je odgovorilo, da tega nimajo, 17 % jih o tem sploh ne nič ve (slika 66), kar je seveda za skrbnika sistema nekoliko nenavadno.



Slika 66: Odgovor na vprašanje 49: Ali ima vaša organizacije dokumentirana IT varnostna priporočila?

Nezadovoljivo stanje kažejo tudi rezultati raziskave ozaveščenosti uporabnikov glede informacijske varnosti. Slika 67 prikazuje, da anketirani skrbniki v veliki večini menijo, da uporabniki niso dovolj ozaveščeni glede informacijske varnosti.



Slika 67: Odgovor na vprašanje 59: Ali menite, da so uporabniki vašega informacijskega sistema na področju informacijske varnosti dovolj ozaveščeni?

Zadnje povsem odprto vprašanje je bilo: "Kaj vam pri opravljanju dela skrbnika informacijskega sistema predstavlja največjo oviro in kako bi to izboljšali?" Izkazalo se je, da je največja težava anketiranih skrbnikov neurejena sistematizacija delovnega mesta skrbnika informacijskega sistema. Poleg tega tistim skrbnikom, ki poleg naloge skrbnika opravljajo še drugo delo, primanjkuje časa za vzdrževanje informacijskega sistema. Ovira so tudi finance, saj je ponekod oprema že zastarela. Težave vidijo tudi v tem, da imajo uporabniki premalo računalniškega znanja in njihova nezainteresiranost za lastno varnost. Naj navedemo nekaj izbranih odgovorov:

- potrebna znanja z različnih področij, rešitev outsourcing;
- sistematizacija: 1 človek na eno šolo!;
- finance in premalo brezplačnih izobraževanj;
- premalo časa za načrtovanje in premalo financ;
- nezainteresiranost uporabnikov za lastno varnost;
- posodabljanje opreme;
- premalo znanja in včasih neodgovornost zaposlenih. Glede neznanja bi morali več časa posvetiti izobraževanju. Za neodgovornost zaposlenih pa bi moralo poskrbeti vodstvo šole;
- neozaveščenost;
- velika količina naprav, aplikacij, baz podatkov, podatkov, ki jih je potrebno ves čas obnavljati, urejati, vzdrževati;
- popravilo strojne opreme, upadate programov, ukvarjanje z minimalnimi napakami na računalnikih – zelo dobro bi bilo, če bi imeli za to lahko zaposlenega računalniškega tehnika;
- ni ovir, razen starost;
- tehnično nepodkovani zaposleni, z večjo pomočjo vodstva in izobraževanjem;
- razčiščeni odnosi – odgovornost;
- ni bistvenih ovir;

- neznanje uporabnikov;
- neizobraženost;
- nezainteresiranost sodelavcev za dobre nasvete;
- malomarno ravnanje z uporabniškimi imeni in gesli (enostavna gesla) – ozaveščanje;
- prostorska stiska in posledično neurejen prostor za delo ter seveda večno pomanjkanje časa; rešitve še ni na vidiku :);
- materialni pogoji;
- pasivnost uporabnikov in včasih vodstva;
- premalo strokovno izobražen, primerno izobraževanje v ta namen;
- informacijsko izredno slabo podkovani uporabniki lahko povzročijo več ur dela, tako ne ostane časa za sistemska opravila in tudi pripravo izobraževanj osebja, zaradi količine zanemarjeno lastno izobraževanje in tako slabša strokovna "podkovanost", plačni sistem v JS ne omogoča plačila za opravljeno delo in tako so edina izbira zunanji izvajalci za bolj zahtevna dela;
- sredstva;
- dosedanja vodstva ne jemljejo resno situacije in niso pripravljena vlagati v varnost. oz. so prepričana, da je ta segment pokrit že s tem, da je na tem mestu nekdo;
- nesistemsko reševanje problemov v OŠ na področju IKT / vsak rešuje po svoje.

Če na koncu povzamemo, so izsledki raziskave pokazali, da se v večini primerov anketirani skrbniki informacijskih sistemov zavedajo problema informacijske varnosti, ki jo poskušajo zagotavljati kljub pomanjkanju časa, denarja in znanja. Vendar je tukaj potrebno izpostaviti tudi, da je večina teh skrbnikov v starosti med 41 in 50 let in jim je kar težko slediti novim tehnologijam. Izkazalo se je, da v osnovnih šolah skrbniki večinoma opravljajo to delo le 30–40 % delovnega časa, preostanek delovnega časa delajo kot učitelji, ravnatelj … To pomeni, da se nalogi skrbništva informacijskega sistema ne morejo posvetiti v zadostni meri.

Večinoma so se skrbniki pripravljeni izobraževati samoiniciativno, kljub pomanjkanju časa, VIZ, kjer so zaposleni, pa jim stroške tovrstnih izobraževanj običajno tudi krije.

Skrbniki na VIZ se v veliki meri zavedajo pomena zagotavljanja informacijske varnosti. Velika ovira pri tem predstavljajo nerešene razmere na nivoju države.
Kar se tiče same varnosti, večina anketiranih VIZ, ki nima internetne povezave v omrežje ARNES, tudi nima urejene ločitve omrežja vsaj na administracijo/upravo in učence.

Zanimivo je, da imajo na anketiranih VIZ običajno urejeno ali vsaj delno urejeno dokumentacijo omrežja, kar je tudi eden izmed pogojev za varno omrežje.
Brezžična omrežja na anketiranih VIZ imajo v večini urejena tako, da imajo postavljen svoj usmerjevalnik, ki opravlja to funkcijo. Izkazalo se je, da imajo anketirani VIZ urejeno avtentikacijo z enim izmed varnostnih protokolov za brezžična omrežja. Varnostna pomanjkljivost je, da lahko gosti na anketiranih VIZ uporabljajo kar njihovo obstoječe omrežje, s čimer pridobijo tudi dostop do šolskih storitev.

Uporaba IPv6 protokola še ni razširjena, čeprav imajo skoraj vsi VIZ, ki so povezani v omrežje ARNES, to možnost. Običajno na anketiranih VIZ nimajo izklopljenih translacijskih mehanizmov, ki omogočajo vzpostavitev IPv6 povezave preko IPv4 tunela. Operacijski sistem Windows 7 in novejši imajo privzeto vklopljen Terredo in 6to4, ki naredi varnostno luknjo v sistemu, v kolikor ta translacijski mehanizem ni izklopljen ali onemogočen s požarnim zidom oz. filtri na usmerjevalniku.

Anketa je pokazala, da so strežniki čedalje bolj razširjeni. Na anketiranih VIZ na teh strežnikih običajno tečejo storitve, kot so: WWW, DHCP, aktivni imenik, LDAP …

Vedno bolj so razširjeni tudi sistemi za upravljanje vsebin, in sicer v veliki večini Joomla in Moodle. Počasi se dviga uporaba Wordpressa, saj so na Arnesu uvedi tudi možnost uporabe le-tega.

Anketa je pokazala, da skrbniki sistemov na anketiranih VIZ kar dobro skrbijo za svoje sisteme, saj na več kot polovici anketiranih VIZ še niso zabeležili vdora v strežnik. V kolikor so ga že zaznali, so strežnik počistili sami. Ne zavedajo pa se, da so tudi gesla na računalnikih šibka točka. Na več kot polovici anketiranih VIZ uporabnikom ni potrebno spreminjati svojih gesel na službenih računalnikih. Je pa pohvalno, ker niti eden ni odgovoril, da na računalnikih nimajo gesel.

Anketirani VIZ opremo v veliki večini hranijo v komunikacijski omari, vendar je le-ta ni v primernem prostoru, zato tudi dostop ni ustrezno varovan.

Zanimiv izsledek je tudi, da skoraj četrtina anketiranih VIZ še nikoli ni imela okvare opreme. Zaskrbljujoče pa je, da je kar v 41 % izpad trajal več kot 3 ure, v 6 % celo več kot en dan.

Vsi anketiranci se zavedajo varnosti shranjenih podatkov, zato imajo urejeno tudi varnostno kopiranje ključnih podatkov na zunanjo enoto (disk, trak, NAS), nekateri celo na lokacije zunaj zavoda.

Nekateri pa se ne zavedajo, kje hranijo dokumente. Polovica anketiranih VIZ uporablja GoogleDrive za upravljanje z dokumenti. Vprašanje je, ali pri tem pazijo, kakšna je vsebina teh dokumentov, saj te dokumente lahko izvažajo v države, kjer zakoni Evropske unije ne veljajo. Poleg tega nihče ne ve, kaj Google s temi podatki počne in kdaj bodo prišle na plano kakšne podrobnosti iz teh dokumentov.

Pričakovano, dokumentacija in ozaveščenost uporabnikov s področja varnosti v anketiranih VIZ bolj šepa. Anketiranci večinoma menijo, da uporabniki niso dovolj ozaveščeni na področju informacijske varnosti.

Pričakovano je bilo, da skrbnikom največjo oviro predstavlja predvsem pomanjkanje časa, znanja in denarja. V veliki meri bi to problematiko lahko rešili z ustrezno sistematizacijo delovnega mesta skrbnika informacijskih sistemov, kjer bi za eno šolo bil, za polni delovni čas, zaposlen en skrbnik. Na drugi strani pa bi morala država zagotoviti finančna sredstva za posodobitev in poenotenje IKT opreme. V letošnjem letu je pristojno ministrstvo izvedlo razpis za nakup računalniške opreme, vendar so ga morali ustaviti zaradi zamrznitve sredstev.

5. PRIMERI DOBRIH PRAKS IZ TUJINE

5.1. Hrvaška

Na Hrvaškem, podobno kot v Sloveniji, skrbi za povezavo in osnovno zaščito omrežij VIZ Hrvaška akademska in raziskovalna mreža (Croatian Academic and Research Network − CARNet).

CARNet upravlja z usmerjevalnikom oz. L3 stikalom, na katerem je nastavljena osnovna zaščita omrežja. Omrežje je, v dogovoru z VIZ, razdeljeno na več podomrežij, ki so zaščitena s filtri, samo lokalno omrežje je v domeni VIZ. Nekateri uporabljajo zaščito, ki jo upravlja CARNet, drugi v svoje omrežje postavijo svoj usmerjevalnik, na katerem izvajajo NAT ali požarni zid.
CARNet ima oddelke razdeljene glede na storitev, ki jo opravljajo:

- Oddelek mrežne infrastrukture, ki je razdeljen na 5 služb:
  - Izgradnja omrežij,
  - Nadzor in vzdrževanje mreže,
  - Omrežne storitve,
  - Dostop za posameznike,
  - Multimedija.
- Oddelek računalniških sistemov in storitev, ki je razdeljen na 4 službe:
  - Služba za sistemsko podporo članicam,
  - Služba sistemske podpore,
  - Služba informacijskih sistemov in storitev,
  - Register .hr domen.
- Oddelek za računalniško varnost, ki se deli na 2 službi:
  - Služba za obdelavo in preprečevanje računalniških-varnostnih incidentov,
  - Služba računalniško-varnostnih storitev.
- Nacionalni CERT,
- Oddelek za pomoč uporabnikom,
- Oddelek za podporo izobraževanju.

Kar se tiče osebe na VIZ, zadolžene za računalniško omrežje, je stanje podobno kot v Sloveniji. To so v prvi vrsti učitelji, ki imajo malce več znanja o računalništvu, ali učitelji, ki jim direktor dodeli to funkcijo zaradi premajhnega števila ur. To predstavlja tudi glavni razlog, zakaj večina nima interesa po izobraževanju na tem področju, saj za to delo niso plačani in koristijo svoj prosti čas.

Nič bolje ni niti na univerzah. Za administratorje računalniških omrežij so organizirali brezplačno udeležbo na Cisco Akademiji, vendar se je tega tečaja udeležilo zelo malo oseb in še od teh ga je zaključila le peščica.

CARNetova služba za računalniško-varnostne storitve v skladu z odločbo Ministrstva za znanost, izobraževanje in šport (Ministrstva znanosti, obrazovanja i sporta) izvaja filtriranje vsebine internetnega prometa. VIZ pošlje na CARNet zahtevek za

filtriranje vsebine in skupine, za katere želi, da se filtrirajo. Na voljo imajo naslednje skupine:

- Drugs,
- Gambling,
- Gambling Related,
- Gruesome Content,
- Hate Speech,
- Hacking,
- Malicious Sites,
- Nudity,
- Profanity,
- Pornography,
- School Cheating Information,
- Spam,
- Tobacco,
- Violence.

V ta namen uporabljajo CA eTrust Secure Content Manager, ki deluje na principu prepovedi prikaza internetnih strani v določeni skupini. Vsaka internetna stran je razvrščena v skupino glede na vsebino, ki jo ponuja. Promet se filtrira na podlagi izbire skupine, ki se ne bo prikazovala.

Razvrščanje strani se izvaja konstantno in nove baze podatkov se preverjajo vsakih nekaj ur. Poleg tega je mogoče tudi ročno prepovedati ali dovoliti prikaz določene internetne strani.

Filtriranje je omejeno samo na promet znotraj HTTP protokola, zato ni mogoče filtrirati elektronske pošte, FTP prometa, HTTPS prometa, P2P prometa (torrent …) itd.

VIZ mora imeti v svojem omrežju urejen sistem za preusmerjanje prometa proxy (npr. Squid), s katerim HTTP promet preusmerijo na sistem za filtriranje vsebin. Urediti morajo tudi preusmerjanje prometa iz vseh ali samo nekaterih računalnikov do proxy strežnika. To lahko storijo s konfiguracijo omrežne opreme ali z ročno nastavitvijo proxy strežnika na vsakem sistemu.

Izvajajo tudi storitev, s katero na CARNetu ozaveščajo članice o ranljivosti njihovega omrežja. Na zahtevo VIZ lahko enkratno ali periodično izvajajo teste ranljivosti omrežja. V ta namen uporabljajo program Nesuss, ki je namenjen odkrivanju ranljivosti omrežja (angl. vulnerability scanner). Gre za računalniški program, s katerim s pomočjo različnih tehnik skenirajo naprave v določenem razponu IP naslovov v omrežju ter na podlagi tako pridobljenih podatkov pridejo do informacij o topologiji in strukturi omrežja, vrsti in tipu naprave, inačici operacijskega sistema naprave, seznamu odprtih vrat itd. Na podlagi teh podatkov se izvedejo še dodatna testiranja z namenom pridobitve ustreznih podatkov o oddaljenih napravah in potrdila o obstoju nekaterih varnostih ranljivosti. Nessus trenutno podpira preko 5400 modulov (angl. plugin) za odkrivanje različnih vrst ranljivost. Tim moduli se dnevno dopolnjujejo. Sam modul običajno vsebuje informacijo o ranljivosti, navodilo, kako potrditi obstoj določene ranljivosti in kako jo odpraviti. V odvisnosti od stopnje tveganja Nesuss razdeli ranljivosti na 5

stopenj: kritična (angl. critical), visoka (angl. high), srednja (angl. medium), nizka (angl. low) in informativna (angl. info).
Po izvedbi testa dobi VIZ poročilo, v katerem so zajeti opisi varnostnih ranljivosti skeniranih sistemov ter navodila za odpravo le-teh. Naslednji korak naredi VIZ, ki mora poskrbeti za odpravo odkritih ranljivosti.

Arnes oz. znotraj njega SI-CERT bi lahko za slovenske VIZ (podobno kot hrvaški CARNet) izvajal periodične ali enkratne teste ranljivosti omrežja in po zaključku testiranja pripravljal poročila ter navodila za odpravo ugotovljenih ranljivosti.

5.2. Estonija

Uspeli smo navezati stik z Edmundom Laugassonom, ki na Univerzi v Talinu v okviru doktorskega študija raziskuje "Strategijo brezplačne programske opreme za upravljanje informacijsko-komunikacijske infrastrukture v Estoniji" (Free software strategies of managing information and communication technology infrastructure in Estonia).

Podobno kot v Sloveniji in na Hrvaškem zagotavlja povezavo v inetnet Estonski NREN, The Estonian Education and Research Network EENet.

Žal je tudi pri njih tako, da je vsak skrbnik informacijskega sistema prepuščen svojim odločitvam, saj nimajo nekega priporočila na nivoju države oz. pristojnega ministrstva. V šoli skrbi za informacijski sistem skrbnik. Na nivoju države imajo HITSA (The Information Technology Foundation for Education), katerega naloga je zagotoviti, da imajo učenci po zaključku šolanja na vseh nivojih pridobljena računalniška znanja, potrebna za razvoj gospodarstva in sociale, ter da so ponujene IKT možnosti spretno uporabljene pri poučevanju in učenju, kar pomaga izboljšati kakovost učenja in poučevanje na vseh ravneh izobraževanja (Hista, 2014).

