POLITEHNIKA NOVA GORICA

POSLOVNO-TEHNIŠKA ŠOLA

DIPLOMSKA NALOGA

DOKUMENTIRANJE ŠOLSKEGA RAČUNALNIŠKEGA OMREŽJA IN ZAŠČITE PODATKOV V NJEM

Marko SPETIČ

Mentor: doc.dr. Bogdan FILIPIČ

Nova Gorica, 2005

ZAHVALA

Zahvaljujem se mentorju doc. dr. Bogdanu Filipiču za njegove nasvete, pomoč in veliko mero potrpežljivosti pri nastajanju diplomske naloge. Posebej se zahvaljujem gospodu Daliborju Čotarju in ostalim zaposlenim v osnovni šoli Srečka Kosovela v Sežani, ki so mi nudili pomoč ter omogočili dostop do potrebnih podatkov. Zahvaljujem se tudi staršema, ki sta mi ves čas študija stala ob strani in me spodbujala.

IZVLEČEK

Pregledna in ažurirana tehnična dokumentacija je za uspešno poslovanje ustanove nujna. Ker so računalniški programi za dokumentiranje že zelo izpopolnjeni, lahko z računalniško podporo odpravimo številne nevšečnosti, ki se pojavljajo z zastarelo papirno dokumentacijo. Tehnične risbe in besedila hitreje posodobimo brez odvečnih popravkov, ki jih zahteva papir. Bistveno je predvsem to, da lahko kadarkoli in od koderkoli dostopamo do želenih podatkov in jih tudi uspešno priredimo v najkrajšem možnem času. Čas, ki ga s tem prihranimo, lahko uporabimo za ostala pomembna dela.

V okviru diplomske naloge smo izdelali računalniško podprto dokumentacijo šolskega računalniškega omrežja in zaščite podatkov v njem. Obravnavana osnovna šola je bila pred leti v večjem delu adaptirana, zato dosedanja tehnična dokumentacija ne ustreza več dejanskemu stanju. Z računalniško podprto dokumentacijo smo računalniško strojno opremo popisali, tako da skupaj s posnetki mrežne napeljave ustrezajo dejanskemu stanju na šoli. Poleg strojne opreme smo vključili še računalniško programsko opremo, ki skrbi za nemoteno delo uporabnikov in varovanje šolskega omrežnega sistema. Posvetili smo se tudi fizični zaščiti podatkov in programski varnostni opremi, ki sta zelo pomembna dejavnika pri delovanju računalniškega omrežja.

KLJUČNE BESEDE

Računalniško omrežje, dokumentacija, računalniško projektiranje, osnovna šola, zaščita podatkov, sistem za upravljanje varovanja informacij

ABSTRACT

Clear and up-to-date technical documentation is obligatory for an instituion to work successfully. Many troubles occurring with the oldfashioned paper documentation can be avoided by computer support because computer programs for documenting are very advanced. Technical drawings and texts are faster and easier updated. There is no unnecessary correction which is needed when using paper. The point is that we can access the data from anywhere whenever we want to and we can adapt it in a very short time. So we can use the saved time for other important work.

The computer-supported documentation for a school computer network and data protection have been prepared in this diploma thesis. The considered primary school building was reconstructed a few years ago so the existing technical documentation does not correspond to the actual state anymore. Using the computer-supported documentation we have made an inventory of the computer hardware. Together with the documention of network connections it corresponds to the actual state at the school. In addition to the hardware, we included the computer software which ensures indisturbed work of users and protects the school network system. We worked on physical protection of the data and on protection software. Both are very important for the operation of the computer network.

KEY WORDS

Computer network, documentation, computer-aided design, primary school, data protection, information security management system

KAZALO

KAZALO SLIK

PRILOGE

1. UVOD

Z razvojem informacijske tehnologije se spreminjajo tudi načini dela in komunikacije v ustanovah. Elektronske zbirke podatkov in dokumenti v elektronski obliki izpodrivajo tradicionalno pisarniško poslovanje. Elektronska pošta nadomešča klasično pošiljanje dopisov na papirju, papirne obrazce in vloge nadomeščajo elektronske vloge. Tako lahko podjetje lažje in ceneje ureja svojo dokumentacijo. Današnja tehnologija namreč omogoča računalniško podprto tehnično risanje, interaktivno delo, urejenost dokumentov in večjo preglednost. Vendar pa uporaba elektronskega gradiva odpira nekatera vprašanja, na katera še ni dokončnih odgovorov. Med zahtevnejšimi sta vprašanji elektronskega shranjevanja gradiva in elektronsko arhiviranje.

V tej diplomski nalogi obravnavamo računalniško podprto dokumentiranje računalniškega omrežja in zaščite podatkov na osnovni šoli v Sežani. Tehnična dokumentacija računalniške opreme šole je bila v večini izdelana v papirni obliki, na prirejenih obrazcih. Vsak obrazec je vseboval svojo številko prostora v šoli in vso pripadajočo tehnično opremo. Sčasoma je takšen dokument postal premajhen in nepregleden. Ker je v šolskem sistemu veliko naprav, je arhiv zelo obsežen, tako da je dostopni čas do podatka zelo dolg. Takšna dokumentacija ne ustreza več sedanjim zahtevam šole, zato smo se odločili, da izdelamo računalniško podprto dokumentacijo šolskega računalniškega omrežja, ki bo v skladu z dejanskim stanjem na šoli. Računalniška izvedba dokumentov bo tako lažja za vzdrževanje in prilagajanje. Dokumentacija bo vsebovala slike računalniške mrežne inštalacije s fizičnim modelom (podatkovni vodi) in logičnim modelom (poenostavljen fizični model), evidenčne kartone elektronskih naprav in seznam vseh naprav.

V nadaljevanju diplomske naloge bomo najprej utemeljili potrebo po izdelavi dokumentacije in navedli cilje in načrt dela. Cilje bomo določili glede na zbrane podatke o trenutni obliki dokumentacije, njeno ujemanje z dejanskim stanjem, pomanjkljivosti in težave, ki jih povzroča dejansko stanje, ter glede na zahteve šolskih določil. Sledil bo opis programskega paketa Visio 2003, zmožnosti programa, tipov diagramov, objektov in šablon, uporabljenih pri delu, in uporabnosti programa

pri dokumentiranju. Obrazložili bomo bistvene elemente risanja. Zatem bomo prešli na varovanje podatkov. Opisovali bomo splošne varnostne zahteve, ki jih določajo današnja merila za varno poslovanje ustanov. Navedli bomo nekatere pasti, ki pretijo in čakajo na napako oziroma pomanjkljivost v sistemu, in rešitve, ki omogočajo kvalitetno odpravljanje nam ponavadi neznanih varnostnih lukenj. Dotaknili se bomo zlonamerne programske kode, varnega shranjevanja podatkov, neprekinjenega dostopa do podatkov in mednarodnega varnostnega standarda ISO 17799, ki pokriva vsa področja varnosti in zaščite.

Zatem bomo prešli na izdelavo računalniško podprtega dokumentiranja strojne opreme in mrežne napeljave. Opisovalo bomo oba modela šolskega omrežja, tako logičnega kot fizičnega, ter se nato posvetili izdelavi evidenčnih kartonov za popis strojne in programske opreme na šoli. Povedali bomo, kako smo modele gradili, kako smo zbirali potrebne informacije, s čim smo si pomagali, čemu in komu bodo modeli služili in kako jih lahko še dopolnimo. Pojasnili bomo, kako deluje šolsko omrežje, kakšno vlogo imajo posamezne naprave in kakšne so njihove naloge. Poglavje o dokumentiranju strojne opreme se končuje s podpoglavjem o opisu naprav, ki jih bomo beležili v evidenčnih kartonih. Podrobneje bomo opisali evidenčni karton, v katerem se bodo beležila stanja računalniških naprav, njihove vhodno-izhodne naprave in nameščena programska orodja. Naslednje poglavje bomo posvetili vidikom varnosti v šolskem omrežju, kot so programska varnostna oprema, fizična zaščita in naloge skrbnika pri zagotavljanju nemotenega delovanja sistema.

V zaključku bomo opisali rezultate dela, pridobitve šole ter kaj smo se z nalogo naučili in kaj lahko v bodoče še spremenimo oziroma izboljšamo. Opisali bomo izkušnje in znanja, ki smo jih pridobili z nalogo. Naše opravljeno delo bo dokumentirano v štirih prilogah. Prikazana bosta fizični in logični model omrežja, evidenčni karton, ki smo ga razvili za popisovanje elektronskih naprav, in seznam vseh evidentiranih naprav. Na koncu bomo pojasnili, kako dokumentacija ustreza šolskim zahtevam in nakazali smer, v katero naj bi se razvijal računalniško podprt sistem dokumentiranja, seveda ob morebitnem povečanju šolskega omrežnega sistema.

2. ANALIZA STANJA NA ŠOLI

Osnovna šola v Sežani je glede informacijske tehnologije zelo napredna. Velik poudarek posveča sodobni strojni in programski opremi, ki se komaj uveljavlja ali je v vzponu. Posledica je velik porast novih strojnih in programskih elementov, ki se vključujejo skozi razvojno in uvajalno obdobje. Na podlagi svojih izkušenj lahko šola zato podaja pridobljeno znanje drugim šolskim ustanovam, ki tudi poskušajo slediti današnji informacijski modernizaciji. Tako je obseg celotnega šolskega omrežja in priključenih naprav vedno večji, kar pomeni, da postajata šolska dokumentacija in arhiv celotnega inventarja prevelika, da bi lahko z njima brez računalniške podpore upravljali zaposleni na šoli. Tako se je kmalu pojavila potreba po podrobnem popisu in arhiviranju stanja šolske mreže, strojnih elementov in programske opreme. Informatik na šoli namreč velikokrat potrebuje informacije o sistemu, ki ga vzdržuje, nadzira, ter odpravlja napake, bodisi strojne ali programske. Zato smo se odločili, da razvijemo podatkovni model, v katerem bo evidentiran vsak delujoč sistem v šolskem omrežju.

Trenutno arhivirano stanje informacijske tehnologije ne zadošča potrebam informatika, saj je nepopolno in ne podaja oprijemljivih točk, ki bi nam bile v pomoč. Dokumentacija se nahaja v papirni obliki, kar povzroča dodatne težave. Vemo, da v obilici papirja hitro izgubimo pregled. Vnašanje novih elementov je zamudno, saj moramo najprej določen dokument poiskati in ga dopolniti oziroma popraviti. Papirna oblika ne dopušča brisanja, zato postane dokument po večkratnem spreminjanju težko berljiv. Po pregledu celotnega arhiva smo prišli do spoznanja, da je le ta nepopoln in neažuren. Nekaj podatkov je zabeleženih, ostali pa se nahajajo v glavah zaposlenih, kar se velikokrat izkaže za ozko grlo. Ker informacija ni zapisana, to zahteva še dodaten čas iskanja osebe, ki lahko informacijo posreduje. Prišli smo do zaključka, da je celotna dokumentacije urejena površno in bi bilo smiselno celoten sistem prečesati do potankosti ter podatke dopolniti in zabeležiti v podatkovno bazo. Tako bi bil arhiv urejen in ažuriran, informacije bi bile dostopne kadarkoli, za skrbnika pa bi to pomenilo enostavnejše upravljanje in bi zanj porabil veliko manj časa kot sedaj.

2.1. Utemeljitev potrebe po izdelavi dokumentacije

Kot smo že omenili, bo urejena, ažurirana in posodobljena dokumentacija šolskega računalniškega omrežja pomagala pri različnih opravilih, za katere je ponavadi zadolžen informatik na šoli. Pa tudi nekateri drugi sodelavci bodo lahko uporabljali podatkovno bazo z informacijami in skicami omrežja. Logični in fizični model omrežja bo služil kot predstavitev strukture in hierarhije šolskega omrežja. Ker se omrežje nenehno razvija in širi, bo ta prikaz zelo uporaben pri predstavitvah notranjim in zunanjim sodelavcem, ki bi se radi seznanili z računalniškim omrežjem. Tudi vzdrževalcem omrežnih napeljav bo v pomoč, saj jim lahko natančno pokažemo potek napeljav in mesta priključitev naprav v omrežje. Sami vemo, da je pred fizičnim posegom v omrežje priporočljivo spoznati njegov način delovanja in vseh priključenih naprav. Vedeti moramo tudi, kakšno funkcijo opravlja posamezna enota, da ne bi prišlo do pomot pri tako obsežnem informacijskem sistemu, kot ga ima šola.

Glavni del dokumentacije, to je popis vseh strojnih elementov in nameščene programske opreme, bomo uporabljali pri zbiranju informacij, ki jih zahteva vodstvo šole. To so informacije o številu računalnikov na šoli, strežnikih, usmerjevalnikih, stikalih, vhodno-izhodnih napravah, ki so sestavni del vsakega računalnika, in različnih tehničnih pripomočkih za prikazovanje oziroma predvajanje. Vsaka ustanova namreč beleži svojo lastnino, tako da ne pride do zapletov, kadar se oprema nabavi ali proda. To velja tudi za šolo. Naša dokumentacija bo poleg podatkov o strojni opremi obsegala še popis programske opreme, saj je priporočljivo vedeti, s kakšno programsko opremo imamo opravka. Če nam je na primer sporočeno, da se je pojavil nek problem v učilnici 202, lahko iz dokumentacije hitro razberemo, kakšna informacijska oprema je tam nameščena in kakšni programski moduli skrbijo za napravo. Točno bomo vedeli, kje se ta prostor nahaja, s kakšno periferijo imamo opravka in kakšna programska oprema teče na računalniku. S fizičnim modelom bomo ugotovili, kje se nahaja naprava in kako je priključena, z evidenčnim kartonom pa bomo pridobili vse ostale podatke o računalniškem sistemu. V vsakem trenutku bomo tudi vedeli, koliko računalnikov »živi« na šoli. Če pride do kakršnekoli spremembe, kot sta odstranitev naprave ali vgradnja nove, lahko podatek o tem

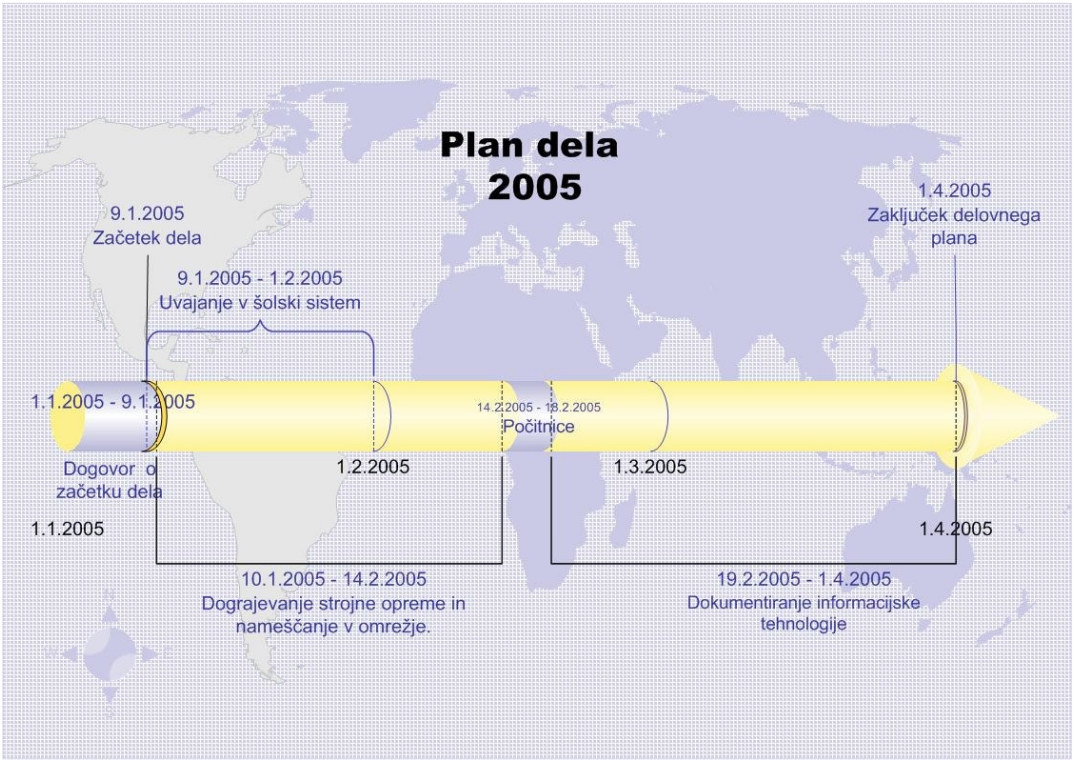
enostavno vnesemo v našo bazo in tako sproti skrbimo za posodobitve. Le tako bomo imeli v vsakem trenutku na razpolago sveže informacije.

Sodobna oblika tehnične dokumentacije prinaša številne prednosti, ki jih uporabnik lahko s pridom izkorišča le, če je za takšno delo usposobljen. Iz izkušenj uporabe papirne dokumentacije se lahko marsikaj naučimo. Ko preidemo na elektronsko obdelovanje podatkov, lahko hitro opazimo koliko dela nam današnja tehnologija prihrani. Elektronski dokumenti so za razliko od papirnih dostopni od kjerkoli, če jih le namestimo v internetno ali lokalno omrežje. Z njimi lahko upravljamo na daljavo ali na računalniku, kjer se nahajajo. Ni potrebno hraniti velikih nepreglednih količin papirja, ki ponavadi hitro zastara in postane odvečen material. Skratka, elektronska oblika dokumentiranja in poslovanja je postala del našega življenja in brez nje si normalnega dela ne znamo več predstavljati.

2.2. Cilji in načrt dela

Glede na podatke o omrežju in varovanju opreme, ki smo jih zbrali, lahko opredelimo cilje in potek dela. Plan dela smo tudi grafično predstavili na časovni premici, kot jo prikazuje slika 1. Plan nas bo vodil skozi obdobje slabih treh mesecev. Točno bomo lahko videli, kako delo poteka glede na cilje in zahteve. Lažje ga bomo nadzirali in se prilagajali morebitnim časovnim odstopanjem.

Če pogledamo našo časovno premico, lahko vidimo dve poglavitni obdobji našega dela, ki sta označeni s pravokotnima oblikama pod časovno premico. V prvem obdobju bomo šolsko omrežje dograjevali, se pravi, bomo nameščali in posodabljali strojno in programsko opremo, ki bo postala del celotnega omrežnega sistema. Ker bomo obiskali vse šolske prostore, bomo hkrati tudi popisovali stanje v šolskih prostorih, kar nam bo prišlo prav pri izvajanju drugega dela plana. Ta del namreč postavlja nalogo dokumentiranja celotnega šolskega omrežja, tako strojne kot programske opreme. V tem obdobju bomo na podlagi zbranih podatkov poskušali ustvariti sliko celotnega omrežja, ki jo bomo nato arhivirali v elektronski obliki.



Slika 1: Potek dela

Najprej bomo narisali enostavnejši logični model omrežja, ki bo prikazoval, kako je omrežje zgrajeno. Zanimali nas bodo osnovni strojni elementi, kot so usmerjevalniki, stikala, požarni zidovi ter strežniki in povezave med njimi. Šolsko omrežje je namreč zelo razgibano in je za navadnega uporabnika težko predstavljivo. Zato bomo poskušali narisati uporabniku razumljivo predstavitev. Naslednja naloga bo risanje bolj kompleksnega modela, to je fizičnega modela, ki bo prikazoval načrt šole in vsa nahajališča strojne opreme po prostorih. Za pomoč bomo uporabili evakuacijski načrt šole, ki ga bomo prerisali, in vanj vnesli še vse pridobljene podatke o opremi.

Ker je bila šola leta 2002 v večjem delu sanirana in posodobljena, nas je zanimal tudi fizični potek omrežnih UTP[1] kablov, ki povezujejo računalniške komponente med seboj v šolski intranet. Ta informacija bo koristna pri napeljevanju ali popravilu napeljav. Lažje se namreč lotimo dela, če nam uporabnik na risbi prikaže, kje v

[1] UTP – kratica za unshielded twisted pair ali neoklopljena sukana parica

prostoru ali objektu želi spremembo na povezavi. Ob uporabi načrta so stvari jasne in točno vemo, kako pridemo do izbrane točke.

Ko bomo narisali oba modela, se bomo lotili naslednje naloge dokumentiranja, to je popisovanja vseh računalniških enot in njihove programske opreme v evidenčne kartone. Evidenčni karton bomo posebej prilagodili šolskim potrebam, tako da bo vseboval vse potrebne podatke, ki jih bo uporabljal sistemski skrbnik ali informatik na šoli. Oblika takega dokumenta naj bi bila dovolj pregledna že na prvi pogled in bi nam enostavno podajala želene informacije. Vsebovati mora le bistvene podatke za računalnikarja, ki ga zanimajo za določeno strojno opremo. Odločili smo se, da za spoznavanje in dokumentiranje porabimo približno polovico časa za vsako. To bi moralo zadostovati za uresničitev zastavljenega cilja. Nad premico vidimo še časovno razporeditev, ki določa tudi uvajalno obdobje, ki bo potekalo kar med dograjevanjem omrežnega sistema. Takrat bomo postopoma spoznali celoten šolski omrežno-računalniški sistem. Nekje v drugem in tretjem mesecu, se bomo podrobneje poglobili v delovanje sistema in začeli z dokumentacijskim popisom računalniškega inventarja.

Na koncu smo se morali odločiti, katera programska orodja bomo uporabili za izdelavo modelov in dokumentacije. Najbolj uporabno orodje v šoli je zagotovo Microsoftov programski paket Office, ki ga uporabljajo predvsem za pripravo dokumentov, seminarskih nalog in predstavitev. Odločili smo se, da za popisovanje elektronskih naprav uporabimo Microsoftovo preglednico Excel, s katero bomo lahko po celicah in nato po listih uredili evidenčne kartone. Lahko bi se odločili tudi za program Word, ki omogoča uporabo tabel, vendar ne dopušča uporabe matematičnih funkcij, ki nas bodo zanimale za statistiko. Zanimalo nas bo, koliko naprav neke vrste imamo, koliko naprav določenega dobavitelja in tako naprej. Zato nam bo Excel prišel zelo prav. Kot drugi program, s katerim bomo narisali logični in fizični model, smo izbrali prav tako Microsoftov izdelek Visio 2003. Kot bo opisano v nadaljevanju naloge, si lahko z njim pomagamo na več načinov, saj ima že vnaprej pripravljene razne tipe diagramov in šablone. Na voljo imamo med drugim tudi grafične elemente za risanje računalniških mrežnih struktur in načrtov prostorov. Ker imamo z obema programoma nekaj izkušenj, nam na srečo risanje modelov ne bo predstavljalo večje ovire, saj bi drugače porabili pri spoznavanju veliko več časa, kot

ga bomo sicer. Koristno je tudi to, da sta programa v sklopu istega programskega okolja Microsoft Office, kar pomeni da je prenašanje dokumentov med njima enostavno in zanesljivo.

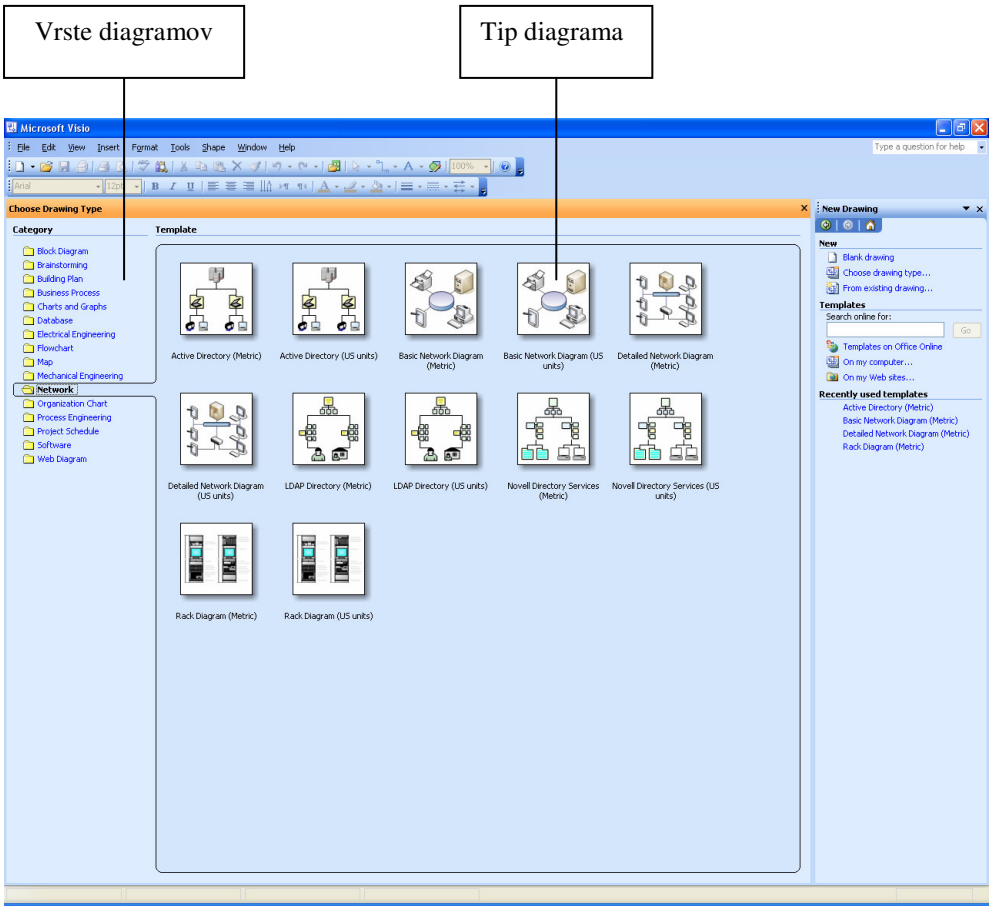
3. TEHNIČNO RISANJE IN RAČUNALNIŠKI PROGRAM VISIO 2003

Pri nastajanju dokumentacije o šolskem računalniškem omrežju smo prišli do vprašanja, katero programsko orodje uporabiti za izdelavo tehniških risb. Potrebovali smo orodje, s katerim bi enostavno in učinkovito dokumentirali šolsko omrežje, ki se nenehno spreminja oziroma nadgrajuje. Po pregledu nekaterih pripomočkov, ki omogočajo takšen zapis, smo se odločili za Microsoftov paket Visio 2003 (Powell, 2002). Visio omogoča pripravo poslovnih in tehničnih diagramov, ki dokumentirajo in organizirajo zapletene zamisli, procese in sisteme. Ugotovili smo tudi, da podpira večino inovativnih avtomatiziranih funkcij. Diagrame narejene z Visiom, lahko objavimo v delovnem prostoru Microsoft SharePoint Portal Server ali jih izvozimo v obliki SVG (Scalable Vector Graphics[2]) ali s posodobljeno funkcijo za shranjevanje v obliki spletne strani. Posebej so nas navdušile, poleg številnih splošnih oblik diagramov, vnaprej pripravljene predloge oziroma šablone (angl. stencils), na katerih so zbrani različni, pomensko sorodni grafični elementi, ki smo jih uporabili za izdelavo posameznega diagrama v logičnem modelu računalniške mreže. Kasneje smo diagrame lahko vključili v poročila (npr. v Word) ali predstavitve (npr. v Powerpoint). Izkazalo se je, da je podpora med Microsoftovimi orodji pri uvažanju in izvažanju objektov zelo dobra, kar smo velikokrat izkoristili.

[2] SVG - Vektorska oblika diagramov, ki pri pretvorbi ohranja zelo dobro kakovost

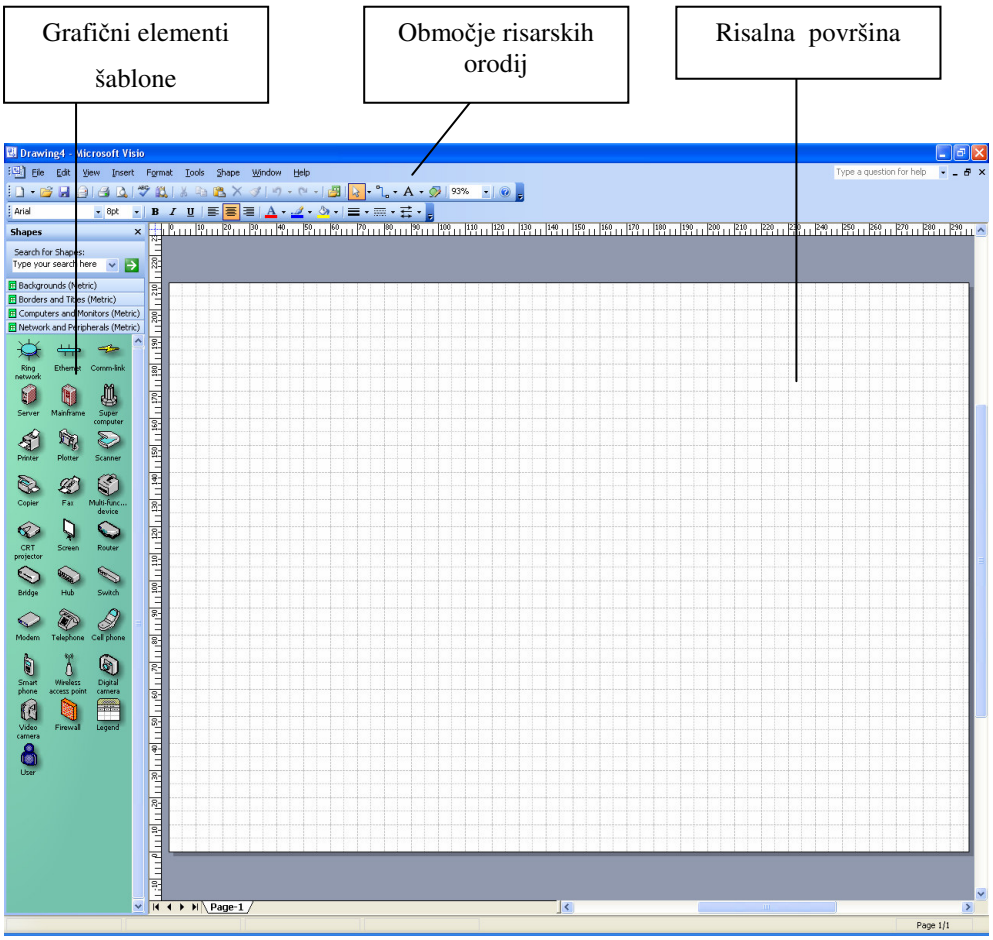
3.1. Splošno o programu Visio 2003

Orodja v Visiu so bila posebej razvita za posamezna strokovna področja, s katerimi lahko pripravljamo poslovne in tehnične diagrame, ki izpolnjujejo zahteve obravnavane organizacije. Na sliki 2 je lepo razvidno, koliko različnih vrst diagramov nam ponuja Visio. Za naše potrebe smo izbrali vrsto diagrama računalniške mreže, v kateri se nahaja več tipov diagramov. Vsak tip diagrama pa ima pripravljen svoj nabor šablon, s katerimi lahko omrežje narišemo na risalno površino (slika 3). Diagram sestavimo preprosto z vlečenjem vnaprej definiranih grafičnih elementov.



Slika 2: Vrste diagramov v Visiu

Na ta način smo lažje dokumentirali stanje omrežja, bolje razumeli, kako sistem deluje, in tudi povečali učinkovitost dela.



Slika 3: Risalna površina v programu Visio

Seveda lahko pri ustvarjanju diagrama uporabimo grafične elemente iz različnih šablon hkrati in tako dosežemo željen rezultat. Posamezno šablono izberemo z izbiro menuja File > Shapes, pri čemer je mapa ena izmed pripravljenih vrst diagramov, šablona pa ena izmed pripravljenih tipov v izbrani vrsti.

Visio 2003 je del programskega okolja Microsoft Office in bo z novimi možnostmi omogočal izgradnjo povezanih rešitev, ki bodo izkoriščale Microsoft .NET in spletne storitve XML[3]. S to različico postanejo dokumenti Visio pametni odjemalci, ki jih je mogoče integrirati s poslovno programsko opremo in uporabiti za nadzor poslovnih podatkov v realnem času.

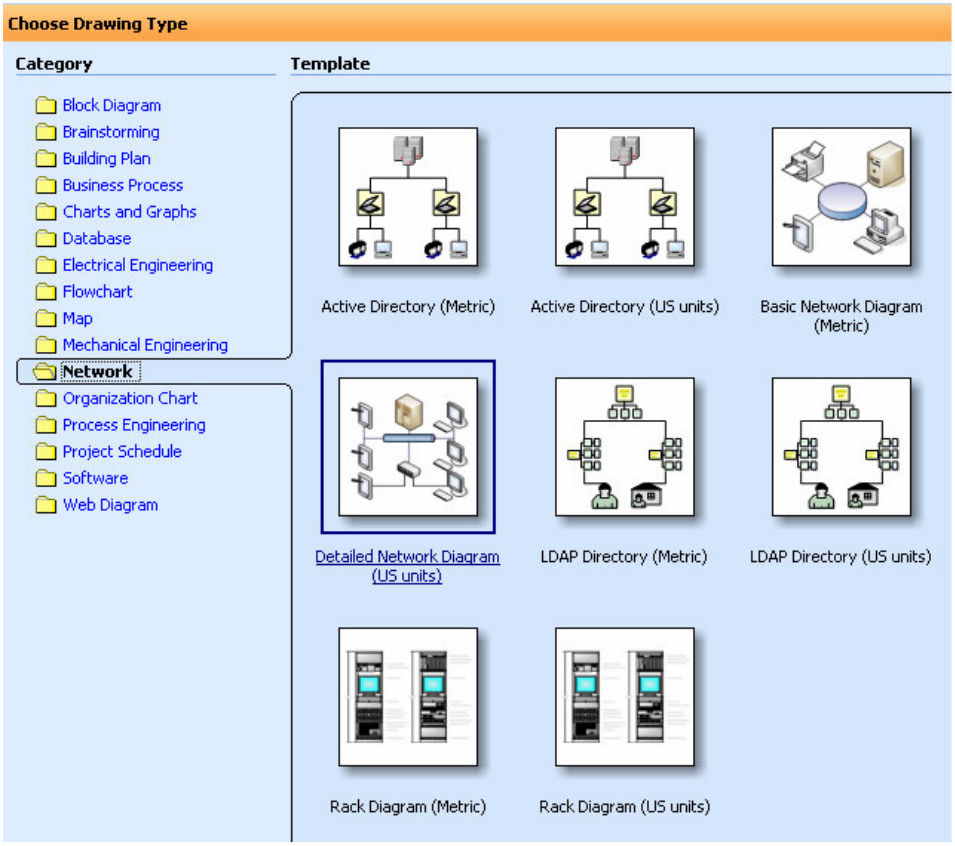
[3] XML - E**X**tensible **M**arkup **L**anguage oziroma razširljiv označevalni jezik

3.2. Zmožnosti programa, uporabljene v nalogi

V tem podpoglavju bomo predstavili šablone in orodja programa Visio, ki smo jih uporabili pri izdelavi tehničnih risb. Naj povemo, da risbe niso risane v merilu, saj to ni bilo poglavitnega pomena. Pri fizičnem modelu računalniške mreže in strojne opreme so nas zanimala samo nahajališča povezav in vtičnic ter lokacija strojnih elementov, kot so računalniki, strežniki, stikala, požarni zidovi in usmerjevalniki, tako da ima računalnikar v šoli lažji pregled oziroma evidenco nad celotnim sistemom.

3.2.1. Izbira ustreznih diagramov pri zagonu programa

Ob zagonu Visia se odpre okno, ki je razdeljeno na dva dela. Slika 4 prikazuje levi del (angl. Drawing Type - Tipi diagramov), ki zasede približno tretjino okna in ponuja izbiro vnaprej pripravljenih diagramov, in desni del, ki zasede ostali dve tretjini okna (angl. Template - Šablona) in ponuja izbiro šablon.

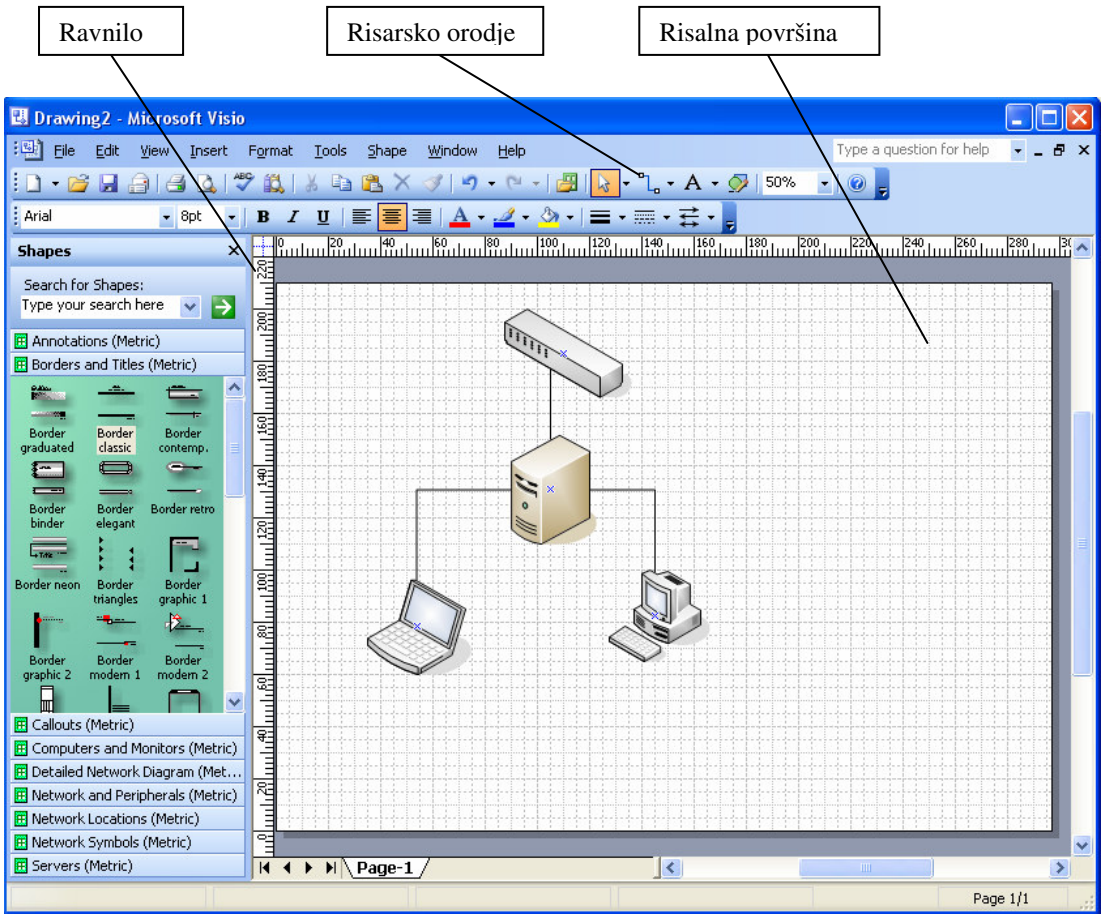


Slika 4: Tipi diagramov

Na sliki 4 je prikazan diagram Network > Detailed Network Diagram. Tukaj se nahaja večina šablon, ki vsebujejo objekte, ki predstavljajo računalniške sisteme, stikala, strežnike, mostove, povezave, modeme in podobne elemente. Objekti so podrobneje opisani v naslednjem razdelku.

3.2.2. Objekti in risalna ravnina

Slika 5 prikazuje glavno okno v programu Visio, v katerem lahko začnemo risati. Levi del okna prikazuje zbirko šablon in grafičnih elementov, desni del pa glavno risalno površino, ki je označena z ravnilom.