Kot primer Laugassonom navaja zaščito njihovega brezžičnega omrežja. Za dostop do škodljivih in neprimernih vsebin uporabljajo storitev OpenDNS. Na usmerjevalniku omejujejo hitrost, pasovno širino in blokirajo razne programe, ki bi lahko upočasnili internet (P2P, strani za video vsebino …). S pojavom tablic in pametnih telefonov je tudi povečana uporaba lastnih naprav učencev. Ker uporabljajo šolsko brezžično omrežje, veljajo prej navedene omejitve tudi za njih. Čeprav imajo učenci skrbniške pravice na svojih napravah, Laugassonom pravi, da nimajo dovolj znanja, s katerim bi lahko spremenili nastavitve naprave in obšli omejitve, ki se izvajajo s pomočjo OpenDNS storitve. Prav tako imajo na dostopnih točkah nastavljeno omejitev, da naprave, priklopljene na brezžično omrežje, med sabo ne morejo komunicirati (Isolation mode).

Včasih upravljavci informacijskega sistema na šolah uporabljajo različne sisteme za zaznavanje vdorov (angl. intrusion detection systems IDS), kar je tudi opogumilo vlado, da je pristojno ministrstvo (Estonian Ministry of Economic Affairs and Communications) pričelo z izvajanjem programa "Snort4All". Ta program priporoča uporabo odprtokodnega IDS/IPS programa Snort in pošiljanje informacij CERT-u. Vendar je odločitev o uporabi programa ponovno v domeni posamezne šole.

Nekatere šole imajo različne dokumente varnostne politike. Večinoma vsebujejo politike, kot so: neprimerna in škodljiva vsebina mora biti filtrirana, lastne naprave se lahko prinesejo v šolo, vendar je uporaba med poukom vnaprej odobrena s strani učitelja ipd. Načeloma učenci tudi ne smejo svojih naprav žično povezati v omrežje VIZ, kar pa jim na VIZ praktično ne morejo preprečiti. DHCP jim deluje samo na enem delu omrežja, javnem delu, ločenem od ostalega omrežja šole. Preko DHCP-ja dobijo vse potrebne podatke za povezavo, ki jih sicer lahko spremenijo, vendar, kot že omenjeno, učenci naj ne bi imeli dovolj znanja za to.

V estonskem primeru sta se vlada in pristojno ministrstvo odločila podpreti program za zaznavo varnostnih vdorov v računalniška omrežja, ki avtomatsko pošilja zaznane informacije CERT-u. Omenjeni program bi lahko uporabili tudi v Sloveniji in bi tako že na nivoju države poskrbeli za dvig varnostne ozaveščenosti skrbnikov računalniških omrežij na VIZ in njihovih uporabnikov.

5.3. Anglija

Na spletu smo zasledili primera varnostne politike dveh šol v Angliji. Gre za Ellesmere Primary School in Chasetown Community School.

V primeru prve šole imajo zapisano, da je namen varnostne politike (Ellesmere Primary School, 2014):

- zagotavljanje zaupnosti, celovitosti in razpoložljivosti informacij in šolskega premoženja;
- zagotovitev, da so uporabniki seznanjeni in ravnajo popolnoma v skladu z zakonodajo;
- zagotovitev, da zaposleni razumejo potrebo po varnosti informacij in IKT ter njihovo odgovornost v zvezi s tem.

Podobno ima v varnostni politiki zapisano tudi Chasetown Community School.

Varnostna politika je namenjena celotnemu osebju šole, ki ima nazor nad ali vzdržuje šolske administrativne, izobraževalne IKT sisteme in podatke. IKT sistem je definiran kot vsaka naprava za avtomatično shranjevanje ali procesiranje podatkov in vključuje glavni računalnik, mini ali mikro računalnik, pametni mobilni telefon, osebni računalnik, delovno postajo, sistem za sporočanje, zunanje naprave za shranjevanje podatkov ipd. IKT podatki so informacije, shranjene ali obdelane s strani IKT in vključujejo programe, tekst, slike in zvok. IKT uporabnik je definiran kot zaposleni v okrožju (County Council employee), učenec ali druga pooblaščena oseba, ki uporablja šolski IKT sistem ali podatke. V nadaljevanju je definirano, da ima lastnik sistema lastninsko pravico do podatkov. V zvezi s tem je vsa programska oprema, podatki in dokumentacija, povezana z delom šole, v lasti okrožja, ki jih bo hranilo za potrebe šole. Uporabljajo tudi programsko opremo in podatke, ki jih pridobi in uporablja ravnatelj in katerih lastnik je zunanje podjetje (Ellesmere Primary School, 2014).

Vodstvo je odgovorno, da šole uporabljajo IKT v skladu z zakonskimi predpisi in ozaveščajo uporabnike o varnostni politiki. V praksi gre tukaj za odgovornost

ravnatelja, ki je tudi odgovoren za dokumentiranje vsake spremembe v varnosti IKT. V praksi lahko ravnatelj prenese dnevne funkcije na skrbnika sistema, ki ga mora določiti pisno. Upravljavec sistema je tako odgovoren za šolsko IKT opremo, sisteme in podatke in ima nadzor nad njimi in njihovo uporabo, vključno z nadzorom dostopa do njih in določanjem ter dokumentiranjem potrebnega nivoja zaščite. Oseba, ki to delo opravlja, mora biti zaposlena na šoli. V primeru, da skrbnik sistema ni ravnatelj, mora biti vodstvo med postopkom imenovanja seznanjeno z občutljivostjo delovnega mesta. Skrbnik mora v primeru suma ali dejanske kršitve informacijske varnosti takoj obvestiti ravnatelja. Ta mora poskrbeti, da se to zabeleži in razišče s pomočjo oddelka okrožja za notranjo revizijo, ki izvaja tudi periodične preglede varnostne politike (Ellesmere Primary School, 2014).

Uporabniki sistemov morajo biti seznanjeni z varnostno politiko in ob sumu ali dejanski kršitvi takoj obvestiti skrbnika sistema.

V nadaljevanju je opisana fizična varnost, ki narekuje urejenost dostopa do prostorov z IKT opremo ali podatkov samo pooblaščeni osebi. Dostop do takšnih prostorov mora biti varovan s kodo in elektronsko ključavnico, da ne bi prišlo do nepooblaščenega dostopa do podatkov, uporabniki ne smejo puščati svojih računalnikov odklenjenih ob njihovi odsotnosti. Prav tako na mizi ne smejo puščati občutljivih podatkov v pisni obliki.

Šolski IKT sistem ni dovoljeno uporabljati na način, ki krši zakon. Takšne kršitve so na primer (Ellesmere Primary School, 2014):

- izdelava, distribucija ali uporaba programske opreme ali podatkov, za katere nimajo licence;
- izdelava ali pošiljanje grozilnih, žaljivih sporočil;
- izdelava, posedovanje ali distribucija nespodobnega gradiva;
- nepooblaščena uporaba šolske infrastrukture v privatne namene.

Skrbnik sistema določa tudi nivo zaščite z gesli, ki je odvisen od občutljivosti podatkov. Gesla morajo biti na vseh sistemih, vključno z zagonskimi (angl. boot) gesli na prenosnih računalnikih, ki imajo slabšo fizično varovanje. Gesla naj bi si običajno zapomnili. Gesla, ki se ne uporabljajo pogosto in jih je potrebno zapisati, je potrebno hraniti na varnem mestu. Uporabniki morajo imeti jasna in pisna navodila o potencialnih nevarnostih napisanih gesel. Prav tako morajo biti uporabniki poučeni o primernih tehnikah za izbiro gesel. Sistem, ki to omogoča, mora uporabnike periodično obveščati o zahtevi za spremembo gesla (npr. enkrat letno). Kadar uporabnik sumi, da njegovo geslo pozna še neko, ga mora nemudoma spremeniti. Gesla ne smejo izdati nikomur, vključno s skrbnikom sistema.

Skrbnik sistema poskrbi tudi za varnostno kopiranje podatkov, ki je odvisno od pomembnosti in količine podatkov. Varnostne kopije morajo biti jasno označene in hranjene v protipožarnem prostoru, ki ni na lokaciji šole. Potrebno je izvajati tudi periodično testiranje obnovitve podatkov iz varnostnih kopij. Zgoraj navedeno velja za strežnike, medtem ko morajo za prenosnike in namizne računalnike poskrbeti sami. Priporočilo je, da se varnostna kopija naredi enkrat tedensko (Ellesmere Primary School, 2014).

Šola uporablja protivirusno zaščito, vendar mora poskrbeti tudi za ozaveščenost uporabnikov. V primeru suma na virus ali sami virusni okužbi, morajo uporabniki o tem nemudoma obvestiti skrbnika sistema, ki poskrbi za čiščenje okužbe.

Odslužene IKT odpadke (izpisi, CD/DVD, trakovi …) je potrebno odstraniti na način, ki se opredeli glede na občutljivost podatkov, ki jih vsebujejo. Npr. papir z natisnjenimi zaupnimi podatki je potrebo uničiti v rezalniku papirja. Podobno velja tudi za odslužено in okvarjeno IKT opremo. Nepooblaščene osebe ne smejo videti podatkov, ki so shranjeni na medijih (Ellesmere Primary School, 2014).

Dostop do elektronske pošte in interneta mora biti odobren s strani skrbnika omrežja. Ves dostop do interneta mora biti vzpostavljen preko enega izmed potrjenih ponudnikov interneta, izjeme pa morajo biti potrjene s strani ravnatelja. Če ima ponudnik dostopa možnost filtriranja prometa, je potrebno to tudi izkoristiti. Šolsko omrežje je sicer namenjeno delovanju šole, vendar se dovoli tudi uporaba v privatne namene, dokler je to sprejemljivo. Prav tako ima šola pravico nadzorovati elektronska sporočila in uporabo interneta (Ellesmere Primary School, 2014).

Proučena angleška primera kažeta na zelo detajlno spisane IKT varnostne politike. S prilagoditvijo na slovensko okolje bi ju lahko uporabili kot osnovo pri oblikovanju priporočil glede varnostne politike na slovenskih VIZ.

5.4. Norveška

V okviru delovne skupine Norveškega NREN-a UNINET so bila pripravljena priporočila za implementacijo IKT varnostne strukture v norveškem visokem šolstvu. Priporočila temeljijo na "primerih dobrih praks", ocene tveganja, regulativnih in komercialnih zahtevah, ki jih je izdal norveški informacijski pooblaščenec (Norwegian Data Inspectorate – Datatilsynet), s poudarkom na obstoječih praksah. Cilj njihovih priporočil je opredeliti enotno strukturo, ki bo omogočila visokošolskim zavodom, da ustrezno zaščitijo informacije in informacijske sisteme. Ključne zahteve za varnost informacij vključujejo (Boe, Enstad in Eilertsen, 2014):

- zaupnost,
- celovitost,
- razpoložljivost.

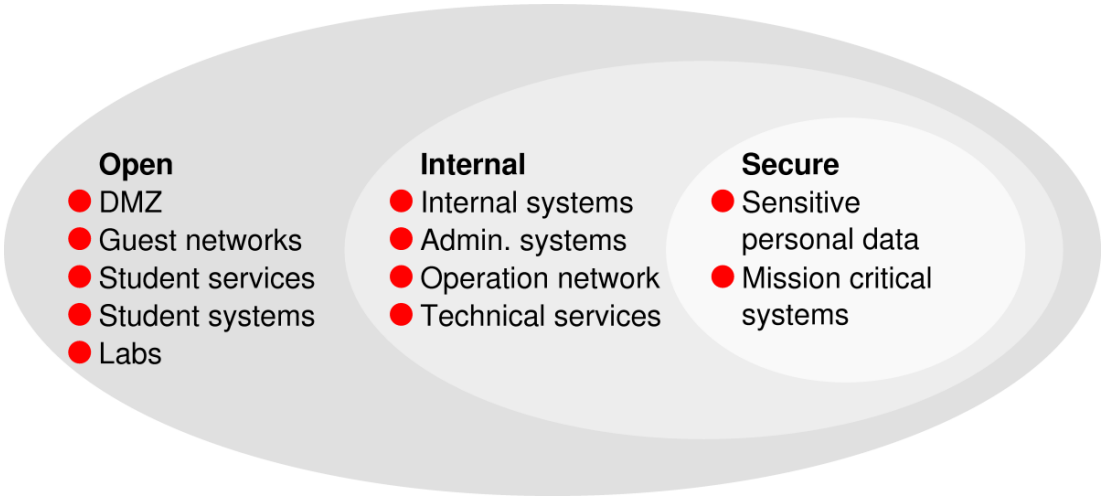
IKT varnostna arhitektura mora izpolnjevati naslednje splošne zahteve (Boe, Enstad in Eilertsen, 2014):

- Institucije morajo poskrbeti za ustrezno zaščito svojih informacijskih dobrin. Varnost in tveganja morajo biti dobro uveljavljena na ravni vodstva in temeljiti na oceni tveganja.
- IKT sistemi morajo biti v skladu z varnostno politiko institucije.
- Upoštevati je treba zakonske zahteve in smernice, kot so EU direktiva o zasebnosti in elektronskih komunikacijah (2002/58/ES), ter lokalno zakonodajo.

- Varnostna arhitektura mora biti v skladu s cilji institucije, kot je določeno v lokalni zakonodaji, ter z vsemi sporazumi, ki jih ima lahko institucija s tretjimi partnerji.
- IKT sistemi morajo biti dovolj zmogljivi in dovolj stabilni v primeru odpovedi.
- IKT sistemi morajo biti dovolj kvalitetni.

Varnostna struktura temelji na naslednjih principih (Boe, Enstad in Eilertsen, 2014):

- Omrežje mora biti razdeljeno na različne cone in varnostne razrede:
  - razdelitev v cone in razrede mora biti v skladu z oceno tveganja;
  - odgovorna oseba za umestitev sistema je skrbnik tega sistema;
  - razdelitev na cone je temeljno načelo varnostne strukture;
  - za vsako cono je potrebno opredeliti minimalno raven varnosti;
  - priporočljivo je, da vzpostavijo tri cone: odprto, notranjo in varno cono;
  - visokošolski zavodi se lahko odločijo za vzpostavitev dodatnih območij v skladu z zahtevami in oceno tveganja;
  - cona na določeni varnostni ravni ne sme imeti dostopa do cone na višji varnostni ravni, razen če je bilo izdano posebno dovoljenje;
  - ni nujno, da ima cona z določeno varnostno stopnjo dostop do območja na nižji varnostni stopnji;
  - vsaka cona vsebuje eno ali več segmentov omrežja, kakor je prikazano na sliki 68;
  - segmenti omrežja v določenem območju lahko delujejo pod različnimi varnostnimi kriteriji;
  - segmenti znotraj določene cone, ki lahko delujejo v skladu s skupnimi varnostnimi merili, se lahko združijo v varnosti razred;
  - segmenti omrežja v isti coni ali varnostnem razredu niso nujno dostopni med seboj.
- Obstajati mora jasna ločitev med strežniki in odjemalci.
- Strežniki in odjemalci morajo biti umeščeni v ustrezne varnostne razrede, ki temeljijo na ocenah tveganja.
- Dostop do storitev mora biti pod nadzorom ustreznih varnostnih pregrad (požarni zid, filtriranje paketov, proxy strežniki, avtentikacijska in pristopna kontrola, VPN …).
- Z virtualnimi strežniki in odjemalci je treba ravnati po istih načelih kot za druge enote.



Slika 68: Primer delitve računalniškega omrežja na cone in segmente (Boe, Enstad in Eilertsen, 2014)

Pisci priporočil predlagajo vzpostavitev treh con, vendar za vsako obstajajo svoja podrobna priporočila, ki so podana v nadaljevanju.

a) Odprta cona

Sem spadajo (Boe, Enstad in Eilertsen, 2014):

- študentska omrežja (interna študentska pošta, datotečni strežnik za domače mape študentov, spletne aplikacije za študente, tiskalniški strežniki);
- omrežje za goste (gostje morajo sprejeti pogoje uporabe);
- DMZ (zunanji spletni strežniki, sprejem elektronske pošte z zunanjih omrežij, zunanji DNS strežniki, VPN);
- Laboratoriji;
- servisi za študentske odjemalce;
- osebna oprema.

Kar se tiče strežnikov, gre za zahteve v zvezi z dobrim upravljanjem sistemov, kot so redno krpanje varnostnih lukenj in onemogočanje nepotrebnih storitev. Priporočen je tudi centrali nadzor nad dnevniškimi zapisi vseh strežnikov. Vsaka članica posebej določi zahteve za odjemalce.

Brezžični dostop do interneta mora biti urejen preko omrežja Eduroam ali podobne implementacije standarda 802.1X. Poseben dostop je potrebno urediti tudi za goste, ki nimajo dostopa do omrežja Eduroam. Podoben način avtentikacije mora biti urejen tudi v žičnem delu, v predavalnicah in sejnih sobah.

b) Interna cona

Sem spadajo (Boe, Enstad in Eilertsen, 2014):

- Osnovne storitve, kot so:
  - DHCP, NTP, SIP, rekurzivni DNS;
  - baze uporabnikov, aktivni imenik;

  - študentski servisi;
  - interni poštni strežniki;
  - datotečni strežniki za domače mape zaposlenih;
  - internetne spletne strani;
  - koledar;
  - sistemi za upravljanje odjemalcev;
  - tiskalniški strežniki.

- Tehnične storitve, kot so:
  - sistemi za upravljanje zgradbe;
  - sistemi za upravljanje avdio/video opreme;
  - oprema za videonadzor.

- Administrativne storitve, kot so:
  - sistemi za arhiviranje;
  - administrativni sistemi;
  - administrativni strežniki, ki niso nameščeni v varni coni (npr. računovodstvo).

- Upravljalno omrežje:
  - strežniki za nadzor omrežja in servisov, stikal, usmerjevalnikov, dostopnih točk …

To so interni segmenti, ki jih uporabljajo zaposleni in ostali, povezani z zavodom. Do teh segmentov naj ne bi bil omogočen dostop iz naprav, ki niso v omrežju članice. Za strežnik v interni coni veljajo enake zahteve kot v odpri coni. Za odjemalce velja, da imajo skrbniške pravice samo skrbniki sistemov. Glede operacijskega sistema morajo ustrezati zahtevam zavoda. Protivirusna programska oprema mora biti posodobljena na zadnjo različico. Naprave, ki niso v lasti zavoda in le-ta za njih ne skrbi, naj ne bi bile v tej coni.

Vse naprave v tej coni morajo biti avtenticirane (npr. 802.1X) in vsi uporabniki avtenticirani preko centralne baze uporabnikov. Sistemi, ki ne podpirajo centralne avtentikacije, morajo biti še posebej zaščiteni.

c) Varna cona

Sem spadajo (Boe, Enstad in Eilertsen, 2014):

- Občutljivi osebni podatki:
  - različni podatki o bolniku (v primeru, da ima šola svojo ambulanto);
  - administrativni sistemi, ki vsebujejo občutljive osebne podatke;
  - posnetki videonadzora.
- Kritični sistemi:
  - sistemi za zaklepanje;
  - kontrola pristopa;
  - raziskovalni podatki;
  - varnostne kopije;
  - druge informacije, pomembne za informacijsko varnost, kot je določeno z oceno tveganja.

V varni coni je potrebno poskrbeti še za dodatne varnostne ukrepe, kot so: preverjanje celovitosti, zaznavanje vdorov, šifriranje podatkov, utrjevanje varnosti in centralno hranjenje dnevniških zapisov. V to cono naj ne bi vključevali odjemalcev. Tisti, ki dostopajo do storitev v tej coni, naj bi bili vključeni v interno cono. Posebno skrb je potrebno nameniti tudi oddaljenemu dostopu (Boe, Enstad in Eilertsen, 2014).

Uporabnike, ki želijo dostopati do varne cone, je potrebno ponovno avtenticirati (Boe, Enstad in Eilertsen, 2014).

V priporočilih so definirali tudi 3 pojme, in sicer skrbnik sistema, osebni podatki in občutljivi osebni podatki.

Skrbnik sistema je oseba, ki je znotraj zavoda zadolžena za to, da se sistem uporablja v skladu z veljavnimi sporazumi, zakonodajo in predpisi. Skrbnik sistema je odgovoren za opredelitev in ureditev dostopa do podatkov v sistemu in zagotavlja, da ima organizacija ustrezno podporo uporabnikom ter napisane postopke za uporabo sistema (Boe, Enstad in Eilertsen, 2014).

Občutljivi podatki so informacije in lastnosti, ki jih povežemo z določeno osebo.

Občutljivi osebni podatki se nanašajo na (Boe, Enstad in Eilertsen, 2014):

- rasne ali etnične pripadnosti; politična mnenja, verska ali filozofska prepričanja;
- kazenske evidence;
- podatke, povezane z zdravjem;
- spolno življenje in spolno usmerjenost;
- članstvo v sindikatu.

Na norveškem so pripravili dobra priporočila, kako urediti segmentacijo računalniškega omrežja z razdelitvijo storitev v različne cone varnosti. To idejo bi lahko uporabili tudi v naših varnostnih priporočilih.

6. PREDLOGI ZA IZBOLJŠANJE VARNOSTI RAČUNALNIŠKIH OMREŽIJ VIZ V SLOVENIJI

Kakor že omenjeno, je bilo v Sloveniji v šolskem letu 2013/2014 registriranih 2084 VIZ. Opravljena anketa je pokazala na različne razloge, zakaj stanje glede informacijske varnostni na VIZ ni tako, kot bi si ga želeli.

V nadaljevanju bomo podali predloge, kaj bi se po našem mnenju dalo storiti na posameznem nivoju in kako bi lahko k izboljšanju varnosti računalniških omrežij na VIZ pripomogli država, Arnes in pa sam VIZ.

6.1. Kaj je potrebno urediti na nivoju države?

V Sloveniji je za VIZ trenutno pristojno Ministrstvo za izobraževanje, znanost in šport (v nadaljevanju ministrstvo). Poleg VIZ spada pod okrilje ministrstva tudi Arnes, katerega naloga je zagotavljanje omrežne storitve organizacijam s področja raziskovanja, izobraževanja in kulture ter omogočanje njihovega povezovanja in medsebojnega sodelovanja.

Anketa, ki smo jo izvedli, je pokazala, da so skrbniki računalniških omrežjih na anketiranih VIZ običajno na tem delovnem mestu zaposleni le med 30 in 40 % delovnega časa, v preostalem delovnem času opravljajo delo ravnatelja, učitelja … To predstavlja težavo, saj na anketiranih VIZ nimajo zaposlenega, ki bi se lahko nalogi skrbništva računalniškega omrežja in vzdrževanja IKT opreme posvečal v zadovoljivi meri. Pomanjkanje znanja in časa skrbnikov na VIZ posledično privede do pomanjkljivo vzdrževane opreme, kar nedvomno negativno vpliva na razpoložljivost računalniškega omrežja na VIZ. Anketa je torej pokazala, da je največja težava anketiranih skrbnikov neurejena sistematizacija delovnega mesta skrbnika informacijskega sistema. Naloga ministrstva bi bila, da uredi sistematizacijo skrbnika IKT na VIZ. Med njegove naloge bi sodila: skrb za IKT opremo, omrežje VIZ, izobraževanje uporabnikov … Tako bi se skrbnik lahko v celoti posvetil svojemu delu in se na tem področju tudi dodatno izobraževal.

Težavo predstavlja tudi nizek nivo računalniškega znanja uporabnikov VIZ. Le-ti so zaradi neznanja in posledično nezainteresiranosti velika grožnja v sistemu, saj jim kot takim najbrž ni mar niti za varnost kot tudi ne za podatke. Z dodatnim izobraževanjem skrbnikov, kot je bilo omenjeno že prej, bi lahko novo pridobljeno znanje prenesli tudi na uporabnike in tako vsaj delno omejili nevarnosti v informacijskem sistemu.

Še hujšo oviro pa predstavljajo finance, saj je ponekod oprema že zastarela in dotrajana. Ravno v letošnjem letu je pristojno ministrstvo izvedlo razpis za nakup računalniške opreme, vendar so ga morali zaradi blokiranih finančnih sredstev s strani ministrstva za finance ustaviti, kar se na dolgi rok lahko izkaže kot velika napaka. Država bi morala takšna sredstva VIZ-om zagotoviti, ne pa vzeti. S takšnim mačehovskim odnosom so se skrbniki primorani "znajti" po svoje, kar pa lahko dodatno ogrozi stabilnost in varnost informacijskih sistemov VIZ.

Ministrstvo sicer vsako leto izda "Priporočila o standardih in normativih programa Računalniško opismenjevanje in informatika", ki podrobneje opisujejo informatizacijo naslednjih VIZ: samostojni vrtci (z enotami), osnovne šole (z vrtci in/ali s podružnicami), srednje šole in srednješolski centri (z višjimi šolami), dijaški domovi, zavodi, ki izobražujejo učence s posebnimi potrebami, ljudske univerze ter glasbene šole. V priporočilih je opisano (MIZŠ(a), 2014):

- opredelitev računalniške opreme po prostorih zavoda;
- kdo so uporabniki računalniške opreme na zavodu;
- računalniška oprema na zavodu;
- lokalna računalniška omrežja, povezava v internet, in omrežne storitve.

V teh priporočilih je omenjeno tudi računalniško omrežje, vendar opisuje samo zahtevo, da morajo na VIZ omogočiti dostop do podatkov in programov na lokalnem strežniku in internetu z vseh računalnikov. V tehničnem delu je sicer zapisano, da je nujno upoštevanje varnostnih standardov, toda kot primer je navedena zgolj povezava do Arnesove spletne strani z informacijo o omrežju Eduroam. Ta dokument bi bilo potrebno dopolniti oz. izdelati priporočila in specifikacije za omrežno opremo, kar bomo poskušali podati v nadaljevanju.

Arnes po svojih najboljših močeh poskuša VIZ pomagati pri varovanju računalniškega omrežja. Vendar na tem področju nastopi težava zaradi pomanjkanja kadra in financ. Da bi bila Arnesova podpora VIZ bolj učinkovita, bi morala država okrepiti Arnes tako kadrovsko kot finančno. Arnes bi tedaj lahko ponudil več storitev in izobraževanj za skrbnike VIZ.

6.2. Kaj lahko stori Arnes?

Arnes je javni zavod, ki zagotavlja omrežne storitve organizacijam s področja raziskovanja, izobraževanja in kulture, omogoča njihovo povezovanje in medsebojno sodelovanje ter sodelovanje s sorodnimi organizacijami v tujini. Zaradi nenehnih sprememb tehnologije se Arnes sproti prilagaja potrebam svojih uporabnikov in jim želi dolgoročno zagotoviti enake možnosti sodelovanja v enotnem evropskem prostoru. Pogoj za to je tesno povezana omrežna infrastruktura z enotnimi tehnološkimi in varnostnimi standardi ter ustrezne storitve, ki jih na celotnem evropskem območju vzpostavljajo in vzdržujejo nacionalne izobraževalne in raziskovalne mreže.

Poleg samega povezovanja nudi Arnes tudi elektronsko pošto s protivirusno zaščito, razne oblike gostovanja spletnih strani in strežnikov, registracijo in upravljanje domen, digitalna strežniška potrdila, videokonference in prenos videa v živo … Na področju povezovanja VIZ-om nudi tudi upravljanje usmerjevalnika in stikala, prioriteto promet ter filtriranje prometa proti in iz omrežja VIZ. Omrežne storitve lahko ponudi le VIZ-om, ki so povezani v omrežje ARNES.

Poleg tega znotraj Arnesa deluje tudi SI-CERT (Slovenian Computer Emergency Response Team), ki je nacionalni odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij. Opravlja koordinacijo razreševanja incidentov, tehnično svetovanje ob vdorih, računalniških okužbah in drugih zlorabah ter izdaja opozorila za upravitelje omrežij in širšo javnost o

trenutnih grožnjah na elektronskih omrežjih. SI-CERT samostojno izvaja nacionalni program ozaveščanja "Varni na internetu" in sodeluje v projektu SAFE-SI (Si-cert, 2014).

SI-CERT na svoji spletni strani redno obvešča o novih ranljivostih in nevarnostih. Preko spletne strani je možno oddati tudi prijavo varnostnega incidenta.

S pomočjo svojih strokovnjakov bi Arnes lahko za skrbnike VIZ pripravil priporočila za izgradnjo, vzdrževanje in varovanje računalniških sistemov. Leta 2002 so bila na Arnesu, v okviru projekta "Zagotavljanje varnosti", izdelana priporočila o varnosti v šolskih omrežjih. V dokumentu so bile opisane najbolj pogoste storitve, ki so se takrat uporabljale: elektronska pošta, WWW, FTP, DNS, terminalski dostop, NTP, NetBIOS, IRC, ICMP, izmenjava datotek ter multimedijske konference in tehnologija "multicast". Med drugim je bilo opisano tudi, kako nastaviti zaščito omrežja na Cisco usmerjevalniku in Linux operacijskem sistemu. Tehnološki napredek, število novih storitev in groženj pa se je od leta 2002 korenito spremenilo, zato bi bilo potrebno ta priročnik prenoviti in dodati navodila za: nakup komunikacijske opreme, zaščito omrežja s pomočjo mehanizmov, ki jih omogoča današnja komunikacijska oprema, delitev omrežja, ustreznost prostora … Predlog takih priporočil, ki so bila pripravljena v okviru tega magistrskega dela, se nahaja v prilogi 2.

Na podlagi posodobljenih priporočil in priročnikov bi Arnes lahko hkrati ob opravljanju pregledov IKT sistemov skrbnike izobraževal na temo informacijske varnosti. Takšen prenos znanja bi bil lahko zelo učinkovit, saj bi Arnesovi strokovnjaki delili svoje znanje in izkušnje, skrbniki VIZ pa bi na tak način pridobili najboljšo podporo in pomoč pri vzdrževanju in varovanju računalniških sistemov.

Pri pregledu primerov dobrih praks iz tujine smo naleteli na zanimivi storitvi, ki ju izvajajo na Hrvaškem. Storitev preverjanja ranljivosti omrežja in uporaba programske opreme za nadzor naprav in storitev (Nagios) sta dodatni storitvi, ki bi ju lahko za VIZ v Sloveniji izvajal Arnes.

6.3. Naloge vodstva VIZ in skrbnika računalniška sistema VIZ

Primarna naloga vodstva VIZ je, da se zave pomembnosti varnosti informacijskega sistema in zagotovi ustrezna sredstva za njeno vzpostavitev in izvajanje. Skrbniku informacijskega sistema mora zagotoviti vso moralno in materialno podporo.

Skrbnik informacijskega sistema na VIZ mora pripraviti varnostno politiko, ki jo mora vodstvo potrditi.

Varnostna politika je dokument oz. zbirka dokumentov, ki opredeljuje tako varnostne zahteve − cilje organizacije, kakor tudi postopke za doseganje teh zahtev − varovalne ukrepe. Mednarodni standard, ki pokriva področje informacije varnosti, je ISO/IEC 27000. Ukvarja se z varovanjem podatkov pred nepooblaščenim dostopom, razkritjem, uničenjem, uporabo, nerazpoložljivostjo ali spremembo. Samo področje varnostne politike je določeno v standardu ISO/IEC 27000. Priporočamo, da se pri pripravi varnostne politike na VIZ oprejo na omenjeni standard.

Namen varnostne politike je (Ellesmere Primary School, 2014):

- zagotavljanje zaupnosti, celovitosti in razpoložljivosti informacij in šolskega premoženja;
- zagotovitev, da so uporabniki seznanjeni in ravnajo popolnoma v skladu z zakonodajo;
- zagotovitev, da zaposleni razumejo potrebo po varnosti informacij in IKT ter njihovo odgovornost v zvezi s tem.

Ciljna publika so uporabniki IKT storitev (zaposleni, učenci/gojenci, zunanji sodelavci) ter zunanji izvajalci.

V nadaljevanju je navedeno, kaj naj bi varnostna politika vsebovala.

Najprej je potrebno določiti skrbnika varnostne politike, katerega naloga bo (Ellesmere Primary School, 2014):

- priprava in vzdrževanje dokumentov varnostne politike;
- razvoj postopkov za zagotavljanje splošne integritete omrežja in sistemov;
- izvajanje analiz in obravnavanje tveganj;
- zagotavljanje ozaveščenosti zaposlenih glede varovanja informacij ter ustrezne usposobljenosti upravljanja z varnostnimi incidenti;
- izvajanje varnostnih ukrepov za izboljšanje stanja varovanja informacij;
- izvajanje nalog na področju projektiranja, varovanja in izkoriščanja, informacijske infrastrukture;
- načrtovanje preventivnih ukrepov;
- pripravljanje predlogov in izvedba korektivnih ukrepov ob varnostnih incidentih.