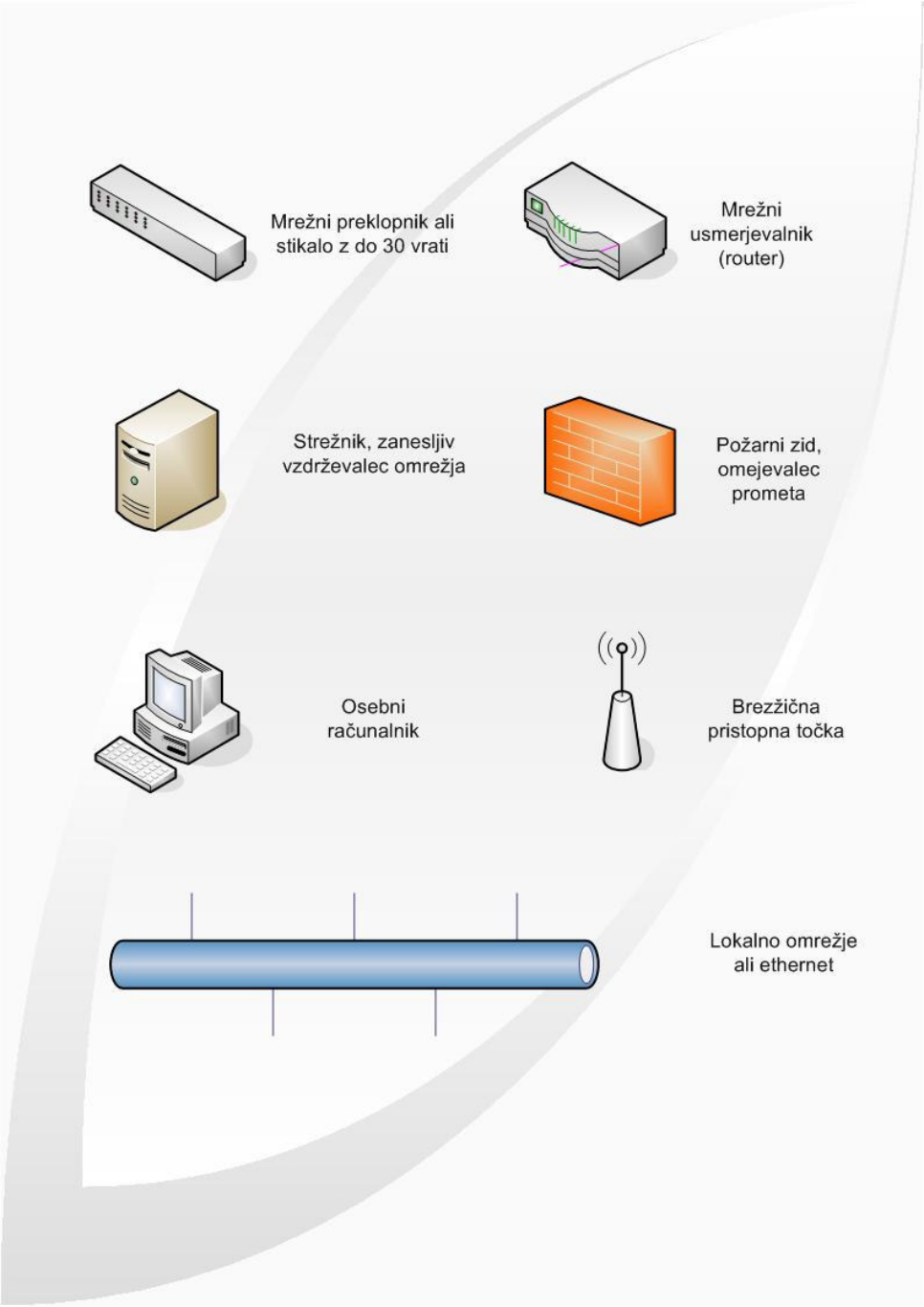


Slika 5: Risalna površina

Na risalni površini vidimo nekaj grafičnih elementov, ki smo jih poskusno prilepili in povezali v celoto z risarskim orodjem. Risba predstavlja strežnik, na katerega sta povezana računalnik in prenosni računalnik, ter stikalo, ki usmerja mrežni promet na

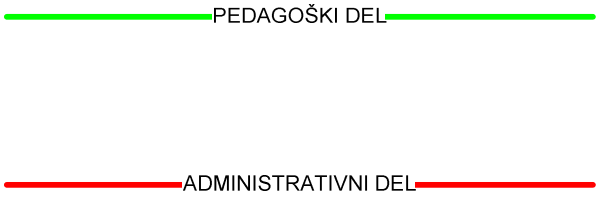
določena mesta. Z uporabo tega pristopa smo prišli do fizičnega in logičnega modela računalniške mreže na šoli in ju predstavili v prilogi 1 in 2.

Pri risanju logičnega modela smo uporabili grafične elemente, ki so prikazani na sliki 6.



Slika 6: Grafični elementi omrežja

Delovanje celotnega omrežja bomo opisali v petem poglavju, ki govori o dokumentiranju strojne opreme in mrežne napeljave. Lokacije elektronskih naprav, ki smo jih predstavili z grafičnimi elementi, lahko vidimo v fizičnem modelu računalniškega omrežja, ki je opisan v podpoglavju 5.2. Pri načrtovanju fizičnega modela mreže smo uporabili iste grafične elemente, le da smo jih drugače razporedili, povezali z orodjem za povezavo in jo barvno označili, kot prikazuje slika 7.



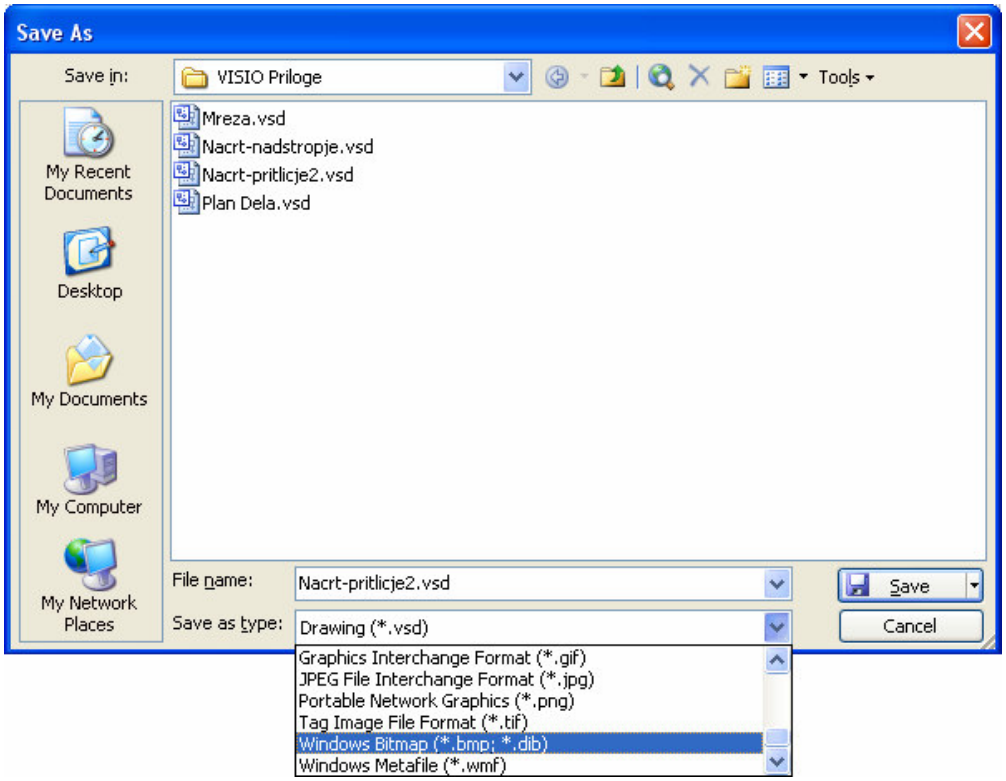
Slika 7: Mrežna povezava

Zelena barva prikazuje mrežno povezavo na pedagoškem nivoju, rdeča barva pa na administrativnem nivoju. Oba dela sta fizično ločena, tako da učenci, ki komunicirajo na logičnem nivoju, ne morejo dostopati do administrativnega dela oziroma komunikacije, ki jo uporabljajo učitelji.

3.2.3. Shranjevanje diagramov

Program Visio 2003 omogoča shranjevanje risb na več načinov. Osnovni način je shranjevanje v datoteko s končnico *.vsd (Visual Studio). To pomeni, da datoteko zna odpreti in njeno vsebino upravljati samo Visio. Pri načrtovanju smo izbrali to vrsto datoteke, saj omogoča popoln nadzor objektov v datoteki. Naslednji možnosti shranjevanja sta zapis *.dwg, ki ga zna odpirati AutoCad, in oblika *.html, ki je pripravljena za objavo na spletu. Zelo uporabno je tudi shranjevanje risb v obliki slike in to v več možnih formatih, kot so *.jpg, *.gif, *.bmp, *.tif in *. wmf. Uporabili smo shranjevanje datotek tipa *.jpg, ki so primerne za tiskanje in predstavitev v Microsoftovem programu PowerPoint. Na sliki 8 vidimo okno, ki se odpre pri shranjevanju diagrama in možnost tipa shranjevanja, Save as type oziroma

Shrani kot tip. Tako kot bomo diagram predstavili, ga tudi shranimo, oziroma se prilagodimo programu, ki bo datoteko obdeloval. Če npr. želimo risbo v nadaljevanju obdelovati v Auto Cadu, jo bomo shranili v obliki Slika1.dwg.



Slika 8: Shranjevanje risbe v programu Visio 2003

4. CELOVITO VAROVANJE PODATKOV

Podatki so največji kapital vsake ustanove in neprekinjen dostop do njih je ključnega pomena. Treba jih je zaščititi pred različnimi grožnjami, ki so jim izpostavljeni. Podatki o omrežjih so še toliko bolj izpostavljeni napadalcem, saj informacijski sistemi niso več zaprti znotraj lokacije ustanove, temveč so zaradi poslovnih potreb povezani v internet. Mala in srednje velika podjetja imajo s tem običajno veliko težav. Ponavadi se takega posla lotijo kar sama, kar pa njihovi materialni in človeški viri težko prenesejo. Tako so raznovrstne zaščite pred vdori zelo pomanjkljive in so lahek plen za marsikaterega zlonamernega uporabnika. Kakovostno zaščito lahko postavimo samo ob pomoči izkušenega in v tej smeri sveže izobraženega administratorja, ki nenehno spremlja dogajanje na tem področju. Znano je namreč, da so zlonamerneži skoraj vedno korak pred nami in našimi zaščitami, tako da je zelo pomembno tudi zgodnje odkrivanje njihovih nepooblaščenih dostopov.

Pomen varnosti v informacijski tehnologiji in škoda, ki nastane zaradi incidentov, ki ogrozijo varnost računalniških sistemov, sta postala predmet različnih študij. Ena takih je vsakoletna raziskava računalniškega kriminala in informacijske varnosti, ki jo izvaja Computer Security Institute (CSI) v sodelovanju z FBI. Rezultati raziskave so v določenih primerih zelo šokantni. Celotna škoda in izgube, ki so jih utrpela podjetja, znašajo več kot 300 milijonov dolarjev in se letno skoraj podvajajo. Posamezna podjetja so oškodovana tudi za več kot 5 milijonov dolarjev. Omenimo, da so najpogostejši razlogi za škodo virusi, sledijo jim tatvine prenosnikov in zloraba omrežnih komunikacij, nato onesposobitve storitev, nepooblaščen dostop in kraja zaupnih podatkov. Zanimiv je podatek, da velik odstotek sodelujočih ne ve, ali je prišlo do zlorabe njihovega sistema ali ne (Štrakl, 2001).

V nadaljevanju bomo navedli nekatere pasti, ki neprestano pretijo pred našimi vrati in čakajo na našo napako oziroma pomanjkljivost v sistemu, in rešitve, ki omogočajo odpravljanje nam ponavadi neznanih varnostnih lukenj. Seveda ni metode, ki bi zagotavljala 100% varnost pred vdori.

4.1. Varnostna politika

Poti za zmanjšanje verjetnosti vdora na najmanjšo možno mero je več in tudi stroški varovanja so različni, saj niso vsa okolja enako privlačna za vdiralce. Pravilno in uspešno varovanje informacijskega sistema pa temelji na hierarhiji varnostnih sistemov in mehanizmov (slika 9). Vsak sloj varnostne hierarhije je odvisen od slojev pod njim. Če nižji sloji niso dovolj dobro definirani in postavljeni, tudi gornji sloj ni ustrezno varovan. Na primeru je najlažje razumljivo. Če nimamo ustrezno rešenega fizičnega varovanja, nam lahko kdo nepooblaščeno odtuji strojno opremo in podatki so izgubljeni, tudi če imamo skrbno izdelan sistem overjanja uporabnikov. Najnižja raven hierarhije je varnostna politika, ki je ponavadi temelj celovitega pristopa k varnosti. Obsega tako fizično in tehnično varovanje kot tudi pravila, ki določajo načine varovanja, kaj se sme in kaj ne, kako naj se uporabljajo računalniški viri, pa tudi postopke in kazni, če bi prišlo do kršitve varnostnih postopkov (Štrakl, 2001).

Slika 9: Varnostni sistem

Postavitev varnostne politike je niz tehničnih in organizacijskih dejavnikov. Organizacijski dejavniki določajo, kaj se varuje in stopnjo varovanja, tehnični dejavniki pa to varovanje izvajajo. Pri definiranju politike morajo sodelovati strokovnjaki z obeh področij, tako da se ne spregleda opisanih elementov varnostne politike. Ni nujno da so vsi našteti elementi uveljavljeni pri določenem informacijskem sistemu, vsekakor pa moramo biti nanje pozorni pri definiranju lastne varnosti. Varnostna politika mora biti prirejena posebnostim našega informacijskega sistema.

4.2. Elementi varnostne politike

Varnostna politika najpogosteje obsega naslednje mehanizme:

- fizično varovanje omrežja in sistema,
- definiranje pravic do dostopa,
- varovanje medomrežnih povezav,
- javne storitve,
- povezovanje prek javnega omrežja,
- zaščito datotek,
- sistem varne prijave,
- zaščito pred zlonamerno programsko opremo.

Fizično varovanje razumemo kot varovanje fizičnega dostopa do vitalnih delov informacijskega sistema in komunikacijske opreme. Osrednji računalnik, strežniki, usmerjevalniki, stikala (angl. switch) in druge komunikacijske naprave morajo biti v posebnem prostoru. Vstop v ta prostor mora biti varovan. Vedeti moramo, da so lahko strežniki in komunikacijska oprema zelo ranljivi ob neposrednem delu z njimi, zato morajo imeti dostop do njih le pooblaščeni delavci oziroma administratorji. Priporočljivo je, da se vsi vstopi v komunikacijski prostor zapisujejo in pa tudi vse dejavnosti, ki so bile v njem izvedene. K fizičnem varovanju prištevamo tudi ožičenje krajevnega omrežja. Mora biti namreč takšno, da onemogoča nepooblaščene priključitve ali prisluškovanje. Ker se za ožičenje največkrat uporablja sukana parica (UTP), ki ponavadi nima oklopa, je tako mogoče prisluškovati z indukcijo. Priporočljivo je, da so ožičenja zato v namenskih jaških, ki naj bodo iz kovine.

Pomemben element je prav tako **definiranje pravic do dostopa** za posamezne uporabnike. Tu določimo, katere storitve omrežja in sistema lahko uporabnik uporablja. Določimo, do katerih virov ima uporabnik dostop, kako poteka prijavljanje v sistem, katere storitve se uporablja in katere storitve so izrecno prepovedane. Pri povezavi v internet se določi, katere storitve interneta so dovoljene, s katerimi računalniki v internetu uporabniki lahko vzpostavijo povezavo, s katerimi aplikacijskimi protokoli se lahko povezujejo in ali je določen uporabnik sploh lahko vzpostavi povezavo z internetom. Pravila povezovanja z internetom se uveljavijo na požarni pregradi (angl. Firewall).

Ker smo danes priča množičnim potrebam po medsebojnem povezovanju krajevnih omrežij, bi jih morali izvesti čim bolj varno. Najpogostejši varnostni mehanizem, ki omogoča **varno povezovanje** je požarni zid. To je nekakšen filter, ki prepušča želeni promet, vse ostalo pa zavrača. Pri povezavi krajevnega omrežja z internetom najpogosteje ni cilj imeti na voljo vse vire, ki jih ponuja internet, ampak imamo tudi določene javne storitve, ki jih ponujamo vsem ali nekaterim uporabnikom interneta. Najpogostejše javne storitve so izmenjava elektronske pošte, javni spletni strežniki in javni strežniki FTP. Do vseh teh strežnikov mora biti zagotovljen dostop iz omrežja internet, zato so tudi najbolj podvrženi morebitnim napadom. Javne strežnike namestimo v zunanje omrežje požarnega zidu. To območje imenujemo demilitarizirano območje ali storitveno omrežje.

Klicni dostopi so najpreprostejša oblika povezovanja oddaljenih uporabnikov s krajevnim omrežjem ali internetom. Vsi klicni dostopi morajo biti zajeti v varnostno politiko. Pri prijavi uporabimo dodatne varnostne mehanizme, metode enkratnih gesel. Pri neprekinjeni povezavi tega problema ni, saj se prijavimo le enkrat, linijo pa povežemo preko požarnega zidu, ki preprečuje nepooblaščene dostope od zunaj. Znotraj samega sistema imamo skladišče informacij, ki niso namenjene vsem, tudi vsem zaposlenim ne. Te datoteke lahko vzdržuje že sam operacijski sistem z ustreznimi pravicami datotečnega sistema, vendar pa to ni dovolj, saj ima skrbnik možnost brati te datoteke ali izdelovati varnostne kopije in jih pozneje obnoviti v drug računalnik. Zato se uporablja sistem za kodiranje datotek, ki omogoča zaščito pred nepooblaščenim branjem.

Za **prijavo v računalnik** ali omrežje imamo najpogosteje sistem uporabniškega imena in gesla. Klasični sistem s statičnimi gesli ima številne slabosti, saj omogoča večkratno prijavo z istim geslom, hkrati pa ga je s prisluškovanje mogoče zajeti in zlorabiti. Zato poznamo sisteme enkratnih gesel, na podlagi izzivov in odzivov, uporabe časovne sinhronizacije ali elektronskih kartic. Vsi sistemi zahtevajo, da ima uporabnik pri prijavi posebno elektronsko kartico – generator kode, ki poda enkratno geslo. Še naprednejši so sistemi, na podlagi bioloških lastnosti uporabnika (prstni odtis, prepoznava govora).

Ker se danes preko omrežja pretaka veliko datotek z najrazličnejšo programsko kodo, obstaja velika verjetnost, da se k uporabniku, brez njegove vednosti prenese **zlonamerna programska oprema**. Sem najpogosteje prištevamo viruse in trojanske konje. Virusi so najpogostejši razlog za izgubo ali onesposobitev normalnega delovanja našega sistema. Vnos takšne programske opreme v krajevno omrežje pa je lahko zelo različen, od brskanja po svetovnem spletu prek elektronske pošte do neposrednega vnosa prek medija (Štrakl, 2001).

Varnostna politika zajema najrazličnejša varnostna vprašanja, pri njeni postavitvi pa moramo upoštevati značilnosti lastnega informacijskega sistema. Upoštevati moramo tudi, da se varnostna politika s časom spreminja, saj se ves čas uvajajo nove storitve, ki v obstoječi politiki niso zajete. Omrežje je treba nadzorovati, popravljati novo odkrite razpoke v sistemu varnosti in ga obvezno posodabljati. Vse spremembe je treba nujno zapisati v dokument, ki opisuje varnostno politiko. Skratka na omrežno varnost je treba gledati celovito. Delne rešitve posameznih elementov varnosti niso prava pot. Pa še pomemben nasvet: bolje je imeti slab dokument varnostne politike kakor nobenega.

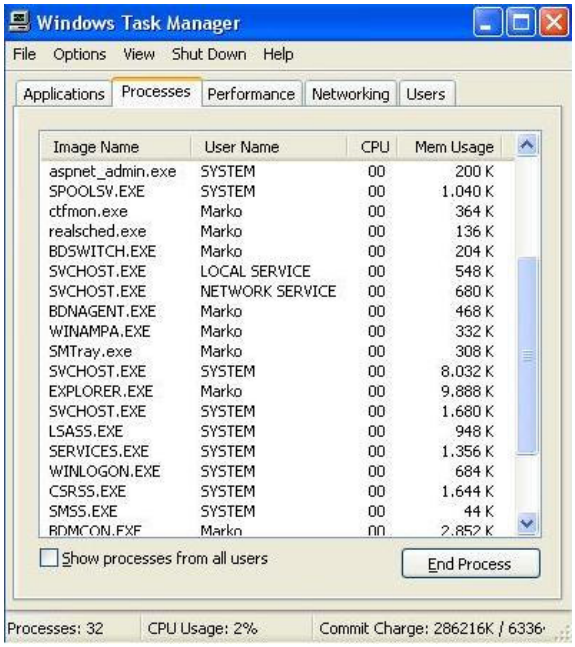
4.3. Vohunsko programje ali spyware

Kdor želi najvišjo stopnjo varnosti pred nepooblaščenimi vdori v sisteme, potrebuje posebna orodja za odkrivanje škodljive kode, imenovane vohunsko programje ali spyware. Vohunski programi so zlonamerni programski moduli, ki se brez naše vednosti zmuznejo skozi varnostne zidove in prisluškujejo dogajanju v računalniku z namenom pridobivati različne informacije, pri čemer so na prvem mestu prijavna gesla. Zavedati se moramo, da v primerih, ko je vohunski program pridobil naše geslo in ga uspešno posredoval, ne gre za vdor, saj se nepooblaščenec prijavi z veljavnim imenom in geslom, ter tako razpolaga z našimi zaupnimi podatki. Takšne vstope pa je zelo težko odkriti.