V naslednjih korakih je potrebno:

- določiti politiko fizičnega varovanja:
    - varovanje fizičnega dostopa, ki naj zajema:
        - evidentiranje vstopa zunanjih oseb v prostore VIZ,
        - varovanje opreme,
        - način hranjena komunikacijske opreme,
        - časovni okvir, kdaj lahko učenci uporabljajo računalniško opremo,
    - varovanje računalnikov in opreme,
    - pravilno namestitev opreme,
    - postopke za prijavo okvare opreme,
- določiti politiko rabe informacijskega sistema:
    - korektna uporaba šolskega informacijskega sistema (npr. nalaganje škodljive programske opreme je kršitev varnostne politike),
    - postopki ob sumu, da je na informacijskem sistemu škodljiva koda,
    - nadzor informacijskega sistema,
    - dostop do podatkov v informacijskem sistemu, ki naj zajema:
        - opredelitve, kdo in kako lahko dobi uporabniško ime in geslo za dostop,
        - določitev ustreznih uporabniških pravic,

        - časovna opredelitev veljavnosti uporabniškega računa (npr. ob odhodu učenca ali zaposlenega iz VIZ),
        - postopek ob prijavi suma zlorabe ali odtujitve,
        - ureditev oddaljenega dostopa,
    - upoštevanje načela čiste mize in praznega zaslona,
- določiti politiko primerne rabe internetnih storitev:
    - nadzor dostopa do svetovnega spleta in njegovih storitev,
    - vzpostaviti politiko uporabe elektronske pošte,
- določiti politiko varovanja podatkov:
    - kontrola dostopov do podatkov,
    - nadzor uporabe izmenljivih medijev,
- določiti politiko zunanjih izvajalcev (vsi dostopi zabeleženi),
- določiti politiko upravljanja omrežja:
    - urediti sinhronizacijo časa,
    - zagotoviti ločitev omrežij in vzpostaviti nadzor dostopa do omrežja,
    - določiti politiko upravljanja incidentov,
    - urediti dnevniške zapise,
    - urediti izvajanje varnostnih kopij,
- določiti politiko vzdrževanja informacijskih sistemov:
    - vzdrževanje opreme in vzdrževalna dela,
- določitev varnostne politike povezane z uporabnikom:
    - izobraževanje uporabnikov
- določiti ukrepe ob kršenju varnostne politike.

7. ZAKLJUČEK

Vzpostavitev ustreznega nivoja informacijske varnosti je ključnega pomena pri zagotavljanju neprekinjenega delovanja računalniškega omrežja v VIZ.

V nalogi smo prikazali stanje na področju varovanja IKT v VIZ v Sloveniji. S pomočjo ankete, na katero je odgovorilo 97 skrbnikov računalniških omrežij na VIZ, smo preverili, kako skrbijo za varnost IKT. Rezultati ankete so pokazali, da kljub rednemu delu poskušajo skrbniki čim bolje poskrbeti za varnost sistemov na njihovem VIZ. V želji po pridobitvi dodatnih znanj se večinoma samoiniciativno, nekateri celo na lastne stroške, udeležujejo izobraževanj. Vsi so si enotni, da imajo premalo časa, za kar krivijo sistematizacijo delovnega mesta skrbnika. Dodatne težave jim povzročajo tudi uporabniki (zaposleni), ki jih ne skrbi niti za lastno varnost. Glede na izkušnje in podane odgovore skrbnikov lahko sklepamo, da so na anketo odgovorili naprednejši skrbniki, ki imajo na svojih zavodih poskrbljeno za varnost sistemov.

Po pregledu podatkov, dostopnih na spletu, in dobljenih informacij NREN-ov ter kontaktnih oseb iz drugih držav smo pridobili informacije, kako se z varnostjo spopadajo v drugih državah. Podobno kot v Sloveniji večinoma nimajo predpisane sistemske ureditve, kako poskrbeti za varnost, zato si vsaka šola prilagaja rešitve glede na svoje potrebe. Nekatere države uporabljajo rešitve na podlagi odprte kode (Estonija), medtem ko drugje uporabljajo plačljive rešitve (Hrvaška). Preučili smo možnosti, kako lahko posamezne primere dobrih praks uporabimo v Sloveniji.

Glede na to, da v Sloveniji ni sistematično urejenega delovnega mesta skrbnika informacijskega sistema v VIZ, niti ni določena varnostna politika na nivoju pristojnega ministrstva, bi že ureditev teh dveh področij, skupaj z dopolnjenimi priporočili o standardih in normativih programa Računalniško opismenjevanje in informatika, dvignila nivo ozaveščenosti na VIZ in pripomogla k izboljšanju varnosti in zaščite.

Arnes bi lahko, z znanjem svojih strokovnjakov, izvajal izobraževanja na temo informacijske varnosti, s čimer bi se dvignil tudi nivo znanja skrbnikov informacijskih sistemov na VIZ. S pomočjo novih storitev, kot je npr. preverjanje ranljivosti omrežja, bi se "luknje" v omrežju prej odkrile in zakrpale. Poleg tega bi Arnes lahko izdelal priporočila za izgradnjo, vzdrževanje in varovanje računalniških sistemov. Predlog takih priporočil smo pripravili v okviru tega magistrskega dela.

Ena izmed prvih in najpomembnejših nalog VIZ je preveriti trenutno stanje in na podlagi potreb izdelati varnostno politiko. Za to nalogo je potrebno določiti osebo, ki bo ustrezno dokumentacijo pripravila in skrbela za njeno izvajanje. Opredeliti je potrebno ukrepe ob kršitvi varnostne politike ter poskrbeti za njihovo dosledno izvajanje. Skrbniki računalniških omrežij na VIZ so v anketi navedli tudi, da so uporabniki premalo ozaveščeni o informacijski varnosti, kar predstavlja veliko varnostno tveganje. Zato je potrebno poskrbeti tudi za redno in sistematično izobraževanje uporabnikov računalniških omrežij na VIZ.

Na podlagi celovitega pregleda obstoječega stanja nad obravnavano problematiko smo podali predloge, kako lahko na različnih nivojih doprinesemo k izboljšanju stanja na področju zagotavljanja informacijske varnosti na slovenskih VIZ. Upamo si trditi, da bi z realizacijo naših priporočil lahko dosegli korak naprej na tem področju. Seveda pa se zavedamo, da so ključni element zagotavljanja varnosti ljudje. Niti najboljša priporočila, navodila in varnostne politike ne koristijo, če se skrbniki računalniških sistemov, uporabniki samih sistemov, predvsem pa vodstva VIZ ne zavedajo resnosti problematike zagotavljanja varnosti IKT omrežij in podatkov na VIZ.

LITERATURA IN VIRI

Bøe, G., Enstad, P.A., Eilertsen , Ø: Recommended ICT Security Architecture In the Higher Education Sector, dosegljivo na: http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-ufs122.pdf, junij 2014.

Brezavšček, A. (2008): Varnost informacijskega sistema, učno gradivo, Univerza v Mariboru, Fakulteta za organizacijske vede, Kranj.

Brezavšček, A. (2009): Varnost računalniških omrežij, učno gradivo, Univerza v Mariboru, Fakulteta za organizacijske vede, Kranj.

Cisco: IPv6 First-Hop Security Concerns, dosegljivo na naslovu: http://www.cisco.com/web/about/security/intelligence/ipv6_first_hop.html, maj 2014.

CiscoLive: Understanding and Preventing Layer-2 Attacks in IPv4 and IPv6 networks (BRKSEC-2202), CiscoLive Melbourne 2013 , dosegljivo na naslovu: https://www.ciscolive.com/, maj 2014.

Dos.Wikipedija, dosegljivo na naslovu: http://sl.wikipedia.org/wiki/Napad_za_zavrnitev_storitve, julij 2014.

Dumpster Diving.Abaut.com, dosegljivo na naslovu: http://netsecurity.about.com, junij 2014.

Ellesmere Primary School: ICT Security Policy, dosegljivo na: http://www.ellesmereprimaryschool.org.uk/Ellesmere_Primary/Policies.html, junij 2014.

Firewal.cx: Presentation layer, dosegljivo na: http://www.firewall.cx/networking-topics/the-osi-model/177-osi-layer6.html, junij 2014.

Frogie, S: Security Reference Guide, dosegljivo na naslovu: http://www.informit.com/guides/content.aspx?g=security&seqNum=39 , marec 2014.

Greg M.: Hack the stack: Using snort and Ethereal to master the 8 layer of insecure network, Syngress Publishing, 2006).

Greengard, S.: 6 pogostih napak varnosti IT in kako se jim izognit, dosegljivo na naslovu: http://www.microsoft.com/business/smb/sl-si/varnost/izogibanje-pogostih-napak-pri-it.mspx, marec 2014.

Heartbleed, dosegljivo na naslovu: http://heartbleed.com/, julij 2014
Informacijska varnost. Wikipedija, dosegljivo na naslovu: http://en.wikipedia.org/wiki/Network_security, marec 2014.

Information diving. Wikipedija, dosegljivo na naslovu: http://en.wikipedia.org/wiki/Information_diving, marec 2014.

IP RS(a): Socialni inženiring in kako se pred jim ubraniti, dosegljivo na naslovu: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/socialni-inzeniring-in-kako-se-pred-njim-ubraniti.pdf, marec 2014.

IP RS(b): Varstvo osebnih podatkov, dosegljivo na naslovu: https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/?tx_jzvopdecisions_pi1[showUid]=2197&cHash=325d43da1ff3cefc8012f2764a6cb698, junij 2014.

Kazenski zakonik RS (KZ1-UPB2); Uradni list RS, št. 50/2012, dosegljivo na naslovu: http://www.uradni-list.si/1/content?id=109161&part=u&highlight=Kazenski+zakonik#!/Kazenski-zakonik-%28KZ-1-UPB2%29-%28uradno-precisceno-besedilo%29, maj 2014.

Kozak , G.: Varnost in PHP, najbolj pogoste varnostne luknje in primeri napadov, dosegljivo na: http://gasper.kozak.si/blog/wp-content/talks/phpkonf2009/php_in_varnost-phpkonf_2009.pdf, julij 2014.

MIZŠ: Evidenca vzgojno-izobraževalnih zavodov in vzgojno-izobraževalnih programov, dosegljivo na: https://krka1.mss.edus.si/registriweb/Default.aspx, junij 2014.

MIZŠ(a): Priporočila o standardih in normativih programa Računalniško opismenjevanje in informatika za leti 2014 in 2015, dosegljivo na: http://www.mizs.gov.si/fileadmin/mizs.gov.si/pageuploads/drugo/TransferHw14_Prip_p2_Koncno.doc, avgust 2014.

Moj Mikro: Socialni inženiring, dosegljivo na spletu: http://www.mojmikro.si/v_srediscu/razkritje/socialni_inzeniring, junij 2014.

Murn, A: Prevare na Facebooku, dosegljivo na: http://www.preberite.si/prevare-na-facebooku/, julij 2014.

Safe-si: Projekt SAFE-SI, dosegljivo na naslovu: http://www.safe.si, april 2014.

Shoulder surfing. Wikipedija, dosegljivo na naslovu: http://en.wikipedia.org/wiki/Shoulder_surfing_(computer_security), marec 2014.

Si-cert: Si-cert poročilo o omrežni varnosti za leto 2013, dosegljivo na https://www.varninainternetu.si/wp-content/uploads/sites/3/2014/03/Porocilo-o-omrezni-varnosti_2013.pdf, marec 2013.

Sotirov , A., Stevens , M., Appelbaum, J., Lenstra, A., Molnar , D., Osvik, D. A., de Weger, B.: MD5 considered harmful today, dosegljivo na: http://www.win.tue.nl/hashclash/rogue-ca/, julij 2014.

Strosar , E.: XSS za velike in male, dosegljivo na: http://www.monitor.si/clanek/xss-za-velike-in-male, julij 2014.

Štraser, S.: Celoviti pristop pri zagotavljanju informacijske varnosti v osnovni šoli, magistrsko delo, 2012.

Technopedia, dosegljivo na: http://www.techopedia.com/definition/9760/transport-layer, junij 2014.

Us-cert: DDoS Quick Guide, dosegljivo na: http://www.us-cert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf , julij 2014.

Varni na internetu: Projekt Varni na internetu, dosegljivo na naslovu: https://www.varninainternetu.si/, april 2014.

Vehar, K.: Projekt vpeljave SUV v podjetje Alpina, d. o. o., magistrsko delo, 2012.

Vyncke, E.: IPv6 security, dosegljivo na naslovu: http://go6.si/wp-content/uploads/2011/11/evyncke-ipv6-security-go6.pdf, marec 2014.

Ostala literatura:

Cerar G.: Črni scenariji prisluškovanja, http://www.mladina.si/95334/crni-scenariji-prisluskovanja/ , maj 2014.

Cgisecurity: Ethical Hacking Techniques to Audit and Secure Web-enabled Applications; dosegljivo na naslovu: http://www.cgisecurity.com/pen-test/auditing-and-securing-web-enabled-applications.pdf, marec 2014.

Čeh, B.: Zagotavljanje varnosti računalniških sistemov, diplomsko delo, 2013.

Drča, M.: Varnost v omrežjih s protokolom IPv6, diplomsko delo, 2010.

Experimental Computer Systems Lab : A Survey on Solutions to Distributed Denial of Service Attacks Applications; dosegljivo na naslovu: http://www.ecsl.cs.sunysb.edu/tr/TR201.pd, marec 2014.

Goggi, C.: The Ultimate Network Security Checklist, dosegljivo na naslovu: http://www.gfi.com/blog/the-ultimate-network-security-checklist/ , maj 2014.

Hogg S., Vyncke E.: IPv6 security, Cisco Press, 2009.

Interno gradivo Arnes in Si-cert.

Korpar, D.: Internet in varnost otrok v osnovni šoli, dosegljivo na naslovu: http://student.pfmb.uni-mb.si/~dkorpar/e-prirocnik/index.html, april 2014.

Marn, B.: Primerjava napadov na protokola IPv4 in IPv6, diplomsko delo, 2008.

Penn State Cyber Security Lab: Hacking Techniques in Wired Networks, dosegljivo na naslovu: http://s2.ist.psu.edu/paper/hack-wired-network-may-04.pdf, maj 2014.

Poklar B., Čotar, D., Đorović, A., Tesić, J.: Proxy strežnik v šolskem krajevnem omrežju, dosegljivo na naslovu: http://www2.sts.si/arhiv/proxy/, maj 2014.

Prabhaker M.: Hacking Techniques in Wireless Networks, dosegljivo na naslovu: http://www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.htm , marec 2014.

SIO: Projekt SIO, dosegljivo na naslovu: http://www.sio.si/, april 2014.

The Open Web Application Security Project (OWASP), dosegljivo na naslovu: https://www.owasp.org, marec 2014.

PRILOGE

Priloga 1:

Anketa: Varnost informacijskega sistema na VIZ

Q22 – Splošna vprašanja

1. Spol:

Moški
Ženski

2. V katero starostno skupino spadate?

do 20 let
21–40 let
41–60 let
61 let ali več

3. Kakšna je vaša stopnja izobrazbe?

Srednja šola
Fakulteta
Magisterij, doktorat

4. Kakšno je vaše delovno mesto?

Informatik/ROID
Učitelj/vzgojitelj
Hišnik
Zunanji izvajalec
Drugo:

5. Tip organizacije, kjer ste zaposleni:

Osnovna šola
Srednja šola
Vrtec
Glasbena šola
Višja strokovna šola
Osnovna šola za otroke s posebnimi potrebami
Organizacija za izobraževanje odraslih
Zavod za otroke in mladostnike s posebnimi potrebami
Dijaški dom
Drugo:

6. Koliko % delovnega časa ste zaposleni kot skrbnik informacijskega sistema (računalnikar)?

0–20 %
10–20 %

30−40 %
50−60 %
70−90 %
polni delovni čas

7. Na koliko organizacijah opravljate funkcijo skrbnika sistema?

1
2−4

8. Koliko skrbnikov informacijskega sistema je zaposlenih na vaši organizaciji?

1
2
Več (koliko):

9. Ali ste se v času, odkar vam je bila zaupana vloga skrbnika informacijskega sistema, izobraževali na temo informacijskih tehnologij in/ali zagotavljanja informacijske varnosti?

DA
NE

10. Ali ste se izobraževanja udeležili na lastno iniciativo in/ali stroške ali je za to poskrbela organizacija, kjer ste zaposleni?