Do okužbe računalnika pride na več načinov. Pazljivi moramo biti pri odpiranju prilog elektronske pošte, nevarnost preži tudi pri nekaterih spletnih straneh ali pa ob namestitvi programske opreme. V prihodnosti se bomo morali navaditi sprejemati pošto, ki ima ustrezen nam znan certifikat. Če je podpisana nam znana oseba, je večja verjetnost, da odpiramo neokuženo pošto. Večina programskih hiš že uporablja javne ključe oziroma certifikate pri nalaganju programske kode, ki jih naš sistem prepozna in dovoli tako namestitev. Ko pride do okužbe računalnika, uporabnik ponavadi tega ne zazna, zato je odkrivanje take vrste programske kode težje kot odkrivanje virusa. Pazljivi moramo biti na nekatere odzive našega računalnika. Računalnik deluje malenkost počasneje, saj mora razumljivo poleg običajnega dela spremljati vse dejavnosti, ki jih zahteva vohunski program. Tak program običajno odkrijemo med procesi, ki tečejo in obremenjujejo procesor (slika 10). Programi se zapišejo v register računalnika, da se zaženejo že ob zagonu. Nekateri vohunski programi poleg računalnika, v katerem so nameščeni, napadejo tudi druge računalnike v omrežju in tako obremenjujejo tudi omrežje v podjetju (Šiška, 2002).

Da bi se izognili nepooblaščenemu vdoru vohunske kode v naš računalnik, je najbolje, da pridobimo specializirano programsko opremo, ki sproti preverja, ali je naš računalnik okužen ali ne. Nekatere rešitve je moč dobiti na internetu brezplačno, običajno pa taka oprema ne zadostuje za večje podjetje. Zato se nam nakup profesionalne programske opreme hitro obrestuje. Programi so posebej prilagojeni za

naše podjetje in ponavadi nam programske hiše, pri katerih kupimo takšen paket, po nakupu stojijo ob strani z nadgradnjami in tehnično pomočjo.

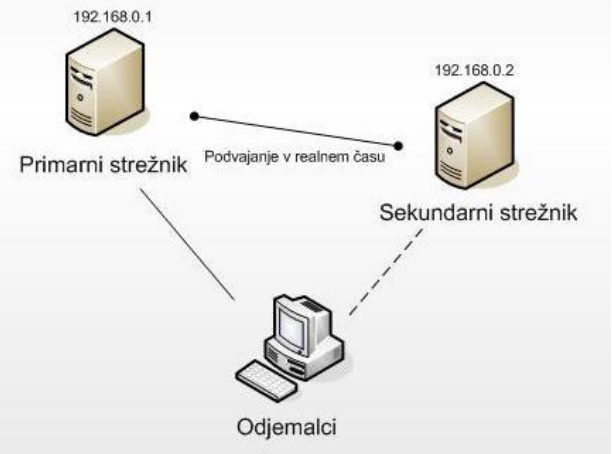


Slika 10: Obremenitev sistema s procesi

Po namestitvi programskega paketa za odpravljanje težav z virusi in vohunskimi programi se program postavi v standardni način delovanja. To pomeni, da redno pregleduje piškotke (angl. cookies), register računalnika, pomnilnik in določene lokacije na trdem disku. Seveda privzeti način ni 100-odstotno zanesljiv, zato je potrebno nekatera mesta preverjati ročno.

4.4. Varno shranjevanje in neprekinjen dostop do podatkov

Neprekinjen dostop do podatkov je v časih sodobnega poslovanja ključnega pomena. Še tako dobro načrtovanje in vzdrževanje informacijskih sistemov ne more zagotoviti, da v strežniku ne bo prišlo do napake oziroma izpada v nekem naključnem trenutku. Takšni izpadi lahko usodno vplivajo na delovanje informacijskega sistema. Sodobno poslovanje zahteva varno spravljene in neprekinjeno dostopne podatke, tudi če se v sistemu zgodi nekaj nepredvidenega. Rešitve, ki jih ponujajo podjetja danes delujejo po načelu podvojevanja (replikacije) podatkov med dvema strežnikoma (slika 11).



Slika 11: Replikacije podatkov

Ko uporabnik opredeli, kateri podatki so zanj pomembni, delo prevzeme sam program. Ta podatke v realnem času samodejno replicira v sekundarni strežnik in jih s tem naredi dostopne tudi pri izpadu primarnega strežnika. Pri izpadu strežnika sistem napako samodejno zazna in uporabnika preusmeri v lokalni ali oddaljeni sekundarni strežnik. Sekundarni strežnik nato prevzeme vlogo primarnega, in to tako, da prevzame celotno njegovo identiteto, skupaj z imenom in IP-številko. Ker celoten sistem deluje samodejno, je za uporabnika popolnoma neopazen. Seveda se potem, ko je bila zamenjana ali popravljena strojna oprema v izpadlem računalniku, zopet vzpostavi primarni strežnik (Zaščita za največje, 2005).

4.5. Mednarodni standard ISO/IEC 17799:2002

Mednarodni standard ISO/IEC 17799 (British standard, 2002) je svetovno znan in razširjen varnostni standard. Je zelo obširen, izčrpen, vsestranski in razumljiv ter pokriva vsa področja zaščite in varovanja informacij. Vsebuje tudi precejšnje število nadzornih zahtev. Glavna naloga standarda ISO 17799 je vzpostavljanje primerne varnostne politike pri razvoju produktov. Omeniti velja, da s podrejanjem razvoja predpisom standarda organizacija lahko pridobi ustrezen certifikat. To pomeni, da standard predstavlja priporočilo o varnosti informacij in informacijskih sistemov. Skratka, standard obravnava varnost informacijskega sistema z različnih vidikov (fizična varnost, tehnološka kompatibilnost, tehnično varovanje premoženja informacijskega sistema).

Po pregledu dokumentacije o varnosti in zaščiti šolskega omrežja smo naleteli na nekatere pomanjkljivosti. Ker je čedalje bolj čutiti porast zanimanja na področju informacijske varnosti, smo se pri definiranju varnosti šolskega omrežja in opreme naslonili na priporočila standarda ISO 17799, ki ponujajo enoten predpis, kako graditi sisteme, ki bodo čim bolj zaščiteni pred neavtoriziranimi dostopi in drugimi nevšečnostmi. Sam standard je organiziran v deset poglavij. Vsako poglavje pa določa oziroma pokriva različno tematiko informacijske varnosti.

Kar se tiče fizične zaščite šolskega omrežja po predpisih standarda, lahko rečemo, da so sistemi varovanja postavljeni po definiciji. Šola namreč uspešno nadzira fizični dostop oseb z video nadzorom in alarmnimi napravami, ki ločeno ščitijo posamezna območja. To so pisarne, sistemska soba in učilnice, kjer se nahaja večina strojne in programske opreme, ter zbornica, kabineti in tudi knjižnica. Prav tako so uspešno varovani kabelski vodi, ki so speljani po posebnih jaških, ki so ločeni od ostale napeljave. Tudi glede nadzora dostopa uporabnikov šola sledi standardu. Uporabniki se prijavljajo v domenski strežnik, ki točno določa njihove pravice in omejitve glede dostopa do informacij. Nad vsakim uporabnikom imamo določeno kontrolo, ki je zapisana v beležnici dogodkov. Kontrole pred zlonamerno programsko opremo se redno izvajajo z ustrezno programsko opremo, varnostne kopije podatkov se beležijo vsakodnevno ob istem času, skrbnik uspešno beleži nastale okvare strojnega ali programskega dela sistema.

Kot smo omenili že na začetku, pa smo pri pregledu varnostnih zahtev naleteli tudi na nekatere pomanjkljivosti. Šola ima določene svoje varnostne potrebe in jih tudi izvaja v skladu z zastavljenimi cilji. Nima pa vzpostavljenih zahtev glede dokumentacije. Trenutno stanje ni zapisano v obliki dokumenta, temveč se nahaja le v glavah zaposlenih. Njihova varnostna politika in klasifikacija sredstev nista ustrezno dokumentirani in shranjeni. Vsa pomembna sredstva, ki so povezana z informacijskim sistemom, je potrebno popisati in hraniti. Postopki, ki so določeni v varnostni politiki, morajo biti zapisani in vzdrževani. Zato smo se odločili, da trenutno stanje šolskega informacijskega sistema analiziramo, pregledamo že obstoječo dokumentacijo, opredelimo vse varnostne zahteve in nato vse skupaj ustrezno dokumentiramo. Tehnične risbe lokalnega šolskega omrežja smo izdelali v Microsoftovem programu Visio 2003, medtem ko smo razpoložljiva tehnična sredstva in lastnosti beležili prav tako v Microsoftovem programu Excel 2002.

V nadaljevanju podrobneje opisujemo vse razvite modele, od tehničnih diagramov do preglednic, kjer se beleži trenutno stanje strojne in programske opreme.

5. DOKUMENTIRANJE STROJNE OPREME IN MREŽNE NAPELJAVE

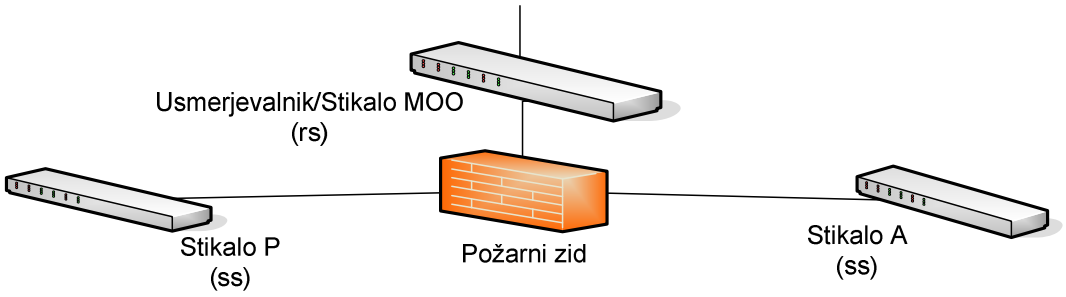
Namen izgradnje dokumentacije računalniške mrežne napeljave je predvsem orientacijski, tako da se lahko kdorkoli, tako informatik kot vzdrževalec, ki bo posegal v šolski mrežni sistem, uspešno seznanil njegovim delovanjem in nahajališči posameznih delov omrežja in priključenih naprav. Nekateri uporabni podatki in informacije o sistemu se nahajajo le v spominu zaposlenih. Takšen način arhiviranja pa onemogoča takojšen dostop do želene informacije, saj moramo najprej izvedeti, kdo informacijo ima in kje se takrat nahaja. Velikokrat se zgodi da potrebujemo odgovor v danem trenutku in je kasnejša informacija neuporabna oziroma takrat nima pomena.

Pri logičnem modelu omrežja nismo potrebovali informacij o nahajališčih opreme, saj nas je zanimal predvsem princip delovanja. Slika le poenostavlja fizični model, tako da lažje razumemo celotno arhitekturo in si predstavljamo, kako poteka pretok podatkov med uporabniki, strežniki in usmerjevalci prometa. Četudi nismo ustrezno podkovani s tehničnim informacijskim znanjem, bomo lahko razumeli bistvo delovanja oziroma namen. Fizični model nam je tako le ustrezna tehnična pomoč pri iskanju določenih napak v sistemu, saj lahko hitro preučimo zgradbo omrežja in priključenih naprav (Ogrinc, 1991). Točno lahko povemo lokacijo posameznega strojnega dela ter izvemo kdo je uporabnik. Imamo nadzor nad vso opremo, ki je vključena v šolski sistem. Cilj izdelave takšnega modela je bil namreč hiter vpogled v sistem, tako da lahko vzdrževalci, ki fizično posegajo v določene dele, hitro najdejo in ne poškodujejo ostalih delov omrežja. Tudi morebitni nov kader na šoli bo lahko lažje razumel celotno arhitekturo in delovanje šolskega lokalnega omrežja.

V nadaljevanju bomo podrobneje opisali oba modela šolskega omrežja, tako logičnega kot fizičnega, ter se nato posvetili izdelavi evidenčnih kartonov za popis šolske tehnične strojne in programske opreme.

5.1. Logični model računalniškega omrežja

Risbo logičnega modela računalniškega šolskega omrežja si lahko ogledamo v prilogi 1. Model je sestavljen tako, da je hierarhija strojnih elementov postavljena od vrha proti dnu. To pomeni, da so najpomembnejši členi oziroma najvišja ali glavna vrata, ki odpirajo sistem, na vrhu in se nato hierarhično razvrščajo po lestvici navzdol. Na primer, slika 12 prikazuje vrhnji del omrežja. Glavno stikalo oziroma usmerjevalnik MMO, ki se nahaja na razredni stopnji (rs) ima pod okriljem dve podstikali P in B, ki se nahajata v sistemski sobi (ss) in fizično ločujeta omrežje na pedagoški in administrativni del, ti dve pa imata pod seboj še nekaj stikal, ki skrbijo za pošiljanje prometa na posamezne dele omrežja. To so višja stopnja in nižja stopnja pedagoškega dela, zbornica, kabineti, knjižnica in uprava, ki spadajo pod administrativni del.



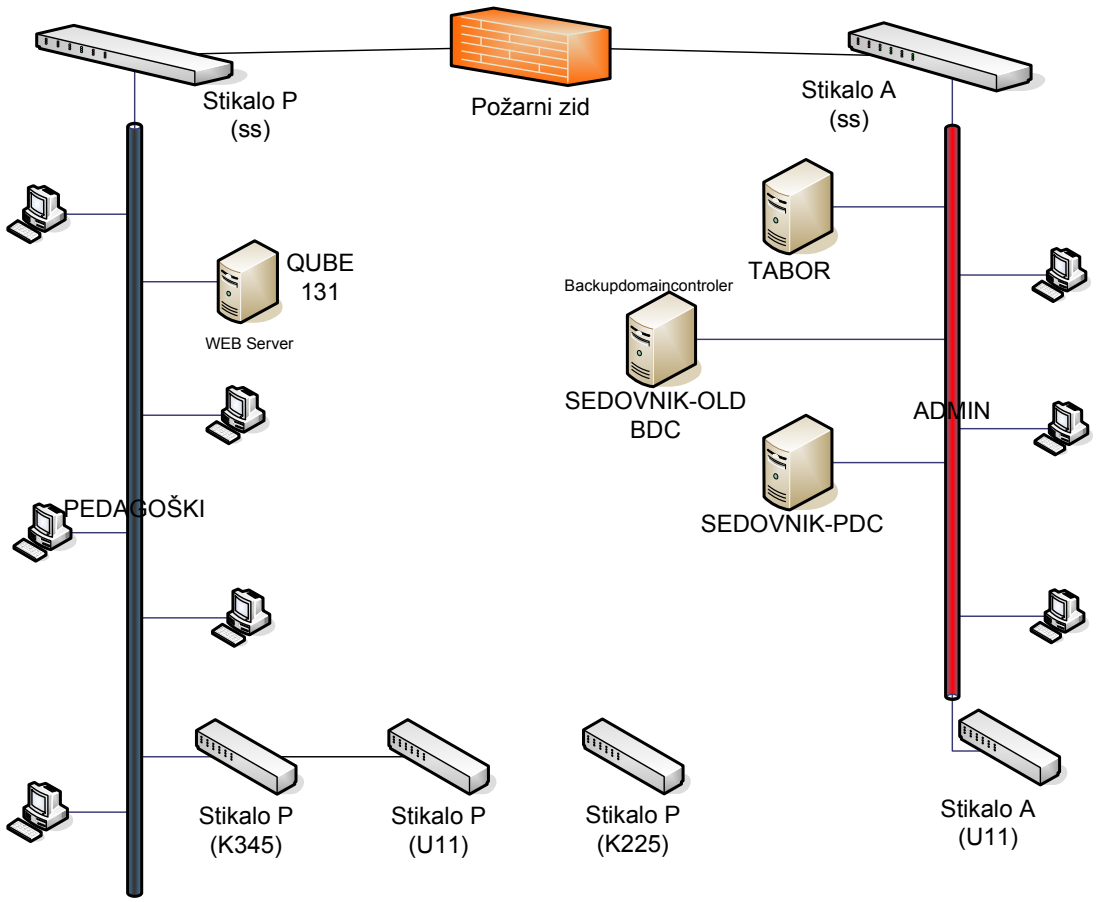
Slika 12: Vrhnji del logičnega modela omrežja

Logično je, da je vstopna točka v omrežje varovana s požarnim zidom, ki filtrira tok podatkov, ki prihaja iz omrežja WAN [4] v naše omrežje LAN[5]. Tako postane omrežje varnejše pred napadalci in zlonamerno programsko kodo. Stopnjo nižje lahko vidimo, kaj vse je pod okriljem posameznega stikala P in A. Na sliki 13 stikalo P vsebuje vse računalnike, ki so vključeni v pedagoški del, in tri podstikala, ki skrbijo za posamezne dele na pedagoškem nivoju, le ta se nahajajo v učilnici (U) in kabinetih (K). Ker je šola zgrajena iz več enot, vsako podstikalo skrbi za svoj del šolskega objekta.

---

[4] WAN – **W**ide **A**rea **N**etwork ali prostrano računalniško omrežje

[5] LAN – **L**ocal **A**rea **N**etwork ali lokalno računalniško omrežje

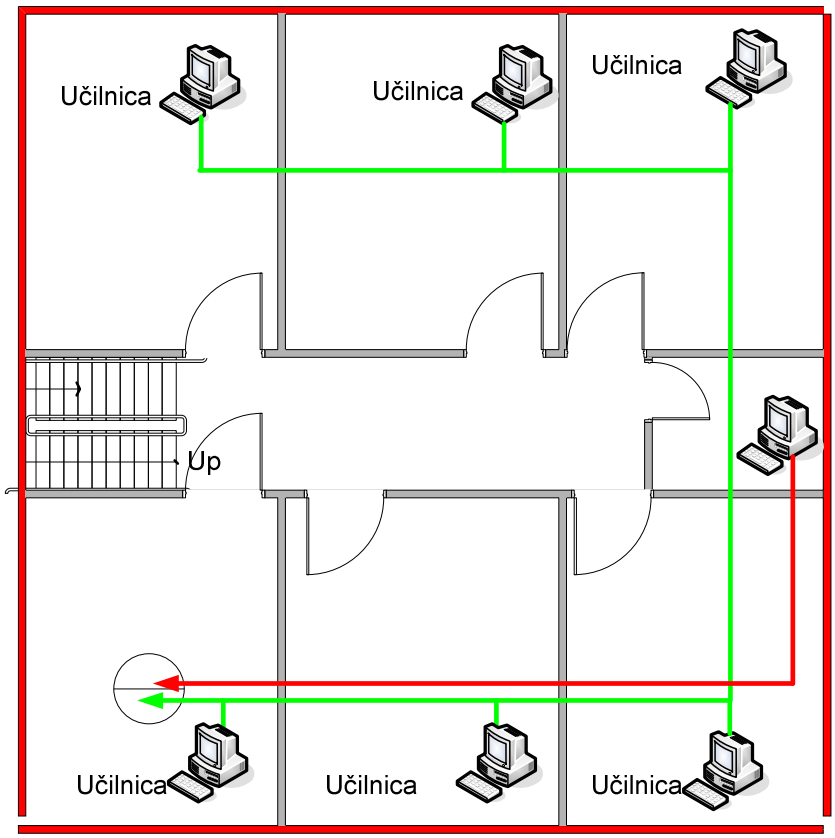


Slika 13: Podstikala šolskega omrežja

Prav tako je logično zgrajen administrativni del, katerega promet usmerja stikalo A(ss). Pod seboj ima le eno podstikalo na nižji stopnji, na katero je priključeno tajništvo. V administrativnem delu omrežja imamo postavljeno vso skrbniško opremo, skupaj s strežniki. Na sliki lahko vidimo strežnike Tabor, Sedovnik in Sedovnik old. Ti strežniki skrbijo, da se lahko posamezni delavci na šoli preko domenskega uporabniškega imena vključijo v sistem in upravljajo s svojimi datotekami, ki se nahajajo na strežniku. Na strežniku ima vsak uporabnik svoj del prostora, s katerim razpolaga, in skupen del, do katerega dostopajo vsi in je namenjen podajanju različnega gradiva. V grobem je strežnik zmogljiv računalnik, kateremu je dodeljena določena naloga, upravljanje z diski, tiskalniki, omrežjem, pošto. Na pedagoški strani lahko vidimo še strežnik Qube, to je spletni strežnik, ki vsebuje podatke za delovanje spletnih strani. Na primeru fizičnega modela bomo natančno prikazali nahajališče posameznega vozlišča ali strežnika in tako razložili princip delovanja oziroma upravljanja s šolskim omrežjem.

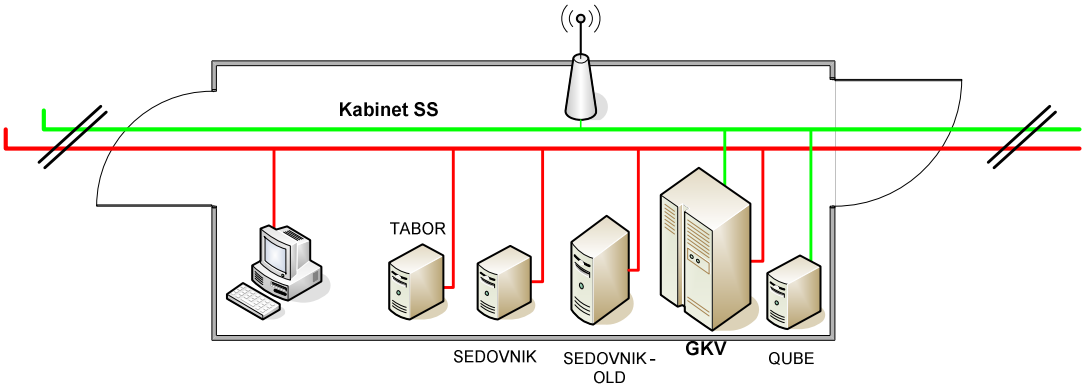
5.2. Fizični model računalniškega omrežja

Fizični model smo narisali zaradi lažje preglednosti strojnih elementov v šolskem omrežju. Vidimo lahko, kje v objektu se nahaja posamezna računalniška enota. V veliko pomoč bo tudi drugim šolskim sodelavcem, ki do sedaj niso imeli možnosti vpogleda v fizično strukturo, ali pa niso imeli podrobne predstave, kako je omrežje v šoli sploh zgrajeno in kako poteka izmenjava podatkov. V prilogi 2 si lahko ogledamo, kako izgleda omrežje na osnovni šoli. Pri risanju smo si pomagali z evakuacijskimi načrti, ki se nahajajo v vsakem večjem predelu šole. V pomoč so nam bili predvsem zaradi risanja tlorisa kleti, pritličja in prvega nadstropja. Tako smo lahko enostavno izrisali celoten podoben načrt šole. Načrt ni risan točno v merilu, ker to ni bilo bistvenega pomena. Poglobili smo se namreč v računalniško omrežje in njegovo napeljavo po zgradbi.



Slika 14: Primer fizičnega modela objekta

Na sliki 14 je prikazan odsek šole v prvem nadstropju. Vidimo šest učilnic, v katerih se nahaja po en računalnik. Na sredini je manjši prostor, imenovan kabinet za učitelje, v katerem je prav tako računalnik. Z zeleno črto so povezani računalniki v pedagoško omrežje, z rdečo črto pa računalniki, vključeni v administrativno omrežje. Računalniki v učilnicah so namenjeni tako učencem kot učiteljem in so postavljeni v delovno skupino Ucilnice. Omogočajo uporabo pisarniških in risarskih orodij ter dostop do lokalnega intraneta in svetovnega spleta. Računalniki v kabinetih, zbornici, računalnici, knjižnici in upravnih prostorih prav tako omogočajo uporabo vseh pisarniških orodij in dostop do svetovnega spleta le da so za razliko od pedagoškega dela omrežja priključeni v šolsko domeno. Uporabnik ima svoje uporabniško ime in geslo, tako da ima svoje lastno namizje, ki se hrani na strežniku, s katerim upravlja. Za vse to skrbi domenski strežnik (Sedovnik) ter strežnik datotek in vseh članov (Tabor), ki se nahaja v sistemski sobi šole, kot prikazuje slika 15.

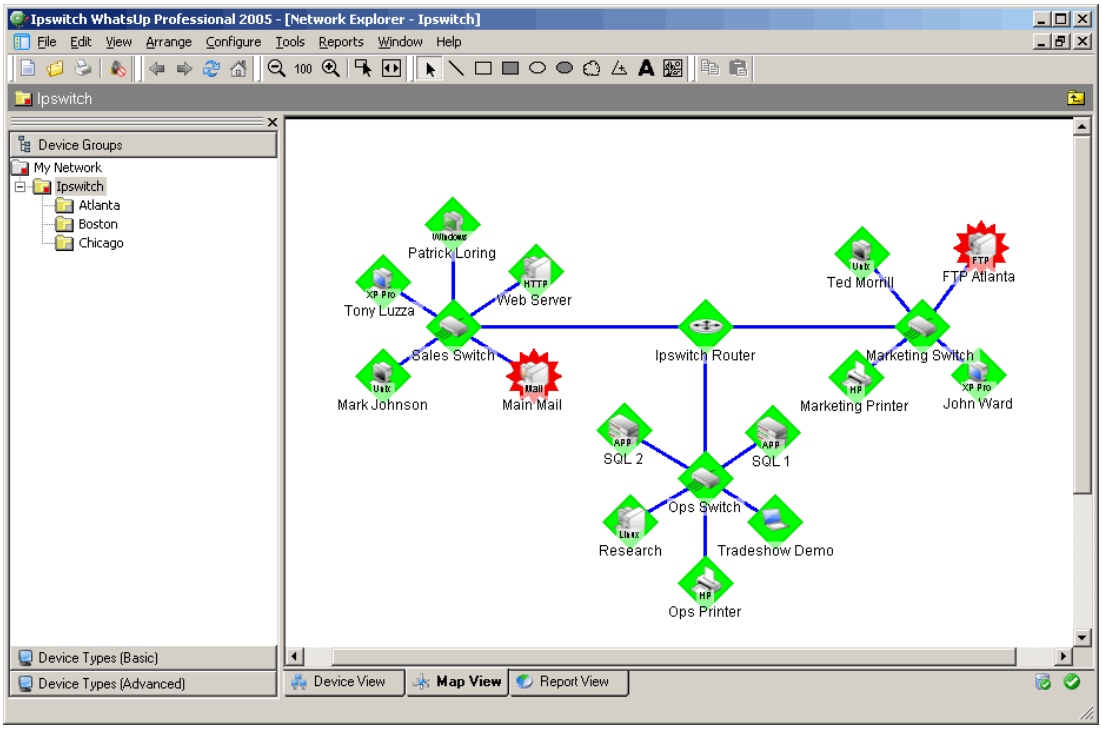


Slika 15: Sistemska soba

Zakaj sploh postavitev strežnikov? Osnovna naloga strežnikov je, da omogočajo dostop do skupnih baz podatkov in datotek ter da omogočajo uporabo skupnega mrežnega tiskalnika na šoli. Druga zelo pomembna funkcionalnost strežnikov je centralizirano shranjevanje varnostnih kopij, za katere skrbi strežnik Sedovnik Old. Vzdrževanje baz podatkov in distribucija programov se centralizira, kar pomeni večjo preglednost in v končni fazi manj dela z vzdrževanjem šolske informacijske tehnologije. Vse pravice dostopa uporabnikov do določenih podatkov se enostavno nastavi in nadzira, kar je v današnjih časih že skoraj nujno. Slika 15 prikazuje sistemsko sobo, kjer se nahajajo vsi strežniški terminali in glavno krajevno vozlišče ali usmerjevalnik (GKV). Lahko bi rekli, da je v tem kabinetu nekakšno »srce« šolskega računalniškega sistema, ki skrbi, da lahko vsi uporabniki v omrežju

nemoteno opravljajo svoje delo. Strežniki skrbijo, da se vse storitve, ki jih uporabniki ali administratorji zahtevajo, izvedejo pravilno in varno, ter v končni fazi zadovoljijo njihove potrebe.

Fizični model šolskega računalniškega omrežja smo gradili postopoma. Celotno sliko smo pridobili tako, da smo vsako učilnico oziroma prostor z računalnikom obiskali in popisali vso računalniško strojno opremo. Hkrati smo še podrobneje pregledali računalniški sistem, orodja in zaščito, ki je nameščena. Vse podatke smo zapisovali v poseben dokument, ki ga bomo v podpoglavju 5.3 podrobneje opisali. Ta dokument smo nato prenesli še v elektronsko obliko, ki bo služila pri nadaljnjem delu informatika na šoli. V naslednji nalogi je bilo potrebno vso strojno opremo logično povezati v mrežo, kot prikazujeta rdeča in zelena linija v prilogi 2. Do teh informacij smo prišli na več načinov. Vidne povezave, smo si ogledali in zabeležili, nekaj podatkov smo pridobili v načrtih zgradbe, ostalo pa smo pridobili iz pogovorov z zaposlenimi. Pri vseh zbranih informacijah smo lahko v prirejen načrt enostavno vnesli vse povezave od računalnika do računalnika dokler se mreža ni logično zaključila. Omenimo še posebno programsko opremo, ki nam je pomagala pri ugotavljanju strukture omrežja. Gre za IpSwitchev izdelek WhatsUp Professional, ki omogoča hitro povratno informacijo o topologiji omrežja in številu naprav, ki so priključene. Zaznavati in prikazovati zna usmerjevalnike, stikala, strežnike, tiskalnike in osebne računalnike. Na kratko, hitro lahko v posebej izdelanem raziskovalnem vmesniku programa logično prikažemo omrežje, kot prikazuje slika 16.



Slika 16: Primer topologije omrežja

Program vsebuje nekaj primarnih raziskovalnih metod, ki jih uporablja pri izrisovanju topologije. Metoda, ki smo jo uporabili mi, je bila SNMP SmartScan. Deluje tako, da prebere IP[6] naslove iz usmerjevalnikove tabele. Tako identificira tip vmesnika, vsa podomrežja in tekoče kritične procese. Na koncu vse enote razvrsti v skupine po posameznih stikalih, ki vzdržujejo dele podomrežij. Zelo uporabna metoda je nadzor neomejenega števila mrežnih naprav in opozarjanje na motnje, ki se pojavijo v omrežju.

[6] Internet Protocol – unikatna 32 bitna številka, s katero se računalnik izkazuje v internetni mreži

5.3. Opis naprav v šolskem omrežju

Razvili smo evidenčni karton, v katerem se bo beležilo stanje računalniških naprav, njihovih vhodno-izhodnih naprav in nameščenih programskih orodij. Današnja dokumentacija obstaja v papirni obliki in ni ažurirana oziroma dopolnjena. Problem se je namreč pojavil zaradi prevelikega števila računalnikov in njihovih komponent, ki so v omrežju. Informatika na šoli namreč velikokrat zanima trenutno stanje vse razpoložljive opreme. Za takšno informacijo pa potrebujemo osveženo bazo podatkov, ki mora biti redno vzdrževana, saj se zastarel in pokvarjen inventar velikokrat zamenja ali popolnoma odstrani (Žumer, 2003). Njegova življenjska doba je razmeroma kratkotrajna, tako da je veliko tudi novih elektronskih naprav, ki prihajajo v hišo. Na kratko lahko rečemo, da se dokumentacija oziroma arhiv šolske strojne opreme veliko spreminja, je zelo obsežen in zato potreben rednega vzdrževanja (Dogša, 1997). Odločili smo se, da kot pomoč pri dokumentaciji opreme uporabimo Microsoftovo orodje Excel 2002, ki omogoča urejanje in razvrščanje podatkov po celicah. Dokumentacija bo tako lažje obvladljiva, saj bo dograjevanje ali popravljanje potekalo hitreje in enostavneje. V vsakem trenutku bomo imeli možnost vpogleda v stanje razpoložljive opreme in število naprav, ki se nahajajo v šoli.

V nadaljevanju bomo podrobneje opisali, kako smo razvili evidenčni karton, da smo ugodili šolskim zahtevam po popisovanju in arhiviranju. Šola redno evidentira sredstva kot so šolske klopi, stoli, omare, pripomočki, orodja, grafoskopi. Ustrezne ažurirane dokumentacije glede šolskega omrežja in priključenih naprav pa trenutno nima. Zato smo razvili evidenčni karton, po katerem se beležita vsa strojna in programska oprema.

V prilogi 3 si lahko ogledamo končno podobo evidenčnega kartona. Odločili smo se, da dokument razdelimo na tri dele, z različnimi vsebinskimi sklopi. Prvi del glave dokumenta vsebuje osnovne informacije o lokaciji strojne opreme in uporabniku oziroma učitelju, ki opremo uporablja. Drugi del glave vsebuje osnovne podatke o napravi, tako da lahko izvemo za kakšen tip računalnika gre in kje se nahaja.

Učitelj	Opis prostora	Št. prostora	Lokacija	Količina
Janez Novak	Učilnica ZGO	203	Višja stopnja	1

Opis naprave	Wearnes Business Station PC 2,0	**Oznaka**	PC-U203
Dobavitelj		**S/N**	BS28008
Datum namestitve		**Evidenčna**	
Tip naprave	PC-C2,0Mhz 256Mb 40Gb		

Slika 17: Glava evidenčnega kartona

Na sliki 17 so razvidne posamezne celice, ki opisujejo naslednje elemente: ime učitelja, opis prostora v katerem se nahaja oprema, številka prostora na šoli, lokacija in pa količine naprav, ki so v prostoru. Drugi del vsebuje celice z vsebino o opisu naprave, njeni prepoznavni oznaki v omrežju, dobavitelju, datumu namestitve v omrežje, evidenčni številki in tipu naprave. Lahko rečemo, da so v glavi zbrani bistveni elementi, ki nas zanimajo.

Jedro dokumenta je tudi razdeljeno na posamezne vsebinske sklope, ki smo jih še nekoliko bolj razdrobili. V prvem delu, ki ga prikazuje slika 18, smo popisovali vse strojne elemente naprave in priključene vhodno izhodne komponente. Vnašali smo

STROJNA OPREMA				V/I KOMPONENTE		
	Tip	**Kapaciteta**	**Količina**		**Tip**	**Količina**
Matična Plošča	Abit	AT/133	1	**Monitor**	LCD 15«	1
Procesor	Celeron	2,0Mhz	1	**Tipkovnica**	Keytronic	1
Pomnilnik	SDR	256Mb	1	**Miška**	Logitech	1
HDD	Seagate	40Gb	1	**Multimedia**		
Grafika	Intel Integrirana	32Mb	1	**CD**		
Zvok	Intel Integriran		1	**CD-RW**		
Ethernet	Intel Integriran	100	1	**DVD**	Toshiba	1
Radix						

Slika 18: Prvi del jedra kartona

tipe vgrajenih elementov, njihove kapacitete in količine. Na drugi strani smo evidentirali še standardne vhodno izhodne naprave, kot so zaslon, tipkovnica, miška, optična enota, slušalke, mikrofon. Drugi del jedra smo uporabili za popisovanje nameščene programske opreme v računalniški enoti. Zanimalo nas je predvsem naslednje: kakšna vrsta programske opreme je nameščena, kakšni popravki so vključeni in kdaj je bil sistem nazadnje posodobljen. Ta del vsebuje samo podatke o sistemski programski opremi kot so operacijski sistemi, programi za zaščito pred zlonamerno programsko kodo ali za zaščito diskovnih razdelkov.

OPERACIJSKI SISTEM in OSTALA SISTEMSKA PROGRAMSKA OPREMA					
Operacijski sistem	**Vrsta**	**Verzija**	**Service Pack**	**Update**	**Opombe**
	WinXP	1	2	30.1.2005	
Ostala sistemska programska oprema orodja, baze, zaščita	SpyBoot				
	Deep	Freeze			
	AVG	Antivirus			
	Firewall	XP			

Slika 19: Drugi del jedra kartona

Sledi še zadnji tretji del jedra evidenčnega kartona, ki vsebuje podatke o aplikativni programski opremi, ki je nameščena v računalniškem sistemu in uporabnikih. Tukaj smo zbrali podatke o različnih orodjih za upravljanje dokumentov, risarskih orodjih, orodjih za predvajanje filmov in glasbe v različnih formatih, raznih internetnih vmesnikih, orodnih vrsticah in Windows dodatkih. V šolskih sistemih smo največkrat naleteli na Microsoftovo programsko opremo za upravljanje z dokumenti, kot so Word, Excel, PowerPoint, Access, potem risarsko orodje Corel Draw, predvajalnike Macromedia in pa Acrobat Reader, s katerim odpiramo dokumente PDF[7]. Na sliki 20 vidimo polje s podatki o skrbnikih in uporabnikih. Namenjeno je poročanju o skrbniku računalniške enote in uporabnikih. Vsaka enota ima namreč določenega skrbnika, ki namešča, odstranjuje ali odpravlja možne programske napake na sistemu, ki so ponavadi zelo moteče. Uporabniki so tako učitelji kot

[7] Portable Document Format - standarden za branje in tiskanje zaščitenih datotek

učenci in imajo namenoma omejene pravice uporabe, tako da je možnost okvare operacijskega sistema nekoliko manjša. Dostop do sistemskih datotek in programov jim ni dovoljen.

APLIKATIVNA PROGRAMSKA OPREMA:

	Vrsta	Verzija	Service Pack	Update	Opombe
MS Office		2003			
Corel Draw		9			
Jasc PhotoShop		6			
Acrobat Reader		5			
K-LiteCodec		3.5			

SKRBNIK-UPORABNIK

Skrbnik naprave	Administrator
Uporabnik1 **Uporabnik2** **Uporabnik3**	User

Slika 20: Tretji del jedra kartona

Sledi še opis noge evidenčnega kartona (slika 21). Tukaj se nahajajo podatki, ki so povezani s šolskim omrežjem, to so razne unikatne številke računalnikov in omrežij, domenska imena, maske omrežij, delovne skupine in nahajališča. Prva celica vsebuje podatek o IP številki računalnika. Takšna številka je unikatna, dodeljena s strani Arnesa in jo ima vsak računalnik, ki je povezan v internetno omrežje. Sledi celica z informacijo o prehodni številki, ki omogoča varno deljenje ene internetne povezave (ISDN, kabelski modem, ADSL, brezžične povezave, najete zveze) vsem računalnikom v omrežju.

IP-RAČUNALNIKA	193.xxx.xxx.xxx
Prehod	193.xxx.xxx.xxx
Ime naprave	PC-U203
Domena	
Maska	255.xxx.xxx.xxx
Delovna skupina	Učilnica
Nahajališče	I-xx

Hitri predogled VS

Slika 21: Noga jedra kartona

Naslednja celica vsebuje opis imena računalnika, ki je razvidno v delovni omrežni skupini. Nato imamo celico o domeni, ki jo izpolnimo samo pri računalnikih v

administrativnem delu omrežja, maski podomrežja, delovni skupini in nahajališču. Maska podomrežja pove mejo med omrežjem in delom IP naslovov, ki jih lahko uporabimo znotraj omrežja. Ta informacija je potrebna za omrežno opremo, kot so usmerjevalniki, ki rabijo za usmerjanje prometa samo podatek o omrežju. Delovna skupina je ime skupine računalnikov, na primer Učilnice, Knjižnica, Zbornica. Nahajališče je oznaka fizičnega priključka v omrežje, ki se nahaja v vsakem prostoru, v katerega vključimo mrežni kabel in tako računalnik povežemo v internetno omrežje.