Možnih je več odgovorov:
Lastna incicativa
Stroške sem kril sam
Stroške je krila organizacija, kjer sem zaposlen
Drugo:

11. Zakaj se izobraževanja niste udeležili?

Možnih je več odgovorov:
Ni bilo primernega izobraževanja
Organizacije, kjer sem zaposlen, ni bila pripravljena kriti stroškov
Ni bilo časa
Takšna izobraževanja me ne zanimajo
Izobraževanje ni bilo točkovano
Drugo:

12. Ali bi se izobraževanja na temo informacijskih tehnologij udeležili, čeprav le-to ne bi bilo točkovano?

DA
NE

13. Ali je omrežje, za katerega skrbite, povezano v omrežje ARNES?

DA
NE

Ne vem

14. Ali je omrežje, za katerega skrbite, ločeno na pedagoški in administrativni del?

DA
NE
Ne vem

15. Vodite dokumentacijo o omrežju na vaši organizaciji (stanje filtrov, dodeljeni in porabljeni IP naslovi, skica omrežja ...)

DA
NE
Delno

16. Imate za usmerjevalnikom, ki ga upravlja Arnes, postavljen še svoj usmerjevalnik?

DA
NE

17. Kakšna je funkcija tega usmerjevalnika?

Možnih je več odgovorov:

Upravljanje omrežja
Brezžično omrežje
Zaščita omrežja
VPN
Drugo:

18. Uporabljate NAT/PAT?

DA
NE
Ne vem

19. Imate postavljen svoj požarni zid (poleg zaščite na usmerjevalniku)?

DA
NE
Ne vem

20. Imate v organizaciji vzpostavljeno brezžično omrežje?

DA
NE

21. Kakšno avtentikacijo za brezžično omrežje uporabljate?

Možnih je več odgovorov:
WEP PSK

WPA/WPA2 PSK
Uporabljamo Eduroam
Ne uporabljamo avtentikacije
Ne vem
Drugo

22. Imate brezžično omrežje za goste v ločenem podomrežju?

DA
NE
Ne vem

23. Uporabljate IPv6 protokol?

DA
NE
Ne vem

24. Imate na operacijskih sistemih Windows Vista in novejših izklopljene IPv6 translacijske mehanizme (Terredo ...)?

DA
NE
Ne vem
Ne vem, kaj je IPv6 pokol

25. Ima vaša organizacija postavljen strežnik?

DA
NE

26. Kje ima vaša organizacija postavljen strežnik?

Možnih je več odgovorov:
Lokalno na organizaciji
Na Arnesu
MS Azure
Amazon EC2/EWS
Drugje:

27. Na strežniku tečejo naslednje storitve:

Možnih je več odgovorov:
WWW
FTP
MAIL
DNS
RADIUS
LDAP
DHCP
Aktivni imenik

28. Uporabljate sistem za upravljanje z vsebinami (CMS)?

DA
NE
Ne vem

29. Kateri strežnika za upravljanje vsebin (CMS) uporabljate?

Možnih je več odgovorov:
Joomla
Drupal
Moodle
Wordpress
Drugo:

30. Ali ste že imeli vdor v sistem (strežnik)?

DA
NE
Ne vem

31. Kaj je bila posledica vdora?

Možnih je več odgovorov:
Razobličenje spletne strani
Kraja podatkov
Strežnik je bil uporabljen v napadih na drug sistem
Strežnik je pošiljal neželeno pošto
Drugo:

32. Ste vdor v sistem zaznali sami?

DA
NE
Obveščeni smo bili s strani SI-CERT-a
Drugo:

33. Kaj ste storili, ko ste opazili oz. bili obveščeni o vdoru v sistem?

Možnih je več odgovorov:

O tem sem obvestil SI-CERT
Strežnik izklopil iz omrežja
Ugasnil strežnik
Počistil strežnik
Zakrpal varnostno luknjo
Sporočil na Arnes, da s filtri onemogočijo dostop do strežnika

34. Ali zaposleni uporabljajo za dostop do službenih računalnikov oddaljeno namizje (RDP)?

DA
NE

Ne vem

35. Imate omogočen dostop do službenih računalnikov preko oddaljenega namizja (RDP)? Iz celotnega interneta

Samo iz določenih IP naslovov
Ne vem

36. Kakšen je časovni razpon zamenjave osebnih gesel na službenih računalnikih?

Do 1x na mesec
Večkrat letno
Uporabnikom ni potrebno spreminjati gesel
Na računalnikih ni gesel

37. Kje se nahaja komunikacijska oprema?

Možnih je več odgovorov:
V klimatiziranem prostoru
V komunikacijski omari
V posebnem prostoru, ki je namenjen samo računalniški opremi
V tajništvu/zbornici/pri ravnatelju na polici ali pod mizo
V učilnici
Drugo:

38. Kdo ima dostop do prostora, kjer se nahaja komunikacijska oprema?

Možnih je več odgovorov:
Skrbnik sistema
Direktor/ravnatelj
Hišnik
Zaposleni
Učenci
Kdor koli
Drugo:

39. Prostor, kje se hrani komunikacijska oprema, je:

Možnih je več odgovorov:
Zaščiten z alarmnim sistemom
Opremljen z javljalniki požara
V neposredni bližini so gasilni aparati za gašenje računalniške opreme
Prostor je opremljen z avtomatskim gasilnim sistemom
Zaščiten pred vdorom vode
Urejen sistem obveščanja ob izrednih dogodkih (izpad klime, visoka temperatura, izliv vode ...)
Drugo:

40. Ali se obiskovalci lahko prosto gibajo po stavbi organizacije?

DA
NE

41. Ali za zagotavljanju nemotenega delovanja električnih naprav in uravnavanje napetostnih nihanj uporabljate UPS?

DA
NE
Ne vem, kaj je UPS

42. Ali ste že imeli okvaro komunikacijske opreme?

DA
NE

43. Kaj je bil vzrok okvare?

Možnih je več odgovorov:
Dotrajanost
Udar strele
Izliv vode
Nestrokovno ravnanje
Nepooblaščen dostop
Drugo:

44. Koliko časa je trajal povprečni izpad?

do 1 ure
2−3 ure
več ur
en dan
več

45. Imate za vzdrževanje strojne opreme urejeno vzdrževalno pogodbo?

DA
NE
Ne vem

46. Imate urejeno varnostno kopiranje ključnih podatkov?

DA
NE
Ne vem

47. Kaj uporabljate za hranjenje varnostnih kopij?

Možnih je več odgovorov:
Isti strežnik, na katerem se nahajajo izvorni podatki
Zunanjo enoto (disk, CD, trak ...)
GoogleDrive

MS One Dive
Arnes Shrambo
Arnes Mapo
Amazon
Drugam:

48. Kateri program/storitev uporabljate za delo z dokumenti?

Možnih je več odgovorov:
MS Office na računalnikih
Office 365 v oblaku
GoogleDrive
LibreOffice
Drugo:

49. Ali ima vaša organizacije dokumentirana IT varnostna priporočila?

DA
NE
Ne vem

50. Ali menite, da so uporabniki vašega informacijskega sistema na področju informacijske varnosti dovolj ozaveščeni?

DA
NE
Ne vem

51. Kaj vam pri opravljanju dela skrbnika informacijskega sistema predstavlja največjo oviro in kako bi to izboljšali?

Priloga 2

PRIPOROČILA ZA ZAŠČITO INFORMACIJSKIH SISTEMOV V VIZ V SLOVENIJI

Navodila so izdelana na podlagi analize trenutnega stanja v Sloveniji in v skladu s predlaganimi smernicami in dobrimi praksami iz tujine.

Gre za nadgradnjo priročnika "Varnost šolskih omrežij", ki je bil leta 2002 izdan s strani Arnesa.

1. Osnove zagotavljanja varnosti omrežij VIZ

Osnovni pogoji za zagotovitev sprejemljive ravni varnosti šolskega omrežja so (Straus, 2002):

- ustrezna oprema, ki ima možnost zagotavlja spodaj napisanega;
- fizična ločitev šolskega omrežja od interneta, kar je glavna naloga usmerjevalnika prometa ali L3 stikala (stikal z okrnjenimi funkcijami usmerjevalnika), s katerim je šola povezana v internet;
- fizična ločitev administrativnega dela omrežja od pedagoškega dela v učilnicah, brezžičnega in omrežja za goste (segmentacija omrežja);
- uporaba brezžičnih omrežij z enim izmed varnostnih protokolov;
- uporaba znanih in varnih internetnih storitev;
- filtriranje internetnega prometa;
- zaščita strežnikov in ostalih naprav v omrežju.

Prvi pogoj je izpolnjen, če je VIZ povezan v omrežje ARNES. Vmesnik, s katerim se ta usmerjevalnik ali L3 stikalo poveže v omrežje ARNES, imenujemo WAN vmesnik (angl. wide area network). Lokalna omrežja na VIZ so priključena na vmesnike, ki jim pravimo LAN vmesniki (angl. local area network). Usmerjevalnik prometa ali L3 stikalo si lahko deli več organizacij. Taki priključni točki rečemo Točka Skupine Priklopa (TSP). V tem primeru je vsaka organizacija priključena na svoj LAN vmesnik preko stikala.

1.1. Nakup komunikacijske opreme

Najprej je potrebno kupiti ustrezno komunikacijsko opremo, da se bodo lahko zagotavljali varnosti mehanizmi. V nadaljevanju je za posamezen tip naprave podanih nekaj priporočil.

Tehnična priporočila za stikala:

- podpora VLAN:
  - protokol 802.1Q (VLAN tagging, VLAN trunking ...);
- na vmesniku z 802.1Q (VLANi) podpora za več VLAN-ov;
- podpora za 802.1s (Spanning Tree per VLAN Group);
- podpora za 802.1w (RSTP − Rapid Spanning Tree Protocol);
- podpora za protokol 802.1X;

- varnostni mehanizmi za IPv4 protokol:
  - Port Security,
  - DHCP Snooping,
  - Dynamic ARP inspection;
- varnostni mehanizmi za IPv6 protokol:
    - IPv6 RA Guard:
  - DHCPv6 Guard,
  - IPv6 Snooping and device tracking,
  - IPv6 Source Guard,
  - IPv6 Prefix Guard,
  - IPv6 Destination Guard;
- broadcast, multicast, and unicast storm control;
- dostop za upravljanje preko SSH ali HTTPS protokola;
- možnost nadzora preko SNMP protokola;
- možnost shranjevanja/nalaganja konfiguracijske datoteke in nalaganja novih verzij programske opreme s TFTP ali FTP;
- podpora zunanjega strežnika za avtentikacijo (TACACS+ ali RADIUS);
- podpora za Quality Of Service (QOS) mehanizme;
- podpora za IPv6 in IPv6 multicast;
- podpora Syslog;
- možnost vgradnje v 19" komunikacijsko omaro;
- v primeru uporabe IP telefonija ali Wifi dostopnih točk, še podpora za standard IEEE 802.3at Power over Ethernet (PoE).

Tehnična priporočila za usmerjevalnik prometa:

- IPv4 in IPv6 statično usmerjanje;
- Ethernet;
- podpora za protokol 802.1q VLAN;
- podpora za "Point-to-Point Protocol over Ethernet" (PPPoE);
- DHCP strežnik;
- dostop za upravljanje preko SSH ali HTTPS protokola;
- možnost nazora preko SNMP protokola;
- podpora za Quality Of Service (QOS) mehanizme;
- podpora Syslog;
- podpora za VPN protokole (potrebno paziti koliko VPN tunelov se lahko zaključi in koliko prometa zmore šifrirati in dešifrirati).

Tehnična določila za brezžične dostopne točke:

- vsaj dva ločena radijska vmesnika, ki delujeta hkrati; eden na 2.4 GHz vmesniku in eden na 5 GHz vmesniku;
- vsaj en 2.4 GHz radijski vmesnik, 802.11n, navzdol združljiv z odjemalci 802.11b in 802.11g;
- vsaj en 5 GHz radijski vmesnik, 802.11n, navzdol združljiv z odjemalci 802.11a;
- radijski del mora znati delovati z dvema ali večimi antenami v načinu MIMO, z vsaj dvema prostorskima tokovoma (angl. spatial stream);

- zadoščati mora slovenskim predpisom za radijske naprave glede moči oddajnika, frekvenc in ostalih tehničnih določil;
- hkratna uporaba vsaj 4 SSIDjev;
- zmožnost oglaševanja vsaj 4 SSIDjev hkrati;
- šifriranje brezžične povezave z WPA2 (s strojno podprtim šifriranjem AES), po standardu 802.11i;
- podpora WPA2-PSK;
- podpora WPA2 + 802.1x (WPA2-Enterprise);
- hkratna uporaba WPA2-PSK in WPA2-Enterprise na ločenih SSIDjih;
- podpora WMM QoS po standardu organizacije WiFi;
- protokol 802.1Q;
- dinamično umeščanje uporabnika v VLAN glede na nastavitve RADIUS;
- dodeljevanje uporabnika v VLAN glede na SSID, na katerega se uporabnik priključuje;
- ločeni VLAN za upravljanje dostopne točke (angl. management access), lahko tudi zgolj neoznačen (angl. untagged, native);
- nastavljanje z uporabo varnega spletnega vmesnika (protokol HTTPS);
- dosegljiv z oddaljenega računalnika preko protokola SSH;
- podpora Syslog.

Točke, ki so primerne za vzpostavitev omrežja Eduroam in so bile testirane, so objavljene na spletni strani Arnesove AAI skupine: https://aai.arnes.si/eduroam/oprema.

2. Varovanje omrežne opreme

Ustrezna oprema je brez koristi, če ni primerno shranjena. Glavna komunikacijska omara naj bo dovolj zračna in naj omogoča vgraditev 19" strežnika. Prostor, kjer bo shranjena oprema, naj bo:

- lociran v pritličju na dvignjenem podu ali višje v zgradbi;
- klimatiziran;
- namestitev gasilnih aparatov za gašenje računalniške opreme (CO2 ali vodno peno) v prostoru;
- namestitev javljalnikov požara in naraščajoče vode;
- vrata in po možnosti zidovi naj bodo izdelani iz ognjevarnih materialov;
- napajanje opreme v komunikacijski omari naj bo na ločeni varovalki;
- Za preprečitev izpada ali nihanja električne energije naj se omogoči:
    - izklop električnega napajanja s samo enim stikalom;
    - urejen sistemom za uravnavanje napetostnih nihanj in nadomestno napajanje (Uninterruptible Power Supply – UPS), ki naj ima primerno moč glede na opremo priklopljeno nanj.

Vendar pa nam vse varnostne funkcije, ki jih omogoča oprema, ne koristijo, če fizični dostop do prostora ni zaščiten. Prostor naj bo:

- lociran tako, da je lahek dostop omogočen samo pooblaščenim osebam;
- vsi vstopi naj bodo kontrolirani s pomočjo kontrole pristopa;
- dostop do prostora naj ima samo skrbnik sistema in njegov pomočnik;

- gibanje po stavbi VIZ naj bo nadzorovano.

S fizično zaščito preprečimo fizični dostop do opreme in posledično napade, ki jih napadalec lahko izvede(kraja podatkov, prisluškovanje, napad na strojno opremo …).

3. Segmentacija omrežja

Omrežje mora biti razdeljeno na različne cone in varnostne razrede, ki morajo biti v skladu z oceno tveganja. Vsaka cona ima lahko eno ali več omrežij. Priporočljivo je, da se vzpostavijo tri cone: odprta, notranja in varna cona. Dostop do storitev pa mora biti pod nadzorom ustreznih varnostnih pregrad.

3.1. Določitev con

V nadaljevanju bodo prestavljene posamezne cone in katere storitve v njih umestiti.

a) Odprta cona

V odprto cono bi umestili:

- omrežje za goste,
- zunanje spletne strežnike,
- tiskalniške strežnike,
- aplikacije za učence,
- osebno opremo (domači telefoni, domači prenosniki, domače tablice …).

Za vse strežnike je potrebno urediti, da se vodijo dnevniški zapisi in izvaja redno krpanje varnostnih lukenj ter posodabljanje. Na strežnikih naj se onemogočijo nepotrebne storitve.Npr. če se strežnik ne uporablja kot DNS strežnik, je smiselno na njemu to storitev izklopiti.

Za dostop do brezžičnih omrežij je smiselno imeti urejeno omrežje Eduroam ali podobno implementacijo standarda 802.1X. Poseben dostop (npr. WPA2-PSK z dolžino ključa vsaj 25 znakov) je potrebno urediti tudi za goste, ki nimajo dostopa do omrežja Eduroam in zagotoviti enkrat tedensko menjavo gesla. Primer skripta za menjavo gesel na Cisco in Lancom dostopnih točkah najdete na spletni strani Arnesove AAI skupine (https://aai.arnes.si/eduroam/dodatnoPSK). Podoben način avtentikacije mora biti urejen tudi na žičnem delu v učilnicah.

Z vzpostavitvijo omrežja Eduroam se preprečijo napadi na brezžična omrežja, kot so: prisluškovanje (promet med dostopno točko in odjemalcem je šifriran), napadalec se brez uporabniškega imena in gesla ne more prijaviti v brezžično omrežje, prestrezne dostopne točke (vsaka dostopna točka mora biti vpisana v Radius strežnik).