Evidenčni karton vsake naprave smo zaključili s hitro bližnjico do seznama elektronskih naprav, ki jo lahko vidimo na dnu slike 21 pobarvano v oranžno. Ker je Excelov dokument obsežen in vsebuje veliko tako imenovanih listov, smo si bližnjico omislili zato, da lahko uporabnik hitreje dostopa do različnih evidenčnih kartonov. Ko seznam preberemo do konca, enostavno kliknemo na bližnjico hitri predogled, ki nas zopet postavi v osnovni meni naprav, kjer so evidentirani vsi šolski prostori s pripadajočimi elektronskimi napravami, kot je prikazano na sliki 22.

SEZNAM ELEKTRONSKIH NAPRAV

Št. Prostora	Opis prostora	Tip Naprave	Oznaka	Količina
K347	Kabinet	DTK P566 128 MB 10 GB Ethernet	PC-K347	1
U302	Učilnica	DTK P566 128 MB 10 GB Ethernet	PC-U302	1

Slika 22: Seznam elektronskih naprav

V seznamu naprav arhiviramo prostore po številkah (K347 - kabinet, U - učilnica), njihove opise, tipe naprav, ki se nahajajo v prostoru in njihove oznake ter količine, ki nam pomagajo pri zbiranju informacij o vseh razpoložljivih napravah na šoli. Tako smo vzpostavili krožni cikel, po katerem se uporabnik giblje.

6. VARNOST V ŠOLSKEM OMREŽJU

Cilj računalniške varnosti je zaščititi dragocene in občutljive podatke in hkrati omogočiti dostop pooblaščenim uporabnikom. Z varnostnimi ukrepi preprečimo brisanje in spreminjanje podatkov, krajo ali poneverbo podatkov in prekinitve ali motnje poslovanja. Vdori, zloraba podatkov in onemogočanje storitev tudi znižujejo ugled napadenega, na kar je večina podjetij še posebej občutljiva. Zato ni presenetljivo, da se o varnosti veliko govori in v zvezi z njo vse več ukrepa. Brez ustrezne zaščite je lahko vsak del omrežja oziroma vsak omrežni vir podvržen morebitnim zlorabam s strani neavtoriziranih oseb. Upravljalci omrežij pa se lahko proti tem zlorabam zaščitijo.

Poskusu zlorabe omrežnega vira rečemo napad (angl. attack). Napad je lahko usmerjen na infrastrukturo, kot so usmerjevalniki, stikala in podobno, ali proti končnim napravam, kot o osebni računalniki in v večini primerov strežniki. Strežniki so namreč elementi omrežja, ki jih zlahka identificiramo (spletni strežnik). Z omrežno infrastrukturo je drugače, saj so usmerjevalniki in stikala za samega uporabnika transparentni, zato jih je teže locirati in usmeriti napade nanje. Po drugi strani omrežne naprave v primerjavi s strežniki poganjajo veliko manj programske opreme. Iz tega sledi, da so napadi na takšno opremo redki in manj uspešni, če pa so že uspešni, so lahko zelo nevarni, saj napadalec z eno potezo zruši celo omrežje in ne samo enega strežnika. Zaradi enega strežnika v omrežju bodo uporabniki ravno tako dostopali do interneta, če pa se npr. zruši usmerjevalnik ali stikalo, je naše omrežje mrtvo, ker se ves promet naenkrat ustavi že na vhodu. Če navedemo nekaj vrst napadov, ki so najpogostejši, lahko začnemo z napadom, ki onemogoča izvajanje storitev (angl. Denial of Service – DoS), sledi napad z ugibanjem gesla ter napad na znane varnostne luknje. Napadalec namreč preobremeni informacijski sistem preko njegovih zmogljivosti in to iz različnih virov, tako da ne moremo točno določiti, kje se napadalec nahaja. Ta grožnja sicer ne ogroža varnosti informacij, vendar moti redno poslovanje in prav tako ovira poslovanje (Hribar, 2003).

Informacijska tehnologija k sreči ponuja orodja, s katerimi lahko omilimo, če ne že popolnoma onemogočimo naštete grožnje, med katerimi nekoliko izstopa že omenjena dostopnost informacijskih sistemov. V ta namen postavimo požarno

pregrado (angl. Firewall) med internet in sisteme, ki sodelujejo pri izmenjavi podatkov. Požarno pregrado šola ima in jo oskrbuje. Dobra lastnost požarnih zidov je, da ne le omejijo dostop do notranjih sistemov, temveč tudi zavračajo vhodni promet na podlagi ocene, da poteka napad DoS in tako zavarujejo sistem pred prevelikimi obremenitvami. Ostale poglavitne tehnologije, s katerimi zagotovimo zaupnost, verodostojnost, integriteto in nezanikanje, so vezane na simetrično in asimetrično kriptografijo, infrastrukturo javnih ključev in vedno bolj uveljavljeni digitalni podpis, ki ga šola že uporablja. V nadaljevanju bomo opisovali, kako šola skrbi za svojo varnost, tako na fizičnem kot logičnem nivoju (Žagar, 2002).

6.1. Programska varnostna oprema

Past se skriva v tem, da so ustanove vse bolj odvisne od avtomatizacije poslovnih procesov, povezovanje avtomatiziranih elementov v enovit sistem pa povečuje ranljivost oziroma izpostavljenost. Najbolj sporen je namreč dostop do svetovnega spleta, kjer se poskušamo predstaviti svetu s svojimi storitvami ali izdelki. Če sistem ni ustrezno zaščiten, lahko nehote omogočimo zlorabo dostopa in storitev omrežja nelegitimnim uporabnikom, ki nam povzročajo škodo. Ker je človeški nadzor nad vse bolj zapletenimi sistemi v omrežju, ki so vse bolj zmogljivi, težak, če ne že nemogoč, nam izdelovalci omrežne opreme v ta namen ponujajo strojne in programske rešitve, katerih edini namen je preprečevanje nelegitimne uporabe omrežja ter omrežnih virov. Ti sistemi, ki jih uporablja tudi šola in jih bomo zato opisali, pa morajo biti čim bolj avtonomni, sami po sebi varni, transparentni za legitimnega uporabnika ter neprepustni za vse druge poskuse nelegitimne rabe (Stubelj, 2002).

Kot smo omenili že v četrtem poglavju, omrežna varnostna politika določa, naj bodo vsi postopki uporabe in zaščite omrežja zapisani v posebnem dokumentu, ker bomo le tako lahko preverili, ali dejansko stanje ustreza začrtanim merilom. Dokument služi tudi kot zapis naših aktualnih znanj, ki smo jih dosegli s področja varnosti in jih seveda sproti dopolnjujemo. V evidenčni karton smo zato vključili tudi popise programske varnostne opreme, ki se izvaja na šolski strojni opremi. V vsakem trenutku lahko pogledamo, kakšna zaščita je nameščena na posamezni komponenti in

kdaj je bila nazadnje posodobljena. Na sliki 23 vidimo, kako smo šolsko varnostno programsko opremo vključili v evidenčni karton.

OPERACIJSKI SISTEM in OSTALA SISTEMSKA PROGRAMSKA OPREMA

	Vrsta	Verzija	Service Pack	Update	Opombe
Operacijski sistem	WinXP	5,1	2	12.2.2005	
Ostala sistemska programska oprema orodja, baze, zaščita	Deep Freeze Spy-Bot S&D AVG - antivirus			12.5.2005 12.2.2005	

Slika 23: Popis varnostne programske opreme

Celica ostala sistemska programska oprema vsebuje tri vrste programov, ki skrbijo za zaščito računalnika. To so antivirusni program AVG, program za odkrivanje zlonamerne vohunske programske kode SpyBot in programska računalniška zaščita sistemske particije Deep Freeze. AVG antivirus skrbi za zaščito računalnika pred različnimi virusi. Omogoča redno posodabljanje in ročno odkrivanje okuženih datotek ter sprotno transparentno pregledovanje poštnega predala, v katerem bi se lahko nahajala okužena priponka. Spybot je prav tako program za odkrivanje okuženih datotek z vohunsko kodo, ki jo poznamo pod imenom trojanski konj ali črv. Računalnik ščiti tako, da poskuša že pred namestitvijo črva na naš računalnik postaviti prepreko in odbiti takšno vrsto datotek. Med ročnim pregledom zna črva ali trojanca tudi poiskati v registru operacijskega sistema in ga odstraniti. Tretji varnostni program pa se nekoliko razlikuje od ostalih dveh, saj ni namenjen odkrivanju okuženih datotek, temveč ščiti določen segment trdega diska. Ponavadi je to sistemska particija C:, kjer se nahaja operacijski sistem, ki je zelo občutljiv, če mu kakšen del sistemskih datotek nevede zbrišemo. Deep Freeze je zelo uporaben, saj zna celoten sistemski del zamrzniti. Lahko bi rekli, da si zapomni celotno datotečno strukturo (angl. Image file) in jo ob morebitnih spremembah pri ponovnem zagonu obnovi. Lahko rečemo, da v grobem nadomešča strojno rešitev, znano PCI kartico Radix, ki jo bomo opisali v nadaljevanju.

Poleg omenjenih zaščit šola uporablja še protivirusno programsko opremo F-Secure, ki predstavlja nekakšen skupek vseh zaščitnih programov v enem. S centralnim

upravljanjem in enostavnim uporabniškim vmesnikom lahko nadzorujemo protivirusno zaščito, aktiven požarni zid, aplikacije, ki jih uporabniki poganjajo, ter onemogočamo vdore. Pri tem je zanimivo, da lahko administrator centralno določa, kateri programi imajo dostop do interneta. Tako lahko na primer onemogočimo poganjanje programov za izmenjavo datotek. Na evidenčnem kartonu v prilogi št. 3 lahko vidimo tudi, da beležimo, kdo je skrbnik računalnika in kdo uporabnik. To pa hkrati pomeni, da je računalnik zaščiten z geslom in omejen s pravicami. Navadni uporabniki imajo omejen dostop do datotek in nimajo pravic nameščanja programske opreme, kot to lahko stori skrbnik. Edina možna težava je, da lahko pomotoma zbrišemo sistemsko datoteko. Takrat nam v pomoč priskočita že omenjena Deep Freeze ali strojna zaščita Radix, ki sistem povrneta v prejšnje stanje.

Če na kratko povzamemo stanje zaščitne programske opreme na šoli, lahko rečemo, da lokalno vsak osebni računalnik v omrežju vsebuje:

- požarni zid antivirusnega programa,
- protivirusni program (AVG, F-Secure),
- program za odkrivanje vohunske zlonamerne kode (SpyBot, Ad-Aware),
- program za zaščito trdega diska (Deep Freeze),
- omejen račun Windows uporabnika, ki ga določi skrbnik,
- skrbniški Windows račun,
- operacijski sistem, ki temelji na NT tehnologiji.

Kot smo že omenili, je omrežje fizično ločeno na administrativni in pedagoški del. V administrativnem delu omrežja, kjer se uporabniki prijavljajo v domeno, sistemskih zaščit trdih diskov (Deep Freeze ali Radix) ni, ker sistem ob vsaki prijavi ustvari določene spremembe na sistemski particiji in bi seveda ob ponovnem zagonu računalnika uporabnik izgubil svoje spremenjene datoteke.

6.2. Fizična zaščita in zaščita okolja

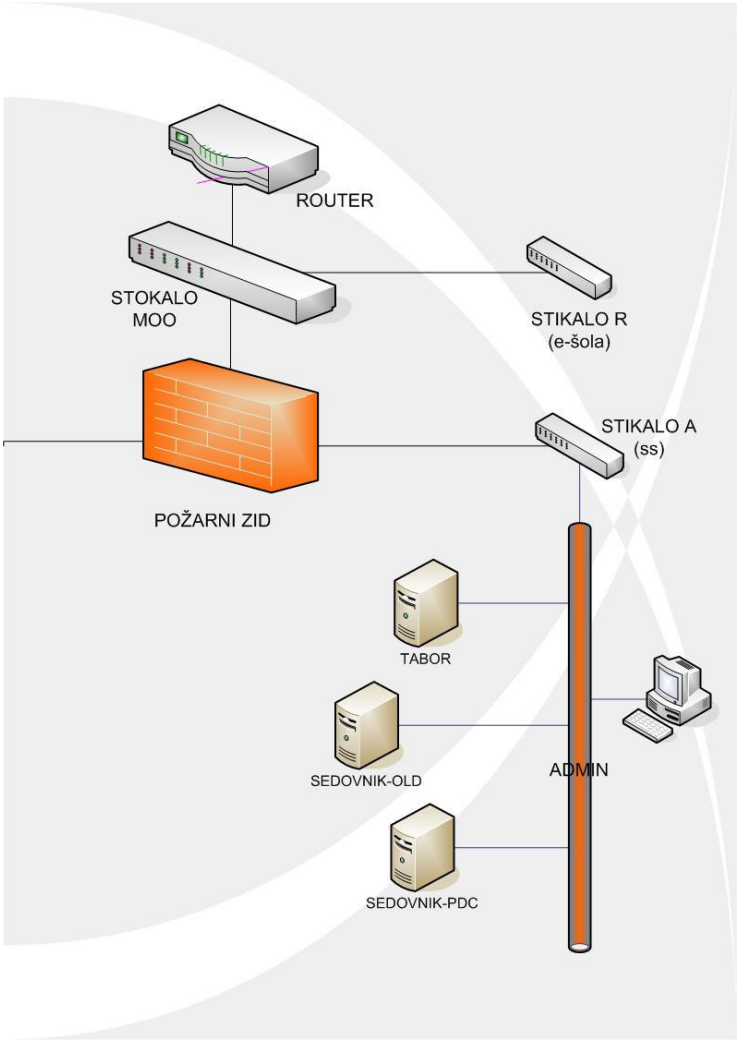
V tem poglavju se bomo osredotočili na že omenjeni britanski standard BS ISO/IEC 17799:2000, ki zagotavlja ustrezne varnostne ukrepe, ki ščitijo informacijska sredstva in dajejo uporabnikom veliko zaupanje. Standard je razdeljen na deset kontrolnih ciljev oziroma delov procesa SUVI[8], mi pa se bomo poglobili v sedmi kontrolni cilj (A.7), ki se navezuje na fizično zaščito informacijskega sistema.

Prvo izmed treh podpoglavij fizične zaščite določa varovanje šolskega območja, kot je preprečevanje nepooblaščenega fizičnega dostopa, škode in motenj v poslovnih prostorih in informacijah. Šola uspešno izpolnjuje cilje in nadzor fizičnega dostopa z alarmnimi napravami, tako da je nepooblaščen dostop nemogoč brez identifikacijskega gesla. Varovana so vsa območja, tako pisarn, kot šolskih prostorov. Glavna vhoda sta posebno zaščitena z video nadzorom. Kot dodaten nadzor pri delu na varovanih območjih šola uporablja sistem prijave z geslom oziroma prijave v domenski strežnik. Vsaka prijava in sprememba na sistemu je zabeležena in se hrani v posebnih datotekah, ki jih upravlja administrator.

Poglavje varovanje opreme obravnava izgubo, poškodovanje sredstev in prekinitev poslovnih dejavnosti. Glavna sistemska oprema je ustrezno zaščitena v sistemskem prostoru in nameščena tako, da je tveganje pred naravnimi in drugimi nesrečami minimalno. Dovod energije je zagotovljen z napravami za nemoteno napajanje ob izpadu električnega toka, električni in telekomunikacijski kabli so zaščiteni pred prestrezanjem in poškodbami. Oprema je pravilno vzdrževana in tako zagotavlja razpoložljivost in celovitost. Sistemski administrator ima na razpolago dostop do sistemske sobe tudi izven šolskih prostorov, na daljavo. Dostop je ustrezno zaščiten z gesli in požarnimi zidovi. V ta namen je prilagojen šolski usmerjevalnik, ki zna odpreti pot skrbniku do glavnega strežnika. Šola ima na razpolago posebno varovano sobo za hranjenje uničene ali zastarele opreme, ki je vsebovala šolske informacije. Pred uničenjem je zagotovljeno, da se vse informacije zbrišejo in arhivirajo na nadomestni del. Tretje podpoglavje vzpostavlja zagotavila za preprečevanje kraje

[8] Sistem za upravljanje varovanja informacij

informacij in naprav za obdelavo informacij. Tudi odstranjevanje opreme in informacij ali programske opreme, ki so last šole, brez dovoljenja vodstva ni mogoče. Med fizično zaščito spada tudi že omenjena razdeljenost omrežja na administrativni del, ki je označen z rdečo barvo in drugi pedagoški del. Povedali smo že, da se v sistemski sobi, ki je ustrezno varovana (slika 24), nahajajo trije strežniki, ki skrbijo za nemoteno delovanje šolskega sistema.



Slika 24: Strežniška oprema na administrativnem delu omrežja

Tukaj velja omeniti bistvo arhiviranja in varovanja podatkov s tehnologijo RAID[9] Level 5, ki se izvaja na strežnikih Sedovnik Old in Tabor, ki ju poganjata

[9] Redundant Arrays of Inexpensive Disks – Redundančno polje neodvisnih diskov

operacijska sistema Windows NT4 in Windows Server 2003. Kaj sploh je in kako deluje tehnologija RAID? Osnovna ideja je združiti male in poceni trde diske v diskovna polja, ki po sposobnostih in hitrostih presegajo delovanje standardnih diskov (RAID, 2005). Takšna diskovna polja potrebujejo posebno krmilno logiko, kar lahko dosežemo s posebnim krmilnikom RAID ali z nastavitvami v nekaterih zmogljivejših operacijskih sistemih (NT, Linux, Win2000, XP). Glede na način uporabe delimo diskovna polja v več vrst, ki so označena s številkami od 0 do 6. V šolskem sistemu se uporablja diskovno polje RAID Level 5. Prednost diskovnih polj je velika varnost podatkov. Gre za konfiguracijo s pari enakih diskov, v kateri se podatki podvajajo. Polje je v primerjavi z enim diskom hitrejše pri branju in počasnejše pri pisanju, če odpove en disk lahko brez problema uporabljamo drugega in ne izgubimo podatkov. Večji strošek je le, da moramo nabaviti vsaj še en trdi disk, v našem primeru pa dva, tako da imamo tri identične diske. Naj omenim da metoda level 2 zahteva sedem navadnih diskov, to pa zaradi nadzornih bitov, ki kasneje omogočajo obnovitev datotek ob odpovedi. Način Level 5 je v praksi najbolj uporabljen predvsem zaradi dejstva, da odpravlja ozko grlo paritetnega diska, kar se kaže pri uporabi velikega števila diskov v sistemih RAID 3 in 4. Z uporabo tega sistema sicer izgubimo kapaciteto enega diska, vendar je zagotovljena zanesljivost, saj lahko sistem navzlic odpovedi enega izmed diskov obnovi vse podatke in nemoteno deluje dalje. Tako poleg naprav za neprekinjeno dovajanje energije uporabimo še aplikacijo za neprekinjeno razpoložljivost podatkov in dosežemo, da so naši podatki na razpolago ob vsakem času.

Vendar pa je po našem mnenju med vsemi zaščitami še najbolj učinkovit požarni zid, ki se nahaja v usmerjevalniku šolskega omrežja, kot je prikazano v prilogi 1. Zaščitni postopki so zapisani v pravilih prepustnosti podatkov skozi posamezna vrata in sum na določen pretok zlonamerne kode, ki jo lahko še v pravem času ustavimo. Omenimo, da je usmerjevalnik prometa šolskega omrežja upravljan s strani Arnesa, tako da zapore vrat in postopki ločevanja podatkov (požarni zid), zagotavljajo zanesljivo prepustnost. Pomembno je, da pregrade same po sebi nimajo razpok v sistemu varnosti, zato tudi ne omogočajo številnih storitev, kot so usmerjevalni protokoli ali nadzor z drugega računalnika. Prva naloga je varnost, šele na to pride na vrsto storitev.

V današnjem času je vse bolj razširjeno spoznanje, da so rob omrežja (priključne točke) tudi pristopna stikala, na katera so vezani uporabniki. V šolskih prostorih je takih vtičnic veliko in je vse težko nadzorovati. V ta namen nam služi standard 802.1x, ki omogoča preverjanje uporabnika, ki zahteva priključitev v omrežje. Podobne rešitve se uporabljajo tudi pri uporabi brezžičnih pristopnih točk. Tako brezžično prijavno točko šola ima in jo uporablja. Vendar pa takšna točka predstavlja večjo nevarnost vdora, zato je bolj varovana in je namenjena samo sistemskemu administratorju. Nekatera podjetja imajo veliko takšnih dostopnih točk, ki so lahek plen za nepooblaščene uporabnike. Takšnega uporabnika tudi teže odkrijemo, saj ga v omrežju vidimo pač kot našega pooblaščenega uporabnika. Pot preko vseh požarnih zidov in zaščit na daljavo je težja, kot pa če se fizično priključimo v sistem in se vsem zaporam izognemo.

Tudi v tem podpoglavju lahko na kratko povzamemo bistvene fizične varnostne elemente, ki ščitijo šolski omrežni sistem:

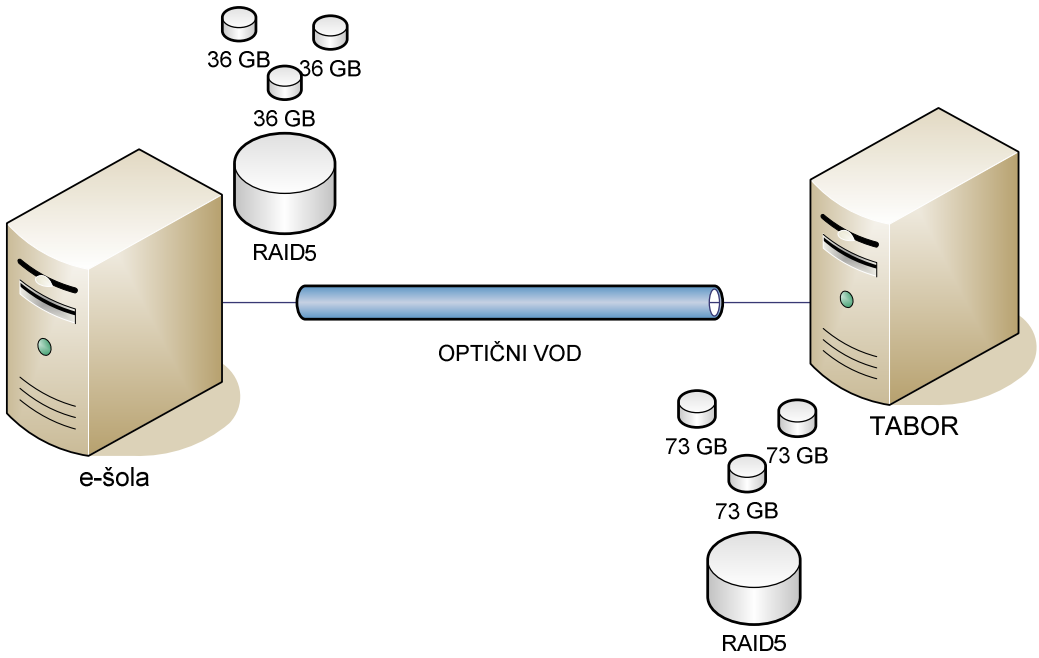
- alarmna naprava,
- video nadzor,
- ločen administrativni in pedagoški del omrežja,
- požarni zid na usmerjevalniku prometa,
- diskovna polja RAID,
- strojna kartica PCI Radix,
- strežniško upravljanje,
- ločeni kanali električne in telekomunikacijske napeljave.

6.3. Nadaljnja skrb za varnost

Računalnikarji dobro vemo, da ni metode, ki bi zagotavljala 100–odstotno varnost tako pred vdori v sisteme kot pred krajo opreme. Lahko se le uspešno približujemo popolni zaščiti, tako da nenehno vlagamo v najnovejšo tehnologijo in se izobražujemo na področju varnostne politike. Žal so napadalci na »privlačna« okolja kljub naši skrbno postavljeni hierarhiji varnostnih mehanizmov vedno korak pred nami in samimi razvijalci varnostnih storitev. Kar nam preostane je, da se veliko zanimamo za računalniško varnost, upoštevamo strokovne nasvete in se v najkrajših možnih časih tudi odzivamo na morebitne napade, ki so se že zvrstili drugje in se jim tako po možnosti izognemo. Velikokrat nas lahko reši informacija o širjenju zlonamerne programske kode, ki pride do nas nekoliko prej kot sam napad. Velik pomen bi tako pripisali posodobitvam programske opreme, tako operacijskih programov kot protivirusnim in protivohunskim programom. Torej bodimo v koraku s časom in se uspešno prilagajajmo celotnemu sistemu, čeprav bomo morali tudi kdaj globlje seči v žep.

Veliko smo razmišljali o morebitnih razpokah in šibkih točkah sistema, katerih odprava bi pomenila velik korak naprej v naši varnosti. Kljub zavidljivi varnostni politiki, ki jo šola izvaja, pa se vedno najde kakšna izboljšava sistema. Omenili smo že, da je »srce« šolskega omrežja skrbno varovano v sistemski sobi. Podatki se vsakodnevno arhivirajo in so varni pred morebitnimi izpadi ostalih šolskih pomnilniških kapacitet. Pomislili smo na morebitno naravno nesrečo, ki se lahko pojavi ravno v sistemski sobi, najsi bo to požar, poškodba vodovodne cevi ali celo kraja samega strežnika. V takem primeru bi prišlo do uničenja arhiva in ostalih varnostnih kopij ter hkrati do popolne izgube vseh podatkov. Tako bi bilo smiselno imeti dva enaka arhiva, vendar na različnih lokacijah. Če katera od pomnilnih komponent zgori ali se trajno poškoduje, imamo še vedno rezervno kopijo podatkov. Pri takšnih nesrečah nam ne pomaga tudi tehnologija RAID. Šola ima izobraževalni center imenovan e-šola, ki se nahaja blizu osnovne šole, v taborniški hišici. Tam se ravno tako kot v šoli nahaja strežnik s tehnologijo RAID, ki skrbi za dvanajst računalnikov, na katere se prijavljajo uporabniki. Na sliki 24 lahko vidimo zamisel, po kateri bi se odvijalo vsakodnevno kopiranje šolskega arhiva v hišico in obratno. Kar bi bilo potrebno je, da bi morali speljati optični kabel od hišice do šole in

nabaviti dva optično-električnega pretvornika. Tako bi bila vzpostavljena dovolj hitra povezava, po kateri bi v zadovoljivem času vsakodnevno prenašali arhive. Tako bi šola postala varna tudi pred morebitnimi naravnimi nesrečami ali odtujitvami same strojne opreme s podatkovnimi nosilci.



Slika 25: Optični vod med e–šolo in šolo

Omenili smo že, da ima šola v sistemski sobi strežnik Tabor, ki vsebuje tri trde diske po 73 GB, ki so združeni v diskovno polje RAID Level 5. Podoben strežnik je tudi v e-šoli, le da so kapacitete trdih diskov trikrat po 36 GB. Ti prav tako delujejo z logiko RAID 5, kot prikazuje slika 24.

S tem poglavjem tako zaključujemo jedro diplomske naloge. Na podlagi izkušenj in pridobljenega znanja, bomo v zaključnem poglavju zapisali naše ugotovitve in usmeritve za nadaljnje delo.

7. ZAKLJUČEK

Napredek tehnologije in medijev je povzročil, da vse več uporabnikov uporablja različne naprave za elektronsko komuniciranje. Tako nastaja vse več podatkov v elektronski obliki, ki se jih velikokrat niti ne more natisniti, oziroma bi s tiskanjem na papir izgubili bistvene značilnosti. Tradicionalno pisarniško poslovanje z razvojem informacijskih tehnologij izpodrivajo elektronske oblike poslovanja. Posledica hitrega uveljavljanja omenjenih tehnologij je rast količine gradiva v elektronski obliki, ki ga je potrebno ustrezno varno arhivirati na posebnih trajnih podatkovnih nosilcih. Podatki morajo hkrati biti tudi dosegljivi in primerni za poznejšo uporabo. Tako se organizacije, ki se odločijo za elektronsko hrambo, soočajo s pomembnimi vprašanji za uspešno poslovanje. Tu mislimo predvsem na ureditev postopkov, ki bodo zagotavljali avtentičnost, celovitost in varnost podatkov. Takšni postopki pa so lahko pretvorbe papirnatega gradiva v elektronsko obliko, postopki za zagotavljanje varne hrambe gradiva in varnostna shema za dostop do shranjenega elektronskega gradiva. Poleg navedenih postopkov pa pri urejeni elektronski hrambi nikakor ne smemo pozabiti tudi na učinkovit nadzor.

V tej diplomski nalogi smo govorili prav o takšnih postopkih. Papirnate dokumente, ki so služili za evidenco šolskega omrežnega sistema, smo pretvorili v elektronsko obliko in jih shranili na ustrezne podatkovne nosilce, ki so postavljeni v varovanih območjih. Ker so podatki dostopni tudi izven šolskega omrežja, smo morali poskrbeti za varno upravljanje in dostop do celotnega gradiva. Za uspešno varovanje pa je potrebno do potankosti razumeti delovanje omrežja, z vso pripadajočo strojno in programsko opremo. Med dograjevanjem šolskega omrežja smo tako prišli do nekaterih bistvenih spoznanj, ki so nam pomagala pri razumevanju delovanja. Spoznali smo, kako omrežje deluje in kateri so najpomembnejši deli, ki s sistemom upravljajo. Naša spoznanja in ugotovitve smo zabeležili v elektronske dokumente, ki smo jih obdelovali z izbranimi računalniškimi programi. Tako nastali diagrami bodo služili zunanjim sodelavcem ali oskrbovalcem, ki bi radi spoznali šolski omrežni sistem in njegovo delovanje. Pravzaprav lahko diagrami služijo tudi kot predstavitev urejenega šolskega omrežja učencem in sodelavcem, ki omrežje velikokrat uporabljajo, vendar si ne znajo predstavljati, kako se njihovi podatki po njem prenašajo. Celotna arhitektura in delovanje omrežja sta skrbno načrtovana in

dodelana, tako da lahko sheme služijo tudi kot primer pri gradnji novih omrežnih sistemov na šolah ali drugih ustanovah.

Naše delo se je začelo s postavljanjem novih računalniških sistemov v šolsko omrežje. Hkrati smo prvotni papirni dokument za popis tehničnih elementov razdelili na manjše dele in si tako ustvarili model trenutnega elektronskega dokumenta kot ga prikazuje priloga 3, ki ustreza šolskim merilom. Takšen dokument smo začeli kmalu uporabljati za popisovanje, pri dograjevanju in spoznavanju sistema. Tako smo dobili obsežnejšo Excelovo datoteko, ki dejansko zajema devetdeset evidenčnih kartonov ali listov, to pa pomeni okrog 600 KB prostora na pomnilnem mediju. Celoten dokument smo dopolnili v roku enega meseca, tako da smo dejansko obiskali vsako fizično napravo, ki se nahaja v šolskem objektu. Ko smo dokončno zabeležili in arhivirali šolske elektronske naprave, smo se lahko lotili risanja fizičnega in logičnega modela omrežja, kot ju prikazujeta prilogi 1 in 2. Podatke o omrežju smo zbirali na različne načine, saj so bili razpršeni po posameznih dokumentih ali sploh niso bili zapisani. Za nekatere podrobnejše informacije o poteku kabelske napeljave smo povpraševali osebe, ki so pri projektu sodelovale. Za dokončno podobo fizičnega in logičnega modela omrežja smo porabili dober mesec. Modela sta arhivirana v formatu slike (*.jpg), ki ju uporabljamo pri predstavitvah, in v formatu (*.vsd), ki ga podpira programski paket Visio 2003. Slednjega uporabljamo za posodobitve ali spremembe. Skupina tako nastalih elektronskih dokumentov zaseda na pomnilnem mediju 5 MB. Novo nastali dokumenti, ki se bodo v bodoče uporabljali za predstavitve ali evidenčne namene, so shranjeni na določenih varovanih podatkovnih nosilcih v sistemski sobi šole. Dostop do njih je omejen in določen s strani skrbnika, ki z dokumentacijo tudi upravlja.

Z vso razpoložljivo dokumentacijo, ki smo jo razvili in dodelali, upravlja le informatik ali skrbnik sistema na šoli, ki ob morebitnih spremembah dopolnjuje manjkajoče podatke. Skrbi, da so evidenčni kartoni posodobljeni in se ujemajo z dejanskim stanjem elektronskih naprav in programske opreme. Vendar pa bi lahko bili v prihodnje potencialni uporabniki tudi nekateri učitelji, ki imajo izkušnje na področju uporabe Excela. Nenazadnje so v večini primerov sami uporabniki računalniških sistemov, ki jih velikokrat spreminjajo in tako sami najbolje vedo, v kakšnem stanju so. Zelo težko je namreč skrbniku celotnega sistema vedeti in

nadzirati, do kakšnih sprememb prihaja na posameznih napravah. Tako bi bilo najbolje, da bi uporabniki sami skrbeli za svoj evidenčni karton, ki bi se nahajal v skupni mapi z določenimi pravicami. Uporabniki računalniške enote se v sistem prijavljajo z gesli ter tako nedvoumno dokažejo svojo identiteto, ki je razvidna tudi v evidenčnih kartonih. Vsak uporabnik tako odgovarja za svoje ažurirane podatke. Smisel beleženja se pojavi v trenutku, ko nas zanima število nekaterih strojnih ali programskih elementov, ki se nahajajo v omrežju. Pri inventuri bomo tako hitro prišli do podatka, ki nas zanima. Morda bomo želeli podatek o računalniških enotah določenega proizvajalca na šoli ali pa koliko barvnih tiskalnikov trenutno imamo. Zanimiv je tudi podatek o prostih IP naslovih, ki jih lahko uporabimo, ali pa v kateri napravi se nahaja določena številka. Takšnih poizvedb je lahko zelo veliko, tako da je smisel beleženja in osveževanja dovolj jasen. Do nekaterih zapletov pri uporabi lahko pride le ob drastičnem povečanju števila naprav v sistemu. Pri Excelovi preglednici smo namreč omejeni glede števila evidenčnih kartonov. Ob takšnih spremembah bi bilo smiselno beleženje podatkov v podatkovno bazo, ki omogoča večje število vnosov. Za začetek bi si lahko pomagali z Accessovo podatkovno bazo. Za šolske potrebe po arhiviranju podatkov je dovolj zmogljiva in uporabna. Morda se kdaj v prihodnosti pojavi še kakšna potreba po beleženju ostalega inventarja, tako da bi bilo takrat smiselno razviti lasten relacijski podatkovni model, ki bi zagotavljal dovolj zmogljiv modul arhiviranja.

Ob vsem tem pa ne smemo pozabiti na uspešno varovanje tako nastalega elektronskega gradiva, ki je bistvenega pomena za uspešno delovanje ustanove. V diplomski nalogi smo se dotaknili celovitega varovanja podatkov, ki zajema bistvene varnostne elemente. Prav tako smo opisali, kako najbolje skrbimo za šolsko omrežje, tako z uporabo fizične kot programske zaščite. Če se ne moremo odločiti, kaj pravzaprav varujemo, potem ni smiselno izvajati tega opravila. Če govorimo o organizaciji, to pomeni, da moramo imeti cilje in usmeritve varovanja. Tudi ko smo že določili cilje, s tem še nismo končali, saj so lahko cilji preozko zastavljeni.

Končno bi navedli še nekatera napačna razmišljanja o varovanju informacij. Prva takšna zmota je, da je varnost informacij stvar oddelka za informacijsko tehnologijo. Tveganja so tudi v vseh drugih poslovnih procesih, ki jih informatiki ne opravljajo in tudi nimajo opravka z njimi. Varnost je stvar celotne organizacije in ne samo enega

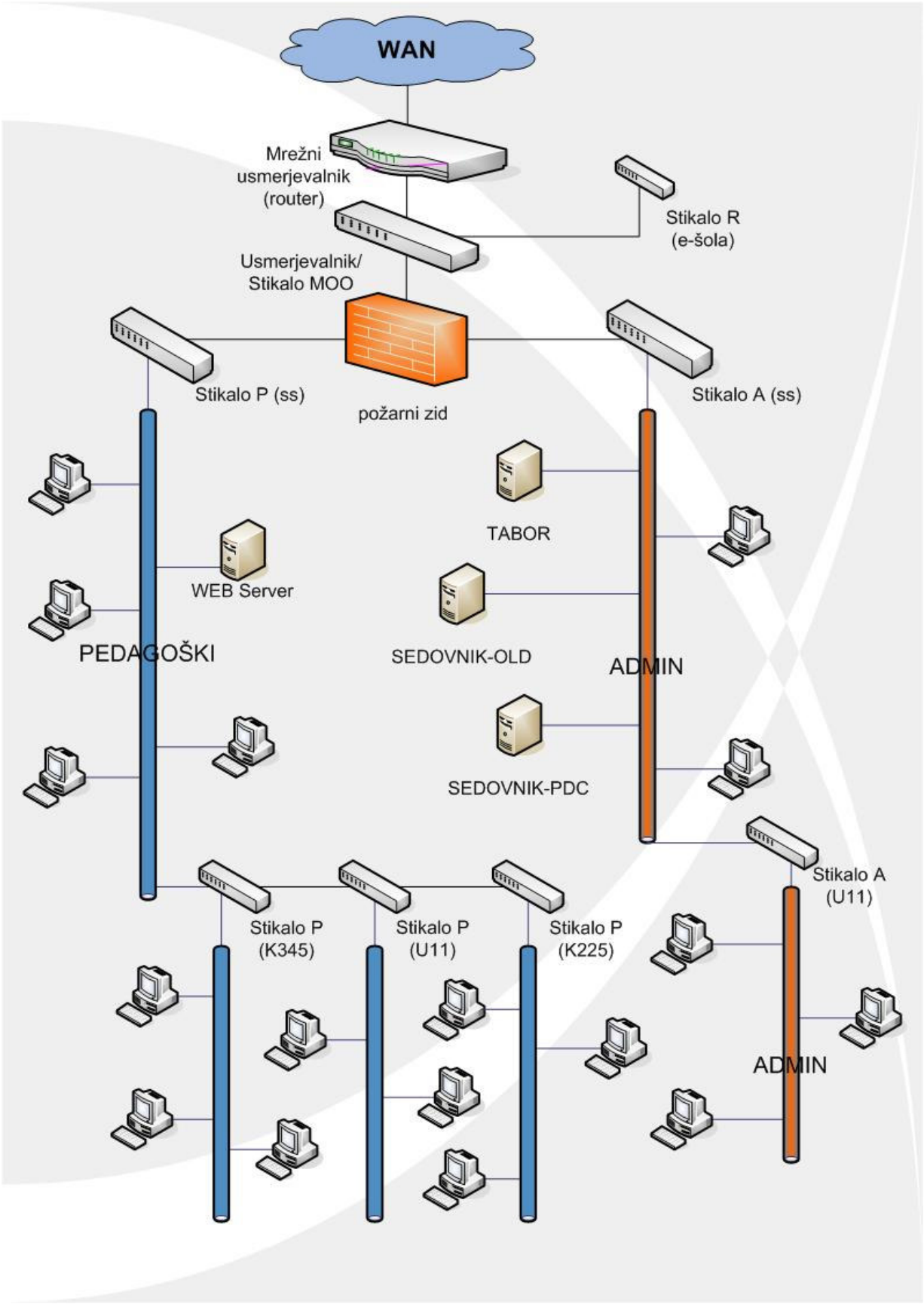
oddelka. Zmotno je tudi razmišljanje, da je za vzpostavitev varovanja informacij v organizaciji kar na dlani dovolj informacij, tako da ne potrebujemo dodatne analize tveganj. Analiza mora biti opravljena za obseg celotnega sistema varovanja in samo ta lahko pokaže vsa tveganja v obsegu in njihove primerjalne vrednosti, ki nam dajejo osnovo za določanje prioritet in ukrepov varovanja (Ključevšek, 2004).

Cilje varovanja z varnostno politiko mora postaviti vodstvo, ki tako postavi zahteve za varovanja. Informatiki jih potem izvedejo v okviru svojih pristojnosti in procesov, ki jih opravljajo. Druge dele varovanja izvedejo preostali zaposleni pri opravljanju procesov v organizaciji. Pomembne odločitve o varovanju informacij sprejemamo samo na podlagi analiz in ne na pamet, kot se v praksi še vse prepogosto dogaja.