Vendar je strežnike in odjemalce potrebno imeti v ločenih omrežjih znotraj te cone.

b) Interna (notranja) cona

V interno cono bi spadale naslednje storitve:

- DHCP-strežnik,
- IP telefonija,
- rekurzivni DNS,
- aktivni imenik,
- interni poštni strežniki,
- datotečni strežniki za domače mape zaposlenih,
- internet spletne strani,
- koledar,
- tiskalniški strežniki,
- sistemi za upravljanje zgradbe (klima, nadzor kurjave …),
- sistemi za upravljanje avdio/video opreme,
- oprema za videonadzor,
- sistemi za arhiviranje,
- administrativni sistemi,
- administrativni strežniki, ki niso nameščeni v varni coni (npr. računovodstvo),
- strežniki za nadzor omrežja in storitev, stikal, usmerjevalnikov, dostopnih točk …

Gre za interne segmente, ki jih uporabljajo zaposleni in ostali, povezani z zavodom; do teh segmentov naj ne bi bil omogočen dostop iz naprav, ki niso v omrežju članice. Za strežnik v interni coni veljajo enake zahteve kot v odpri coni. Za odjemalce velja, da imajo skrbniške pravice samo skrbniki sistemov, glede operacijskega sistema morajo ustrezati zahtevam zavoda, protivirusna programska oprema mora biti posodobljena na zadnjo različico, naprave, ki niso v lasti zavoda in le-ta za njih ne skrbi, naj ne bi bile v tej coni.

Vse naprave v tej coni bi morale biti avtenticirane (npr. 802.1X) in vsi uporabniki avtenticirani preko centralne baze uporabnikov. Sistemi, ki ne podpirajo centralne avtentikacije, morajo biti še posebej zaščiteni.

S protokolom 802.1X se, podobno kot že omejeno pri omrežju Eduroam, prepreči nepooblaščena prijava v računalniško omrežje in izvedba napada znotraj omrežja.

Odjemalci v interni coni morajo biti centralno nadzorovani, skrbniške pravice naj ima samo skrbnik sistema. Vsi operacijski sistemi morajo biti v skladu s pravili zavoda, protivirusni programi pa posodobljeni na zadnjo verzijo. Za interno cono ni priporočljivo, da se v njej nahajajo naprave, ki niso nadzorovane s strani zavoda.

c) Varna cona

V varno cono bi vključili:

- občutljive osebne podatke in posnetke videonadzora,
- sisteme za zaklepanje,

- kontrolo pristopa,
- varnostne kopije.

V varni coni je potrebno poskrbeti še za dodatne varnostne ukrepe, kot so: preverjanje celovitosti, zaznavanje vdorov, šifriranje podatkov, utrjevanje varnosti in centralno hranjenje dnevniških zapisov.

Odjemalcev v to cono naj ne bi vključevali. Tisti, ki pa dostopajo do storitev v tej coni, naj bi bili vključeni v interno cono. Posebno skrb je potrebno nameniti tudi oddaljenemu dostopu.

Uporabnike, ki želijo dostopati do varne cone, je potrebno še enkrat avtenticirati.

3.2. Segmentacija omrežja s pomočjo VLAN-ov

Da bi lahko zagotovili različna omrežja cone, je potrebno na usmerjevalniku in stikalu konfigurirati VLAN-e.

VLAN-i omogočajo skrbniku omrežja logično segmentacijo omrežja v ločene domene "broadcast". Ker gre za logično in ne fizično segmentacijo, lociranje delovnih postaj na isti lokaciji ni več potrebno. Uporabniki v različnih zgradbah lahko tako pripadajo istim omrežjem LAN. VLAN omogoča definiranje domene broadcast tudi brez uporabe usmerjevalnikov.

VLAN omrežja uporabimo zaradi:

- zmogljivosti – zmanjševanje pošiljanja "broadcast" in "multicast prometa na nepotrebne lokacije;
- zmanjšanja uporabe usmerjevalnikov, saj lahko ustvari domene broadcast kar s stikali;
- kreiranja virtualnih delovnih skupin;
- lažje administracije v primeru premikanja uporabnika med omrežji;
- varnosti – uporabnikom, ki uporabljajo iste podatke, lahko dodelimo isto omrežje VLAN, s čimer zmanjšamo možnost, da bi ostali uporabniki omrežja prišli do podatkov.

Vmesniki na stikalu lahko delujejo v 3 načinih:

- Trunk/Tagged – v primeru lahko preko enega vmesnika speljemo več različnih VLAN-ov (primerno predvsem za povezave med stikali), ki so označeni, neoznačena pa pošlje na privzeti VLAN (običajno Vlan1);
- Acess/Untagged – en vmesnik je lahko samo v enem VLAN-u (priklop naprav);
- Hybrid – podobno kot Trunk, vendar v tem primeru lahko določimo, kam naj pošilja neoznačene pakete.

Spodaj bo predstavljen primer konfiguracije Cisco usmerjevalnika in Cisco stikala. Pri konfiguraciji usmerjevalnika (Slika 69) vidimo, da so konfigurirani 3 virtualni vmesniki, kjer jim z ukazom encapsulation dot1Q in številko povemo oznako VLAN-a (VLAN ID).

```
interface GigabitEthernet0/1
 description ===== vmesnik za povezavo do stikala =====
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.2
 description ===== virtualni vmesnik za pedagoški del =====
 encapsulation dot1Q 2
ip address 194.249.103.65 255.255.255.192
!
interface GigabitEthernet0/1.3
 description ===== virtualni vmesnik za administrativni del =====
 encapsulation dot1Q 3
  ip address 194.249.103.129 255.255.255.224
!
interface GigabitEthernet0/1.30
 description ===== virtualni vmesnik za upravljalni del ======
 encapsulation dot1Q 30
 ip address 178.172.73.52 255.255.255.254
```

Slika 69: Primer konfiguracije Cisco usmerjevalnika

Nato pa je potrebno na stikalu naprej vpisati VLAN-e v bazo VLAN-ov. Sledi konfiguracija vmesnikov, kjer povemo, v kakšnem načinu bo vmesnik deloval (access, trunk ali hybrid) in katere VLAN-e bo sprejemal.

Na vmesniku FastEthernet0/24 dovolimo sprejem teh VLAN-nov (switchport trunk allowed vlan 2,3,30) in na posameznih vmesnikih nastavimo željen VLAN (switchport access vlan 2) (sika 69).

```
!
interface FastEthernet0/1
 description ===== vmesnik za pedagoški del =====
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/14
 description ===== vmesnik za administrativni del =====
 switchport access vlan 3
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/24
 description ===== vmesnik za upravljalni del =====
switchport mode trunk
switchport trunk allowed vlan 2,3,30
```

Slika 70: Primer konfiguracije Cisco stikala

4. Filtriranje prometa

Internetni promet in promet med VLAN-i se na usmerjevalniku ali L3 stikalu filtrira na podlagi naslednjih podatkov (Straus, 2002):

- IP naslov izvora prometa (v nadaljevanju client),
- IP naslov cilja prometa (v nadaljevanju server),
- protokol (TCP, UDP, ICMP ...),
- opis storitve (številki vrat na izvoru in ciljnem sistemu, tip, koda ...),
- dodatni podatki za nekatere protokole, npr. oznaka za že vzpostavljene seje po protokolu TCP.

Internetni promet, ki gre skozi filter, se obravnava na dva načina (Straus, 2002):

- kot promet odjemalcev (angl. client) in
- kot promet strežnikov (angl. server).

Poleg te delitve pa se upošteva tudi smer, v kateri poteka promet. Možnosti sta dve (Straus, 2002):

- promet prihaja v lokalno omrežje iz interneta ali drugega VLAN-a (angl. inbound traffic) in
- promet zapušča lokalno omrežje (angl. outgoing traffic).

Slika 71 prikazuje opis storitve WWW. Ta storitev uporablja protokol TCP – vrata na strežniku so običajno 80 (storitev http), odjemalec pa vedno uporabi vrata z neko poljubno številko, ki je večja od 1023.

Odjemalec/ strežnik	Smer	Protokol	Izvorna vrata	Ciljna vrata	Že vzpostavljena TCP seja?	
Server	in	tcp	>1023	80	/	do strežnika
Client	in	tcp	80	>1023	da	do odjemalca
Server	out	tcp	80	>1023	da	od strežnika
Client	out	tcp	>1'023	80	/	do odjemalca

Slika 71: Opis storitve WWW (Straus, 2002)

Prenos podatkov iz varnega v nevarno omrežje ne potrebuje posebnega varovanja. Poskrbeti je potrebno, da imajo paketi, ki zapuščajo varno omrežje, veljavne IP naslove. "Anti–spoofing" filter preprečuje, da bi računalnik iz varnega območja oddal paket z IP naslovom drugega omrežja ali nedovoljen IP naslov (slika 72).

Prenos podatkov v varno omrežje iz nevarnega je potrebno skrbno nadzorovati.

Da bi preprečili dostop iz enega VLAN-a v drugega, so na virtualnih vmesnikih na usmerjevalniku nastavljeni še filtri (ip access-group). Z access-list 112 omejimo dohodni promet na promet, ki izbira iz naslovnega prostora lokalnega omrežja in se vrača nazaj, ter blokiramo ves promet, ki ima za ponorni IP naslov kaj drugega. Poleg tega dovolimo TCP promet, ki je bil začet iz tega omrežja (angl. established) (slika 72).

Z access-list 113 omejimo odhodni promet iz tega dela omrežja. Blokiramo promet iz privatnih IP naslovov, ki se v internetu ne smejo pojaviti, in dovolimo promet iz naslovnega prostora tega omrežja (slika 70). S tem se tudi prepreči spoofing napade, kar pomeni iz vašega omrežja napadalec ne more izvesti DoS napada s spremenjenim IP naslovom.

```
access-list 112 remark outbound access-list on LAN interface (classroom)
access-list 112 remark ----- anti-spoofing
access-list 112 permit ip 194.249.103.64 0.0.0.63 194.249.103.64 0.0.0.63
access-list 112 deny   ip 194.249.103.64 0.0.0.63 any
access-list 112 permit tcp any 194.249.103.64 0.0.0.63 established
access-list 112 deny   ip any any
!
access-list 113 remark inbound access-list on LAN interface (classroom)
access-list 113 deny   ip any 10.0.0.0 0.255.255.255
access-list 113 deny   ip any 127.0.0.0 0.255.255.255
access-list 113 deny   ip any 172.16.0.0 0.15.255.255
access-list 113 deny   ip any 192.168.0.0 0.0.255.255
access-list 113 permit ip 194.249.103.64 0.0.0.63 any
access-list 113 deny   ip any any log
```

Slika 72: Primer zapisa filtra na Cisco usmerjevalniku

Na sliki 72 je prikazano statično filtriranje prometa (angl. angl. packet oriented). Na usmerjevalniku je filtriranje definirano na osnovi TCP/IP paketov, zato je potrebno ob vhodu v bolj varno omrežje definirati filter za vse pakete, ki jim dopustimo vstop. Taki paketi so:

- Paketi, ki pripadajo predhodno vzpostavljeni seji (angl. TCP established). Pri tem je potrebno opozoriti, da usmerjevalnik ne preverja obstoj takšne seje, temveč le preveri ustrezno 'ACK' oznako v glavi paketa. Prav tako velja opozoriti, da obstajajo tako imenovani nezanesljivi protokoli (angl. bad-behaved protocol), ki so sestavljeni iz več podsej in se vzpostavljajo v obe smeri, zato jih z zgoraj omenjenim filtrom ne moremo zajeti. Tak protokol je FTP v aktivnem (privzetem) načinu.
- Od paketov, ki ne pripadajo (zgoraj omenjenim) vzpostavljenim sejam, dovolimo vstop le tistim, namenjenim točno določenim kombinacijam IP naslovov in TCP/UDP vrat. Konkretno dopuščamo le promet za storitve, ki tečejo na strežniku.

Poleg statičnega lahko promet filtriramo tudi dinamično (angl. session oriented). Navadno se izvaja v posebnih napravah − požarnih zidovih, ki delujejo kot utrdba med varnim in nevarnim omrežjem. Požarni zidovi omogočajo celotno funkcionalnost statičnega filtriranja, kot je omejevanje prometa v obe smeri, dodatno pa vršijo razširjen nadzor prometa iz nevarnega omrežja. Dodatni nadzor se izvaja po postopku CBAC (Contex Based Acess Control). Bistvo tega postopka je beleženje konteksta vsake vzpostavljene seje posebej, s tem lahko požarni zid avtomatično prepušča pakete, ki pripadajo predhodno vzpostavljeni seji.

Pred odpiranjem vrat vedno preverite dokumentacijo storitve ali naprave, ki potrebuje odprta vrata, se pozanimajte pri dobavitelju ali s kakšnim izmed programov za pregledovanje prometa (npr. Wireshark) preverite, preko katerih vrat komunicira.

5. Zaščita pred napadi na povezovalni plasti (L2)

Pod specifikacijami opreme smo že omenili funkcije, ki naj jih stikalo podpira. Med njimi so tudi takšne, ki so potrebne za zaščito pred napadi na povezovalni plasti OSI modela in jih ni mogoče zajeti s filtri na usmerjevalniku ali L3 stikalu.

Osnovna varnostna priporočila za preprečevanje preskakovanja med VLAN-i (Vlan Hopping):

- izklopite vse vmesnike, ki niso v uporabi;
- na "trunk" vmesnikih vedno uporabite dovoljenje za posamezne VLAN-e (slika 70);
- Vlan1 ne uporabljajte.

Za preprečitev MAC poplavljanja je potrebno na stikalu omejiti maksimalno število MAC naslovov na določenem vmesniku.

Slika 72 prikazuje nastavitev varnosti vmesnika. Z zgornjo nastavitvijo vmesnika dovolimo maksimalno 3 MAC naslove, ki si jih zapomni, in števec MAC naslovov z vsakim novim naslovom poveča za 1. Ko doseže 3, vse pakete, ki kot izvor nimajo enega izmed 3 naučenih MAC naslovov, zavrže. Po 2 minutah neaktivnosti določenega MAC naslova, se števec maksimalnih MAC naslovov zmanjša za 1 in lahko si zapomni nov MAC naslov.

```
interface FastEthernet0/1
switchport port-security
switchport port-security violation restrict
switchport port-security maximum 3
switchport port-security aging time 2
switchport port-security aging type inactivity
```

Slika 73: Primer omejitve števila MAC naslovov na CIsco stikalu

Ker mora stikalo pregledovati vse pakete, ki prihajajo na vmesnik, lahko pride do povečane obremenitve procesorja (CPU), kar lahko povzroči nedelovanje stikala. Zato z ukazom mls rate-limit layer2 port-security 1000 omejimo število paketov na vmesniku. Zgornji ukaz nastavi omejitev na 1000 paketov/sekundo.

Poleg MAC poplavljanja s to zaščito preprečimo tudi DHCP stradanje. Poleg DHCP stradanja pa se lahko v omrežju postavi tudi lažni DHCP strežnik, ki dodeli napadalčev prehod, da DNS strežnik izvede DOS napad z neveljavnim IP naslovom. Z namenom preprečitve tega na stikalu vklopimo funkcijo dhcp snooping. Na sliki 73 je primer nastavitve. V globalni konfiguraciji povemo, katere VLAN-e bomo pregledovali, na vmesnikih povemo, ali DHCP zahtevkom zaupamo. Na vmesniku, kjer je priklopljen naš DHCP strežnik, nastavimo, da mu zaupamo (ip dhcp snooping trust), ostali vmesniki DHCP odgovorom ne bodo zaupali. Ker podobno kot pri prejšnjem primeru, lahko pride do povečane aktivnosti procesorja, lahko nastavimo omejitev na število (10) paketov/sekundo.

```
ip dhcp snooping vlan 4,104
no ip dhcp snooping information option
ip dhcp snooping
!
interface FastEthernet0/1
ip dhcp snooping trust
!
interface FastEthernet0/2
ip dhcp snooping limit rate 10
```

Slika 74: Primer nastavitve DHCP snooping

Naslednji v vrsti napadov na IPv4 L2 je poplava z ARP paketi. To lahko preprečimo s funkcijo dynamic arp inspection. Ta omogoča, da se dovoli samo izvorne pakete iz MAC naslovov, kateri IP naslov je bil dodeljen preko DHCP strežnika. Ta funkcija deluje s pomočjo prejšnje (dhcp snooping). Dynamic arp inspection v tabeli, ki jo napolni dhcp snooping, preveri, ali za ta MAC naslov obstaja IP naslov. Sicer ta promet zavrže.

Na sliki 74 je prikazan primer nastavitve na Cisco stikalu. Podobno kot pri dhcp snooping globalno nastavimo, na katere VLAN-e bo to vplivalo in na vmesniku nastavimo zaupanje ter maksimalno število paketov/sekundo. V primeru, da imamo napravo(e), ki imajo statično določen IP naslove, ga lahko v DHCP binding tabelo vpišemo s pomočjo globalnega ukaza ip source binding 0000.0000.0001 vlan 4 10.0.10.200 interface fastethernet 0/2.

```
ip dhcp snooping vlan 4,104
no ip dhcp snooping information option
ip dhcp snooping
ip arp inspection vlan 4,104
!
interface FastEthernet0/1
ip dhcp snooping trust
ip arp inspection trust
!
interface FastEthernet0/2
ip dhcp snooping limit rate 10
ip arp inspection limit rate 15
```

Slika 75: Primer nastavitve dynamic ARP inspection

Pri IPv4 protokolu je pridobivanje IPv4 naslova preko "broadcasta" in UDP vrat 67 in 68, pri IPv6 pa gre za ICMPv6 kontrolna sporočila in UDP vrata 546, 547, t. i. SARR (Solict, Advertise, Request, Reply).

Zaščita je skupek varnostnih mehanizmov, združenih pod imenom IPv6 Snooping (IPv6 address glean, IPv6 device tracking, IPv6 neighbor discovery).

6. Filtriranje vsebine internetnega prometa

Za filtriranje vsebine internetnega prometa je potrebno na zavodu postaviti proxy strežnik, ki ima vlogo posredovanja zahtev in odgovorov med internetom in računalniki v lokalnem omrežju. Poleg tega, da usmerja zahteve, ima proxy strežnik še nekaj pomembnih nalog:

- shranjevanje spletnih vsebin v medpomnilnik;
- skrivanje in varovanje krajevnega omrežja pred nezaželenimi posegi z interneta;
- povezovanje lokalnih omrežij na internet;
- omejevanje dostopa;
- omejevanje storitev;
- omejevane pravic uporabnikom do dostopa na internet;
- omejevanje dostopa do neprimernih spletnih vsebin na internetu;
- filtriranje paketov TCP/IP.

Najbolj razširjen je Squid strežnik, ki teče na Linux operacijskem sistemu. Vendar Squid sam po sebi še ne omogoča filtriranja vsebine. Za to je potrebno namestiti še vtičnik squidGuard.

Druga možnost je uporaba storitve OpenDNS, ki jo uporabljajo šole v Estoniji. Gre za spletno storitev, ki v brezplačni licenci omogoča filtriranje vsebine internetnega prometa, vendar pa žal samo za en IP naslov. Vse, kar je potrebno narediti, je registracija na spletni strani https://opendns.com, določiti, za katera IP naslovna območja želimo izvajati filtriranje ter katere vsebine želimo filtrirati.

Z ustrezno licenco je možno filtriranje izvajati tudi s pomočjo Cisco usmerjevalnika.

Na spletu se pojavlja čedalje več neprimernih vsebin in pristojno ministrstvo bi moralo poskrbeti za ustrezno zaščito pred škodljivimi vsebinami. Podobno, kot je to storilo ministrstvo na Hrvaškem.

Vendar pa je v avgustu 2014 Safe.si objavil raziskavo Ofseda iz Velike Britanije. Ugotavlja, da je filtriranje v šolah, ki v veliki meri blokirajo dostop do vsebin, pogosto povzročilo več škode za njihovo siceršnjo prakso e-varnosti. Zanašanje zgolj na filtriranje lahko namreč privede do naslednjih težav:

- omejen dostop do uporabnih virov;
- zmanjšanje odpornosti na tveganja na spletu;
- spodbujanje nenadzorovanega dostopa na drugih lokacijah;
- oviranje pri učenju;
- nepojasnjen dostop do spornih fotografij.

7. Zaščita strežnikov in odjemalcev

Poleg samega nakupa in varovanja omrežne opreme ter konfiguracije komunikacijske opreme je potrebno poskrbeti tudi za logično zaščito. Vsi strežniki in delovne postaje morajo imeti močna gesla. Priporočila za določitev močnega gesla:

- dolžina več kot 12 znakov;
- ne vsebuje vašega pravega imena, uporabniškega imena, imena zavoda;
- ne vsebuje celotne besede;
- je bistveno drugačen od prejšnjih gesel;
- vsebuje naslednje znake: velike/male črke, številke, simbole.

Primer gesla: Rojstni dan mojega sina je 12. december 2004 -> Rdmsj12/dec,4.
Na vseh strežnikih naj tečejo le storitve, ki jih potrebujete, ostale izklopite. Za hranjenje uporabniških imen in gesel uporabite aktivni imenik ali OpenLDAP. Možno je združiti tudi oba mehanizma, saj se OpenLDAP uporablja za prijavo v omrežje Eduroam.

Ker pa filtriranja prometa znotraj istega VLAN-a ni možno, je potrebno za zašito poskrbeti na samih strežnikih in odjemalcih. Usmerjevalnik tudi ne more preprečiti in odkriti okužbe z virusom ali trojanskim konjem. Zato priporočamo, da:

- na vseh strežnikih in odjemalcih vklopite požarni zid;
- na vseh strežnike in odjemalce namestite protivirusni program in ga redno posodabljate;
- strežnike in odjemalce redno posodabljate.

Priporočamo, da vse računalnike povežete v t. i. domeno, ki vam omogoča:

- Skrbniki omrežja uporabljajo strežnike, da nadzorujejo varnost in dovoljenja za vse računalnike v domeni. Tako je preprosto uveljavljati spremembe, saj se te samodejno uveljavijo v vseh računalnikih. Uporabniki domene morajo ob vsakem dostopu do domene vnesti geslo ali druge poverilnice.
- Če imajo uporabniki račun v domeni, se lahko prijavijo v vsak računalnik v domeni in zato ne potrebujejo računa v tistem računalniku.
- Uporabniki bodo lahko spreminjali samo tiste nastavitve, ki jih boste kot skrbnik dovolili.

S pomočjo domene lahko centralno nadgrajujete in kontrolirate vse računalnike. S pomočjo varnostnih politik lahko med drugim določite, kako močno geslo morajo uporabniki imeti in na koliko časa ga morajo spreminjati. Priporočamo, da ga spreminjajo vsaj vsake 4 mesece.

S pomočjo domene lahko prav tako uredite, katere mape naj se uporabnikom preslikajo v uporabniški pogon. Za vsako mapo določite, kdo jo lahko vidi, kdo lahko bere in kdo lahko piše v njej. Npr. učitelji nimajo kaj iskati v mapi

računovodstva in računovodstvo ne potrebuje dostop do mape, kjer ima učitelj shranjene teste.

Na delovnih postajah naj ima skrbniške pravice samo skrbnik, saj si boste tako prihranili marsikatero uro dela in pa zmanjšali možnost za okužbo in zlorabo sistema. Tudi v primeru, da ta računalnik uporablja brezžični dostop do omrežja, se učenci, v primeru, da učitelj pusti odklenjen računalnik, ne bodo mogli dokopati do gesla za to brezžično omrežje.

V primeru, da na sistemih ne uporabljate IPv6 protokola, vam svetujemo, da izklopite translacijske mehanizme (npr. Teredo, 6to4, ISATAP, IPv6 Automatic Tunneling, 6over4). V Windows sistemih so privzeto vklopljeni 6to4, ISATAP in Teredo. Sistem sam vzpostavi tunel in omogoči, da promet ne poteka čez filtre na usmerjevalniku ali požarnem zidu ter s tem omogoči prost dostop do sistemov preko IPv6 naslova. Kako izklopiti tunele v ukazni vrstici (angl. command promt), prikazuje slika 76.

```
netsh int teredo set state disabled
netsh int 6to4 set state disabled
netsh int isatap set state disabled
```

Slika 76: Izklop translacijskih mehanizmov na Windows sistemih

8. Varnostno kopiranje podatkov

Varovanje opreme je ustrezno urejeno, poskrbeti pa je potrebno še za dostopnost podatkov v vsakem času, tudi v primeru fizične okvare strežnika.

Varnostno kopiranje podatkov je zaščita podatkov pred pretvorbo, brisanjem ali spremembo. Varnostna kopija nam po morebitni okvari diska ali celotnega računalnika omogoča nebolečo obnovitev računalnika z vsemi nam pomembnimi podatki v popolnoma funkcionalno stanje.

Varnostno kopiranje lahko izvedemo na več načinov:

- varnostno kopiranje podatkov na isti strežnik, kje se nahajajo izvorni podatki;
- varnostno kopiranje na zunanje enote;
- varnostno kopiranje na oddaljene lokacije.

a) Varnostno kopiranje podatkov na isti strežnik, kje se nahajajo izvorni podatki

To lahko storimo s pomočjo RAID (Redundant array of independent disks) sistema. Gre za standard povezovanja dveh ali več trdih diskov, katerega namen je več diskov povezati v večjo in hitrejšo ali bolj zanesljivo logično enoto. Pri RAID1 zrcalimo disk A na disk B. Pogosto uporabljen je tudi sistem RAID 5. V tem primeru pa ne potrebujemo zgolj dveh pogonov, temveč najmanj tri. Podatki se zapisujejo tako, da se porazdelijo med vse tri diske na način, da v kolikor pride do okvare

enega izmed diskov, podatki s tem niso izgubljeni in preostala dva še vedno delujeta pravilno. Slabost je v nekoliko višji ceni in v tem, da če se okvarita dva diska izmed treh, vseeno izgubite vse podatke.

b) Varnostno kopiranje na zunanje enote

V tem primeru lahko podatke kopiramo na zunanji disk, NAS (Network-attached storage), trak … Pred samim kopiranjem je potrebno določiti, katere podatke, kdaj in kako bomo kopirali. Vendar, če hočemo to avtomatizirati, potrebujemo ustrezno programsko opremo. Obstaja kar nekaj brezplačnih programov, ki imajo svoje prednosti in slabosti. Takšni programi so npr. Areca Backup, Cobian Backup Amanita, DriverBackup. Večinoma omogočajo polno, prirastno izdelavo arhiva ali samo sliko tega, kar želimo. Omogočajo tudi stiskanje in šifriranje podatkov.

c) Varnostno kopiranje na oddaljene lokacije

S pojavom oblačnega računalništva so se pojavile tudi storitve oblačnega shranjevanja podatkov. Poleg vseh večjih tujih ponudnikov (Google, Amazon, Microsoft, DropBox …) omogoča shranjevanje tudi kar nekaj slovenskih ponudnikov (Arnes, Amis, FMC, Arctur d. o. o., Org.Tend d. o. o. …). Vendar pa je pri oddaljenem hranjenju podatkov potrebno preveriti, kje se ti strežniki nahajajo (v Sloveniji, v Evropi, ZDA …) in pa kdo ima dostop do teh podatkov. Namreč, če shranjujete varnostno občutljive podatke na strežnik v tujini in ne veste, kaj se z njimi dogaja, je takšno shranjevanje tvegano.

Zato Arnes vsem VIZ in ostalim upravičencem omogoča varno shranjevanje podatkov na strežnikih v Arnesovem sistemskem prostoru. Na voljo sta dve storitvi Arnes Mapa in pa Arnes Shramba.

V primeru Arnes Mape gre za sistem, katerega osnova je OwnCloud in je potrebno za sinhronizacijo imeti nameščenega odjemalca. Omogoča sinhronizacijo vseh datotek in podmap znotraj ene mape. Prednost je, da so vse datoteke dosegljive kadar koli in kjer koli, saj je mogoč dostop tudi preko spletnega brskalnika, omogoča tudi deljenje datotek in pravice upravljanja s posamezno datoteko ali mapo.

Storitev Arnes shramba je namenjena hrambi varnostnih kopij na sekundarni lokaciji, kar pomeni, da lahko svoj strežnik povežete z oddaljenim diskom in nanj odlagate drugo varnostno kopijo vašega sistema. Do oddaljenega diska se dostopa preko protokola iSCSI. Zaradi varnostnih razlogov je dostop omejen samo na en IP naslov organizacije, strežnik pa mora imeti veljavno ime gostitelja (angl. hostname) in ustrezen reverz.

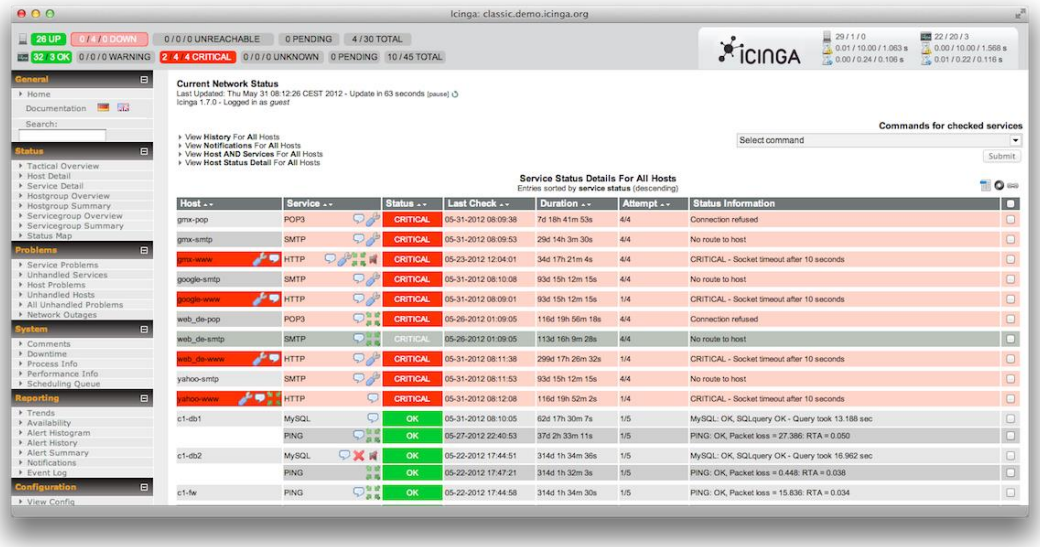
9. Nadzor omrežja

Ko je vsa infrastruktura vzpostavljena in oprema konfigurirana, je potrebno poskrbeti še za nazor delovanja. Obstaja kar nekaj brezplačne in plačljive programske opreme, ki omogoča nadzor omrežja.

Nagios ali Icniga (izhaja iz Nagios) je sistem, ki omogoča spremljanje in preverjanje naprav, ki jih določimo, ter obveščanje, ko gre kaj narobe (npr. nedosegljivost naprave) in ob normalizaciji. Teče na Linux ali Unix operacijskih sistemih. Nekaj funkcij, ki jih Icinga omogoča:

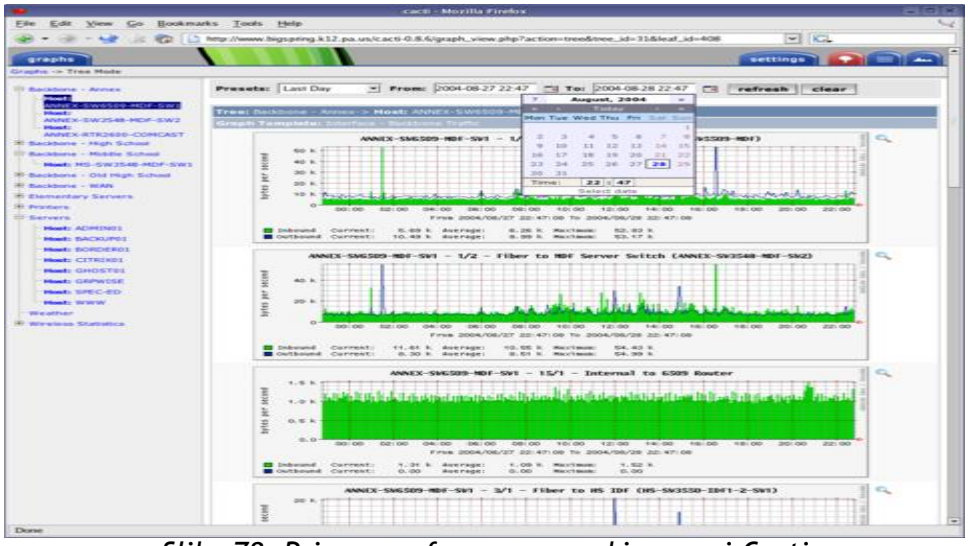
- spremljanje omrežnih storitev (SMTP, POP3, HTTP, PING …);
- nadzor strojnih virov naprav (zasedenost CPE, diska, spomina …);
- obveščanje, kadar pride do težave in ko je težava rešena.