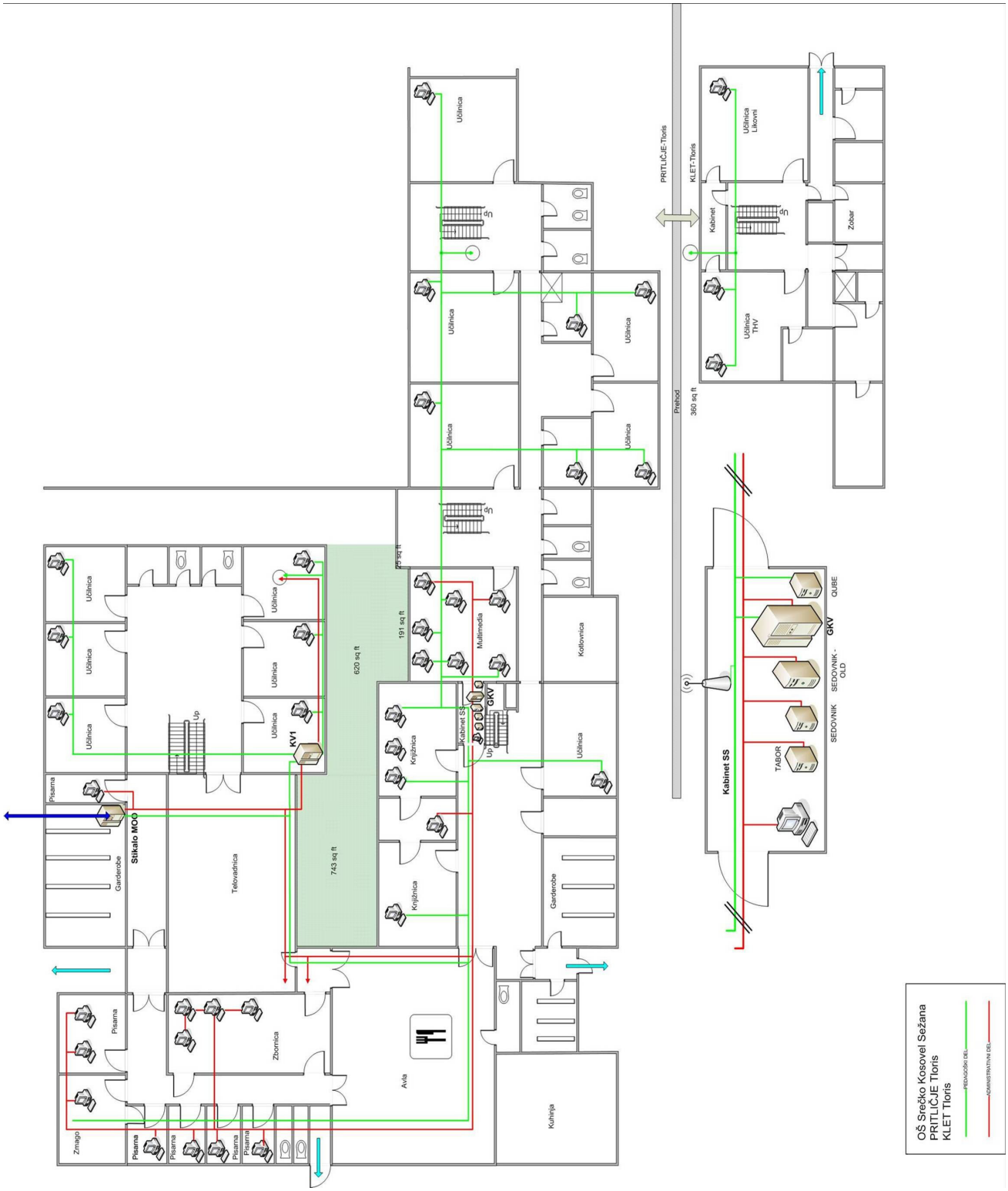
8. LITERATURA

- **British standard** (2002). BS ISO/IEC 17799:2000. Inštitut za informacijsko varnost.
- **Dogša, T.** (1997). Računalniško dokumentiranje in načrtovanje. Maribor: Univerza Maribor.
- **Hribar G**. (2003). Varni sporočilni sistem. Sistem, januar 2003, str. 22.
- Interno gradivo osnovne šole Srečka Kosovela Sežana.
- **Ključevšek R.** (2004). O varnosti. Sistem, junij 2004, str. 14.
- **Ogrinc, E**. (1991). Dokumentiranje v elektrotehniki, Ljubljana: FRI .
- **Powell, P**. (2002). Using Microsoft Visio 2002. Indiana: QUE.
- **RAID** (2005). What is Raid? Pridobljeno 10.07.2005 s svetovnega spleta: http://www.staff.uni-mainz.de/neuffer/scsi/what_is_raid.html.
- **Stubelj. T**. (2002). Standard za varnost. Sistem, september 2002, str. 18.
- **Štrakl M**. (2001). Varnost in varnostna politika. Sistem, marec 2001, str. 14.
- **Šiška A**. (2002). Varna omrežja. Sistem, november 2002, str. 20.
- **Zaščita za največje**. Moj mikro (2005), maj 2005, str. 60-65.
- **Žagar K**. (2002). Varnost pri e-poslovanju. Sistem, december 2002, str. 16.
- **Žumer V**. (2003). E-arhiviranje poslovnih dokumentov. Sistem, junij 2003, str. 14.

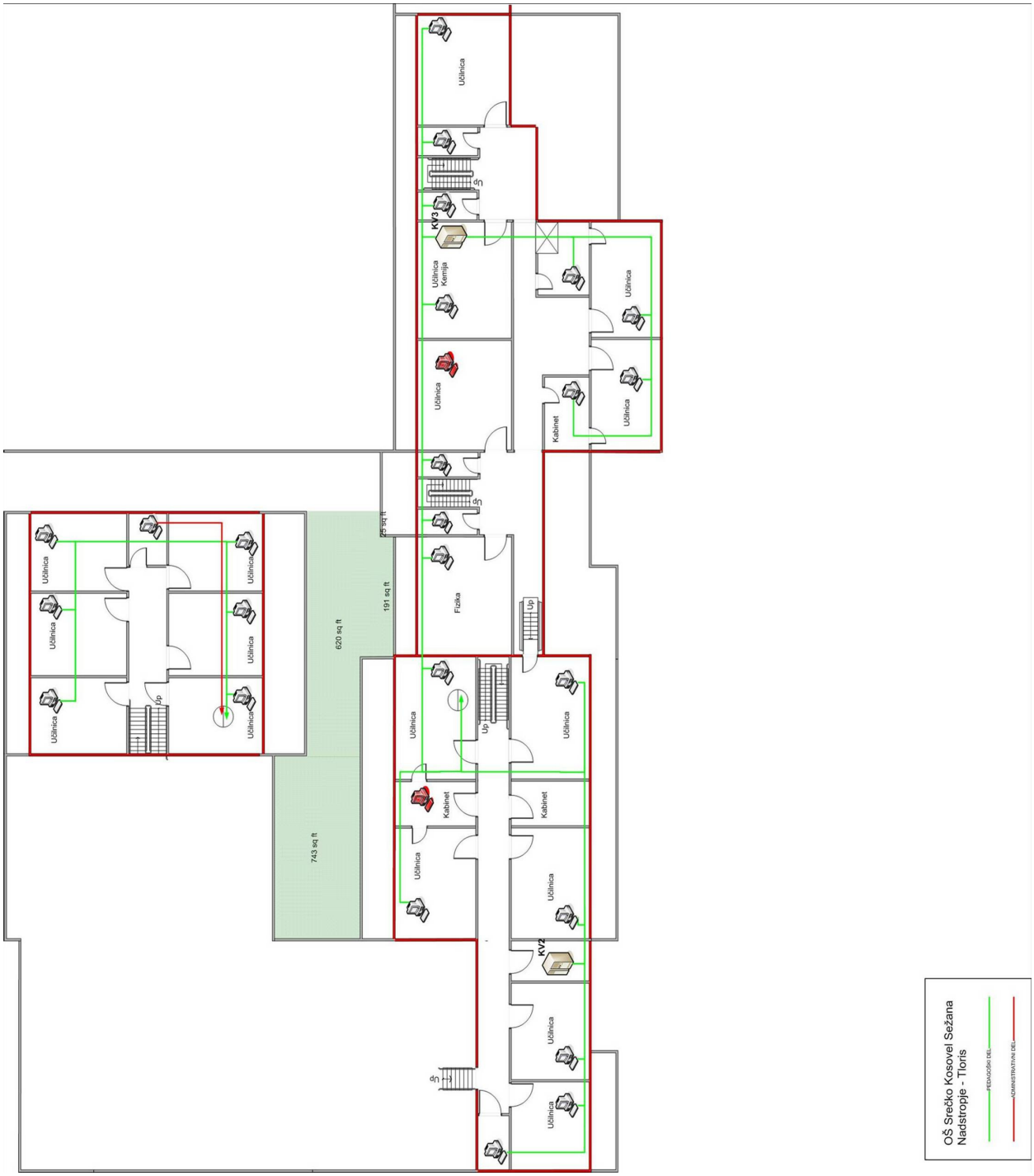
PRILOGA 1


WAN
Mrežni usmerjevalnik (router)
Stikalo R (e-šola)
Usmerjevalnik/ Stikalo MOO
Stikalo P (ss)
požarni zid
Stikalo A (ss)
TABOR
WEB Server
SEDOVNIK-OLD
PEDAGOŠKI
ADMIN
SEDOVNIK-PDC
Stikalo A (U11)
Stikalo P (K345)
Stikalo P (U11)
Stikalo P (K225)
ADMIN

PRILOGA 2


OŠ Srečko Kosovel Sežana
PRITLIČJE Tloris
KLET Tloris
PEDAGOŠKI DEL
ADMINISTRATIVNI DEL
PRITLIČJE-Tloris
KLET-Tloris
Učilnica
Učilnica Likovni
Učilnica THV
Kabinet
Zobar
Prehod
360 sq ft
Kabinet SS
GKV
QUBE
SEDOVNIK - OLD
SEDOVNIK
TABOR
Knjižnica
Multimedia
Kotlovnica
191 sq ft
620 sq ft
743 sq ft
79 sq ft
KV1
Stikalo MOO
Garderobe
Telovadnica
Pisarna
Zbornica
Avla
Kuhinja
Znago
Up

PRILOGA 2


Učilnica
Up
KV3
Učilnica Kemija
Učilnica
Učilnica
Kabinet
Učilnica
Up
191 sq ft
Fizika
620 sq ft
Up
Učilnica
Učilnica
Učilnica
Učilnica
Učilnica
Učilnica
Up
Učilnica
Učilnica
Kabinet
Kabinet
743 sq ft
Učilnica
Učilnica
KV2
Učilnica
Up
Učilnica
OŠ Srečko Kosovel Sežana
Nadstropje - Tloris
PEDAGOŠKI DEL
ADMINISTRATIVNI DEL

PRILOGA 3

EVIDENČNI KARTON ELEKTRONSKE NAPRAVE

Učitelj	Opis prostora	Št. prostora	Lokacija	Količina	
	Kabinet	347	Višja stopnja	1	

Opis naprave	DTK P566 128	**Oznaka**	PC-K347
Dobavitelj	MZF	**S/N**	58829
Datum namestitve	25. januar 2005	**Evidenčna**	
Tip naprave	DTK P566 128 MB 10 GB Ethernet		

STROJNA OPREMA

	Tip	Kapaciteta	Količina
Matična Plošča			
Procesor	Intel Celeron	566	1
Pomnilnik	SDRAM	128	1
HDD	IBM	10	1
Grafika	ATI Rage X1	32	1
Zvok	Integriran		1
Ethernet	3Com		1
Radix			

V/I KOMPONENTE

	Tip	Količina
Monitor	Philips 17"	1
Tipkovnica	DTK	1
Miška	DTK	1
Multimedia		
CD	Teac	1
CD-RW		
DVD		

OPERACIJSKI SISTEM in OSTALA SISTEMSKA PROGRAMSKA OPREMA

	Vrsta	Verzija	Service Pack	Update	Opombe
Operacijski sistem	WinXP	5,1	2	12.2.2005	
Ostala sistemska programska oprema orodja, baze, zaščita	AVG - antivirus Deep Freeze Spy-Bot S&D RegistryMech			12.2.2005 12.5.2005	

APLIKATIVNA PROGRAMSKA OPREMA:

Vrsta	Verzija	Service Pack	Update	Opombe
Office	2003			
Acrobat R	5.0			
Macromedia Play				
K-Lite Codec	3,5			
Mozilla				
Corel Draw	5			

SKRBNIK-UPORABNIK

Skrbnik naprave	Administrator
Uporabnik1	User
Uporabnik2	

Uporabnik3	

IP-RAČUNALNIKA	193.XXX.XXX.XXX
Prehod	193.XXX.XXX.XXX
Ime naprave	PC-K347
Domena	
Maska	2552.XXX.XXX.XXX
Delovna skupina	KABINET
Nahajališče	I-22

Hitri predogled VS

PRILOGA 4

SEZNAM ELEKTRONSKIH NAPRAV

Št. prostora	Opis prostora	Tip Naprave	Oznaka	Količina
K347	Kabinet	DTK P566 128 MB 10 GB Ethernet	PC-K347	1
U302	Učilnica	DTK P566 128 MB 10 GB Ethernet	PC-U302	1
K225	Kabinet	DTK P566 128 MB 10 GB Ethernet	PC-K225	1
K227	Kabinet	DTK P566 128 MB 10 GB Ethernet	PC-K227	1
U202	Učilnica	DTK P566 128 MB 10 GB Ethernet	PC-U202	1
U305	Učilnica	Liko PII-350Mhz 256Mb 4Gb	PC-U305	1
U304	Učilnica	DTK PC-1,7Mhz 256Mb 60Gb	PC-U304	1
K329	Kabinet	PC DFI P-333 256MB 3Gb	PC K329	1
U303	Učilnica	DTK LikoPII-350Mhz 256Mb 4 Gb	PC-U303	1
U308	Učilnica	DTK LikoPII-350Mhz 256Mb 4 Gb	PC-U308	1
U203	Učilnica	PC-C2,0Mhz 256Mb 40Gb	PC-U203	1
U204	Učilnica	PC-C2,0Mhz 256Mb 40Gb	PC-U204	1
U205	Učilnica	PC-C2,0Mhz 256Mb 40Gb	PC-U205	1
U312	Učilnica	DTK PC-1,7Mhz 256Mb 60Gb	PC-U312	1
U301	Učilnica	PC C-700 128MB 30GB DTK PC-1,7Mhz 256Mb 60Gb Laserski tiskalnik	PC-U301 PC-U301-2 T-U301	1 1

U206	Učilnica	PC Liko C-350 256MB 4GB	PC-U206	1
U309	Učilnica	PC Liko C-350 256MB 4GB	PC-U309	1
U207	Učilnica	0		0
K229	Kabinet	Liko DTK 02 PC P1,7 40Gb 256Mb	PC-K229	1

1

K348	Kabinet	PC PII-333 196Mb 5GB 3 Com	PC-K348	1
K349	Kabinet	PC PII-333 256Mb 5GB 3 Com	PC-K349	1
K345	Kabinet	DFI PII-333Mhz 256Mb 3Gb	PC-K345	1
U311	Učilnica	PC P350Mhz 256Mb 4Gb	PC-U311	1
U310	Učilnica	PC P350Mhz 256Mb 4Gb	PC-U310	1
K342	Kabinet	DFI P-333Mhz 256Mb 3Gb	PC-K342	1
U314	Učilnica	DTK PC-1,7Mhz 256Mb 60Gb	PC-U314	1
K350	Kabinet	DFI P-333 256Mb 3Gb	PC-K350	1
U307	Učilnica	Liko DTK 02 PC P1,7 40Gb 256Mb	PC-U307	1
U313	Učilnica	0	PC-U313	0
U201	Učilnica	Liko DTK 02 PC P1,7 40Gb 256Mb	PC-U201	1

U14	Učilnica	PC Liko 02 DTK P-850	PC-U14	1
U10	Učilnica	Liko DTK 02 PC P1,7 40Gb 256Mb	PC-U10	1
U11	Učilnica	PC Liko 02 DTK P-850	PC-U11	1
U9	Učilnica	PC Liko 02 DTK P-850	PC-U9	1
U12	Učilnica	Liko DTK 02 PC P1,7 40Gb 256Mb	PC-U12	1
U15	Zbornica NS	PC Liko 02 DTK P-850 Laserski tiskalnik	PC-ZNS T-ZNS	1

2

U13	Učilnica	PC Liko 02 DTK P-850	PC-U13	1
U16	Učilnica	PC Liko 02 DTK P-850	PC-U16	1
U17	Učilnica	Liko DTK 02 PC P1,7 40Gb 256Mb	PC-U17	1
U18	Učilnica	Liko DTK 02 PC P1,7 40Gb 256Mb	PC-U18	1
U3	Učilnica	Liko DTK 02 PC P1,7 40Gb 256Mb	PC-U3	1
U4	Učilnica	Liko DTK 02 PC P1,7 40Gb 256Mb	PC-U4	1
U5	Učilnica	PC DTK PII-266Mhz 196Mb 5Gb	PC-U5	1

P10	Pisarna	PC Dell 2,4Ghz 512Mb 80GB Laserski barvni tiskalnik	PC-Zmago T-P10	1
P9	Pisarna	PC Dell 2,4Ghz 512Mb 80GB Laserski barvni tiskalnik	PC-P9 T-P9	1
P8	Pisarna	PC Dell 2,4Ghz 512Mb 80GB Laserski barvni tiskalnik	PC-P8 T-P8	1
P7	Pisarna	PC Dell 2,4Ghz 512Mb 80GB Laserski barvni tiskalnik	PC-P7 T-P7	1
P6	Pisarna	PC Dell 2,4Ghz 512Mb 80GB Barvni tiskalnik	PC-P6 T-P6	1
P11	Pisarna	PC Dell 2,4Ghz 512Mb 80GB Barvni tiskalnik	PC-P11 T-P11	1
14	Zbornica	PC Dell 2,4Ghz 512Mb 80GB PC Dell 2,4Ghz 512Mb 80GB PC Dell 2,4Ghz 512Mb 80GB PC Dell 2,4Ghz 512Mb 80GB Barvni Laserski Tiskalnik Namizni Skener	PC-Zbornica-A PC-Zbornica-B PC-Zbornica-C PC-Zbornica-D T-14 S-14	1 1 1 1

				3
306	**MULTIMEDIA**	Oria PC P2,8Ghz 512Mb 60Gb Oria PC P2,8Ghz 512Mb 60Gb Oria PC P2,8Ghz 512Mb 60Gb Oria PC P2,8Ghz 512Mb 60Gb Oria PC P2,8Ghz 512Mb 60Gb Oria PC P2,8Ghz 512Mb 60Gb Oria PC P2,8Ghz 512Mb 60Gb Oria PC P2,8Ghz 512Mb 60Gb PC Dell P-2,45Mhz 512 Mb PC Dell P-2,45Mhz 512 Mb PC Dell P-2,45Mhz 512 Mb PC Dell P-2,45Mhz 512 Mb PC Dell P-2,45Mhz 512 Mb PC Dell P-2,45Mhz 512 Mb Liko PC P2,0Mhz 512Mb 40Gb PC Oria P-2,0 256Mb 40 Gb	PC-Pouk1 PC-Pouk2 PC-Pouk3 PC-Pouk4 PC-Pouk5 PC-Pouk6 PC-Pouk7 PC-Pouk8 PC-Pouk9 PC-Pouk10 PC-Pouk11 PC-Pouk12 PC-Pouk13 PC-Pouk14 PC-Demo PC-Oria	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

		Barvni Laserski Tiskalnik Matrični tiskalnik A3 Secom PC-PIII-800Mhz 384Mb Video Projektor Video Projektor	T-U306 T-U306-2 PC-Server P-U306 P-U306-2	1
	DVORANA	PC PII-333 256Mb 5GB 3 Com	PC-Hala	1
41	**KNJIŽNICA**	PC DTK PII-350Mhz 256Mb 4Gb Liko DTK 02 PC P1,7 40Gb 256Mb PC PII-350Mhz 256Mb 4Gb PC Secom-Sklad PC Oria Wearnes 500 Laserski tiskalnik Matrični tiskalnik	PC-Knj1 PC-Knj2 PC-Knj3 PC-Knj4 PC-Knj5 T-Knj T-Knj2	1 1 1 1 1 1 1
K222	**SS**	Taborniška Lokev Prenosni	PC-Tabor PC-Sedovnik PC-Sedovnik Old PC-Dalibor PC-Qube	1 1 1 1 1
			Skupaj	**88**