Na sliki 77 vidimo primer pregleda dosegljivosti naprav.



Slika 77: Primer statusa naprav v programski opremi Icinga

Rešitev za risanje grafov omrežja pa predstavlja programska oprema Cacti. To je odprtokodna rešitev, ki omogoča risanje grafov iz podatkov, ki jih preko SNMP protokola pridobimo iz omrežnih naprav (promet na vmesnikih, zasedenost CPU, napake na vmesnikih …), in pa podatkov, ki jih pridobi iz drugih virov (npr. Icinga). Slika 78 prikazuje primer grafa v programski opremi Cacti.

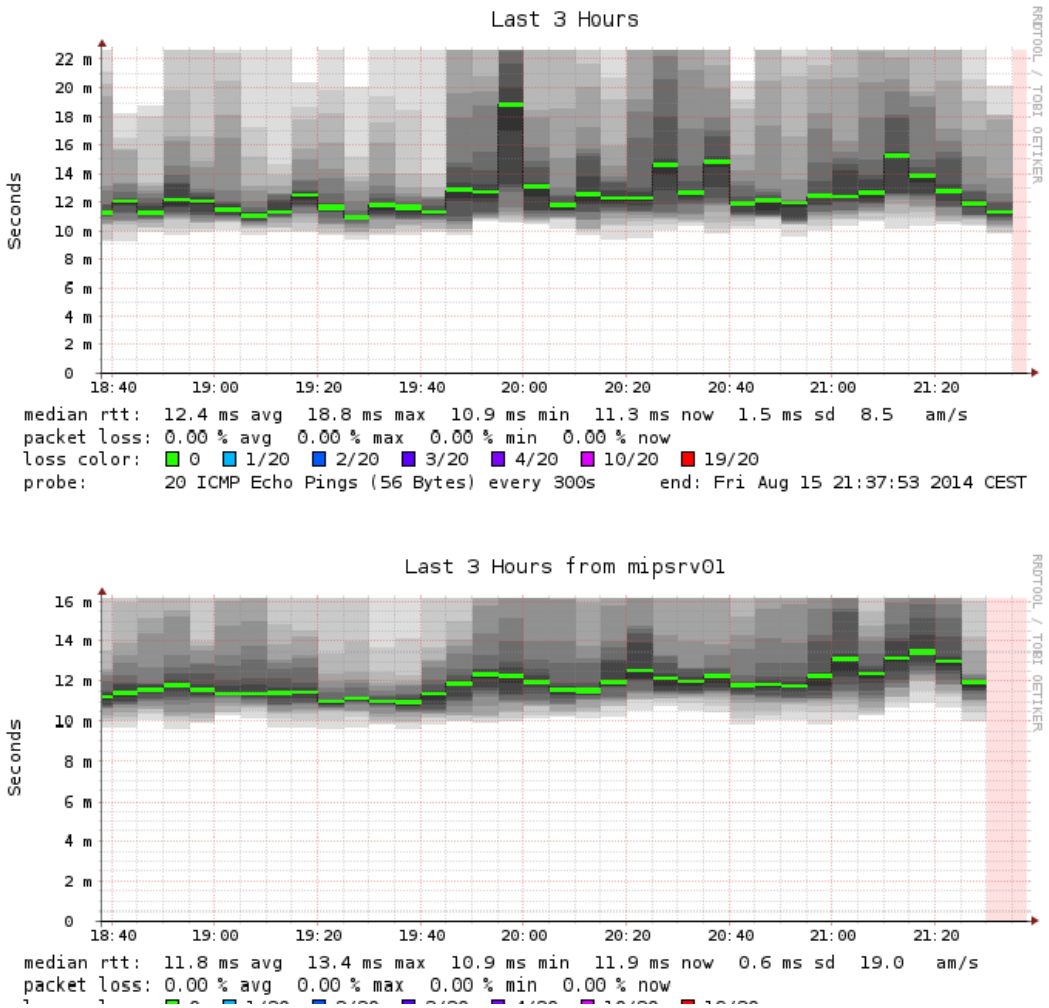


Slika 78: Primer grafa v programski opremi Cacti

Za nazor latence (angl. latency) in izgube paketov do naprav pa je primerno orodje SmokePing. Tudi to je odprtokodno orodje in omogoča npr.:

- preverjanje dosegljivosti naprav,
- preverjanje zakasnitev do naprav,
- preverjanje izgube paketov do naprav,
- preverjanje odzivnost DNS strežnika, Radius strežnika,
- …

Slika 79 prikazuje preverjanje zakasnitev do naprave v omrežju. Na 300 s pošlje 20 ICMP Echo pingov in z zeleno označi izgubo paketov, s sivimi odtenki pa označuje odstopanje med zakasnitvijo med posameznimi poizkusi.



Slika 79: Primer preverjanja zakasnitve naprave s pomočjo programskega orodja SmokePing

10. Izobraževanje in ozaveščanje o informacijski varnosti

Čedalje več groženj je zasnovanih tako, da izkoriščajo najšibkejši varnostni člen v verigi, to so zaposleni. Še zlasti tehnike socialnega inženiringa, kot sta "lažno predstavljanje" in "usmerjeno lažno predstavljanje" (slednje je usmerjeno na določeno osebo ali manjšo skupino), ki sta zelo nevarni.

Zato je potrebno uporabnike ozaveščati o informacijski varnosti, jim sestaviti pisna navodila za varno uporabo informacijske sistema v VIZ in jim objasniti, da gesel ne smejo posojati ali jih shranjevati pod tipkovnico ali v predalu. Iz varnostnih razlogov naj uporabniki vsakič, ko zapustijo računalnik, le-tega zaklenejo ali pa se odjavijo iz sistema. Nastavijo naj se tudi vklop ohranjevalnika zaslona in geslo ob nadaljevanju.

Posebej previdni naj bodo tudi pri odpiranju elektronske pošte. V primeru sumljive vsebine, naj jo raje pobrišejo ali pa pošiljatelja povprašajo o resničnosti sporočila.

Uporabniki, ki obdelujejo občutljive podatke, naj imajo ekrane obrnjene tako, da nepooblaščena oseba teh podatkov ne bo videla (načelo čistega ekrana). Prav tako naj poskrbijo, da ob odhodu iz pisarne z mize počistijo vse občutljive dokumente (načelo čiste mize).

Posebno skrb je potrebno nameniti odpadkom in dajanju odslužene opreme v smeti. Vse nosilce podatkov (trdi diski, USB ključi, CD/DVD …) je potrebno pred tem temeljito pobrisati, saj se lahko kdo dokoplje do podatkov, za katere ni pooblaščen.

Za brskanje po spletu vedno uporabite HTTPS protokol, če spletne strani to omogočajo, saj se s tem oteži prestrezanje informacij, predvsem uporabniških imen in gesel.

Viri in dodatne informacije:

Bøe, G., Enstad, P.A., Eilertsen , Ø: Recommended ICT Security Architecture In the Higher Education Sector, http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-ufs122.pdf

Cacti, http://www.cacti.net/

Icinga, https://www.icinga.org

Spletna stran Arnesa: http://www.arnes.si

Straus, M.: Varnost šolskih omrežij, 2002

KAZALO SLIK

Slika 1: 7 plasti OSI modela (http://www.escotal.com/osilayer.html, 2014) 13
Slika 2: Naloga fizične plasti OSI modela (http://www.soopertutorials.com/technology/networks/139-open-system-interconnection-osi-model.html, 2014) 14
Slika 3: Delovanje povezovalne plasti (http://www.soopertutorials.com/technology/networks/139-open-system-interconnection-osi-model.html, 2014) 15
Slika 4: Glava IPv4 paketa 16
Slika 5: Glava IPv6 paketa 17
Slika 6: Primerjava TCP in UDP protokola (http://networkingtips-tricks.blogspot.com/2010/05/how-transport-layer-works.html, 2014).....18
Slika 7: TCP segment (http://networkingtips-tricks.blogspot.com/2010/05/how-transport-layer-works.html, 2014) 18
Slika 8: UDP datagram (http://networkingtips-tricks.blogspot.com/2010/05/how-transport-layer-works.html, 2014) 19
Slika 9: Sekvenčne številke med vzpostavljanjem seje (Greeg, 2006).....32
Slika 10: ARP tabela pred in po napadu (Greeg, 2006).....33
Slika 11: Primer XSS napada (http://www.codeproject.com/Tips/541155/Really-Simple-XSS-and-a-Solution, junij 2014).....36
Slika 12: Število VIZ v Sloveniji (MIZŠ 2014) 42
Slika 13: Omrežje VIZ, povezano v omrežje ARNES preko enega izmed ponudnikov povezave. 44
Slika 14: Omrežje VIZ, povezano neposredno v omrežje ARNES. 45
Slika 15: Potek prijave uporabnika v omrežje Eduroam (Arnes AAI 2014).....47
Slika 16: Odgovor na vprašanje 1: Spol 50
Slika 17: Odgovor na vprašanje 2: V katero starostno skupino spadate?.....50
Slika 18: Starostna struktura skrbnikov glede na spol na VIZ.....51
Slika 19: Odgovor na vprašanje 3: Kakšna je vaša stopnja izobrazbe? 51
Slika 20: Odgovor na vprašanje 4: Kakšno je vaše delovno mesto?.....52
Slika 21: Odgovor na vprašanje 5: Tip organizacije, kjer ste zaposleni? 53
Slika 22: Odgovor na vprašanje 6: Koliko % delovnega časa ste zaposleni kot skrbnik informacijskega sistema (računalnikar)?.....54
Slika 23: Odgovor na vprašanje 7: Na koliko organizacijah opravljate funkcijo skrbnika sistema? 54
Slika 24: Delež zaposlitve kot skrbnik računalniške sistema glede na tip VIZ.....55
Slika 25: Odgovor na vprašanje 8: Koliko skrbnikov informacijskega sistema je zaposlenih na vaši organizaciji? 55
Slika 26: Odgovor na vprašanje 9: Ali ste se v času, odkar vam je bila zaupana vloga skrbnika informacijskega sistema, izobraževali na temo informacijskih tehnologij in/ali zagotavljanja informacijske varnosti?.....56
Slika 27: Odgovor na vprašanje 10: Ali ste se izobraževanja udeležili na lastno iniciativo in/ali stroške ali je za to poskrbela organizacija, kjer ste zaposleni? (Možnih več odgovorov).....56
Slika 28: Odgovor na vprašanje 11: Zakaj se izobraževanja niste udeležili? (Možnih več odgovorov).....57
Slika 29: Odgovor na vprašanje 12: Ali bi se izobraževanja na temo informacijskih tehnologij udeležili, čeprav le-to ne bi bilo točkovano? 57

Slika 30: Odgovor na vprašanje 13: Ali je omrežje, za katerega skrbite, povezano v omrežje ARNES?.....58
Slika 31: Odgovor na vprašanje 14: Ali je omrežje, za katerega skrbite, ločeno na pedagoški in administrativni del?.....58
Slika 32: Odgovor na vprašanje 15: Vodite dokumentacijo o omrežju na vaši organizaciji (stanje filtrov, dodeljeni in porabljeni IP naslovi, skica omrežja ...)?59
Slika 33: Odgovor na vprašanje 16: Imate za usmerjevalnikom, ki ga upravlja Arnes, postavljen še svoj usmerjevalnik? 59
Slika 34: Odgovor na vprašanje 17: Kakšna je funkcija tega usmerjevalnika? (Možnih več odgovorov).....60
Slika 35: Odgovor na vprašanje 18: Uporabljate NAT/PAT? 60
Slika 36: Odgovor na vprašanje19: Imate postavljen svoj požarni zid (poleg zaščite na usmerjevalniku)? 61
Slika 37: Odgovor na vprašanje 20: Imate v organizaciji vzpostavljeno brezžično omrežje? 61
Slika 38: Odgovor na vprašanje 21: Kakšno avtentikacijo za brezžično omrežje uporabljate? (Možnih je več odgovorov).....62
Slika 39: Odgovor na vprašanje 22: Imate brezžično omrežje za goste v ločenem podomrežju?.....62
Slika 40: Odgovor na vprašanje 23: Uporabljate IPv6 protokol? 63
Slika 41: Odgovor na vprašanje 24: Imate na operacijskih sistemih Windows Vista in novejših izklopljene IPv6 translacijske mehanizme? 63
Slika 42: Odgovor na vprašanje 16: Ima vaša organizacija postavljen strežnik?....64
Slika 43: Kje ima vaša organizacija postavljen strežnik? (Možnih več odgovorov) .64
Slika 44: Odgovor na vprašanje 27: Na strežniku tečejo naslednje storitve (Možnih več odgovorov).....65
Slika 45: Odgovor na vprašanje 28: Uporabljate sistem za upravljanje z vsebinami (CMS)? 65
Slika 46: Odgovor na vprašanje 29: Kateri strežnika za upravljanje vsebin (CMS) uporabljate? (Možnih več odgovorov).....66
Slika 47: Odgovor na vprašanje 30: Ali ste že imeli vdor v sistem (strežnik)? 66
Slika 48: Odgovor na vprašanje 31: Kaj je bila posledica vdora? (Možnih več odgovorov).....67
Slika 49: Odgovor na vprašanje 32: Ste vdor v sistem zaznali sami? 67
Slika 50: Kaj ste storili, ko ste opazili oz. bili obveščeni o vdoru v sistem? (Možnih več odgovorov).....68
Slika 51: Odgovor na vprašanje 34: Ali zaposleni uporabljajo za dostop do službenih računalnikov oddaljeno namizje (RDP)?.....68
Slika 52: Odgovor na vprašanje 35: Imate omogočen dostop do službenih računalnikov preko oddaljenega namizja (RDP)?.....69
Slika 53: Odgovor na vprašanje 36: Kakšen je časovni razpon zamenjave osebnih gesel na službenih računalnikih?.....69
Slika 54: Odgovor na vprašanje 37: Kje se nahaja komunikacijska oprema?(Možnih več odgovorov).....70
Slika 55: Odgovor na vprašanje 38: Kdo ima dostop do prostora, kjer se nahaja komunikacijska oprema? (Možnih več odgovorov).....70
Slika 56: Odgovor na vprašanje 39: Prostor, kje se hrani komunikacijska oprema, je? (Možnih več odgovorov).....71
Slika 57: Odgovor na vprašanje 40: Ali se obiskovalci lahko prosto gibajo po stavbi organizacije? 72

Slika 58: Odgovor na vprašanje 41: Ali za zagotavljanje nemotenega delovanja električnih naprav in uravnavanje napetostnih nihanj uporabljate UPS?.....72
Slika 59: Odgovor na vprašanje 42: Ali ste že imeli okvaro komunikacijske opreme? 73
Slika 60: Odgovor na vprašanje 43: Kaj je bil vzrok okvare? (Možnih več odgovorov) 73
Slika 61: Odgovor na vprašanje 44: Koliko časa je trajal povprečni izpad? 74
Slika 62: Odgovor na vprašanje 45: Imate za vzdrževanje strojne opreme urejeno vzdrževalno pogodbo?.....74
Slika 63: Odgovor na vprašanje 46: Imate urejeno varnostno kopiranje ključnih podatkov? 75
Slika 64: Odgovor na vprašanje 47: Kaj uporabljate za hranjenje varnostnih kopij? (Možnih več odgovorov).....75
Slika 65: Odgovor na vprašanje 48: Kateri program/storitev uporabljate za delo z dokumenti? 76
Slika 66: Odgovor na vprašanje 49: Ali ima vaša organizacije dokumentirana IT varnostna priporočila?.....76
Slika 67: Odgovor na vprašanje 59: Ali menite, da so uporabniki vašega informacijskega sistema na področju informacijske varnosti dovolj ozaveščeni? ..77
Slika 68: Primer delitve računalniškega omrežja na cone in segmente (Boe, Enstad in Eilertsen, 2014) 87
Slika 69: Primer konfiguracije Cisco usmerjevalnika 115
Slika 70: Primer konfiguracije Cisco stikala..... 116
Slika 71: Opis storitve WWW (Straus, 2002) 117
Slika 72: Primer zapisa filtra na Cisco usmerjevalniku..... 118
Slika 73: Primer omejitve števila MAC naslovov na CIsco stikalu 119
Slika 74: Primer nastavitve DHCP snooping 120
Slika 75: Primer nastavitve dynamic ARP inspection 120
Slika 76: Izklop translacijskih mehanizmov na Windows sistemih 123
Slika 77: Primer statusa naprav v programski opremi Icinga 125
Slika 78: Primer grafa v programski opremi Cacti 126
Slika 79: Primer preverjanja zakasnitve naprave s pomočjo programskega orodja SmokePing 127