Univerza v Mariboru

Fakulteta za organizacijske vede

Magistrsko delo

Organizacija in management informacijskih sistemov

CELOVITI PRISTOP PRI ZAGOTAVLJANJU INFORMACIJSKE VARNOSTI V OSNOVNI ŠOLI

Mentor: doc. dr. Alenka Brezavšček

Kandidat: Samo Štraser

Kranj, september 2012

ZAHVALA

Pri izdelavi magistrske naloge se iskreno zahvaljujem mentorici doc. dr. Alenki Brezavšček, ki mi je bila s svojo potrpežljivostjo, strokovnostjo in pravilnimi usmeritvami v veliko pomoč pri izdelavi magistrske naloge.

Za pomoč in podporo pri izdelavi magistrske naloge se najlepše zahvaljujem šolskemu kolektivu Osnovne šole Neznanih talcev Dravograd, še posebej pa ravnatelju g. Marjanu Kovšetu, bivšemu pomočniku ravnatelja g. Ludviku Moriju in lektorici ge. Ireni Kašman.

Zahvaljujem se podjetju EXTIS GmbH, ki mi je omogočilo uporabo Open School Serverja.

Posebna zahvala gre moji družini - staršem, Špeli in sinu Niku ter prijateljem, ki so mi ves čas stali ob strani in me vzpodbujali.

POVZETEK

Informacijska varnost je zelo zahtevno in težko obvladljivo področje. Pri zagotavljanju informacijske varnosti moramo predvideti vse morebitne nevarnosti, saj je informacijski sistem varen toliko, kot je varen njegov najšibkejši člen. Najbolj tipična področja, ki jih moramo pri zagotavljanju informacijske varnosti upoštevati so: sistemska varnost, varnost podatkov, omrežna varnost, fizična varnost, organizacijska varnost.

Zagotavljanje informacijske varnosti v osnovni šoli se zdi na prvi pogled zelo enostavno opravilo, vendar temu nikakor ni tako. Rezultati raziskave, ki smo jo izvedli med slovenskimi osnovnimi šolami, kažejo, da za informacijsko varnost v osnovnih šolah po Sloveniji ni najbolje poskrbljeno. Informacijska varnost je namreč individualna skrb vsake posamezne šole, zato ne moremo govoriti o nekih skupnih in celovitih rešitvah, kot jih npr. uporabljajo ponekod v tujini. V Sloveniji sicer deluje nekaj državnih institucij, ki osnovnim šolam pomagajo pri zagotavljanju informacijske varnosti, vendar bo potrebno na tem področju še marsikaj izboljšati.

V prispevku smo predstavili stanje na področju zagotavljanja informacijske varnosti v slovenskem šolstvu. Predstavili smo tudi nekatere dobre prakse, ki se jih poslužujejo v tujini. V skladu s temi smo oblikovali splošne smernice za izboljšanje informacijske varnosti, ki smo jih uporabili pri prenovi informacijskega sistema na OŠ Neznanih talcev Dravograd. Menimo, da je opisani pristop uporaben tudi za ostale osnovne šole v Sloveniji. Ker ne zahteva velikih finančnih vložkov, ima s tega stališča veliko praktično vrednost.

KLJUČNE BESEDE:

- informacijska varnost
- smernice
- osnovna šola
- odprtokodna programska oprema
- Open School Server

ABSTRACT

The field of IT security is very demanding and difficult to manage. In providing IT security we need to foresee all possible risks, since an information system is only as safe as its weakest link. The most typical fields we must consider in providing IT security are: system security, data security, network security, physical security, organization security.
Although at a first sight providing IT security in an elementary school seems a very simple task, this is not the case. The results of the research we conducted among Slovenian elementary schools have shown that their IT security is not entirely taken care of. IT security is something each school has to take care of itself, so we cannot speak about common and overall solutions, which for example are used in some places abroad. In Slovenia there are some state institutions which help elementary schools with providing IT security, however several improvements are still needed in this field.
In our contribution we have presented the situation in the field of providing IT security in Slovenian schools. We have also presented some good practices used abroad. In accordance with these good practices we have developed general guidelines for improving IT security, which we used to reform the information system at the elementary school Osnovna šola Neznanih talcev Dravograd. We believe the described approach is also useful for other elementary schools in Slovenia. Since it does not require large financial contributions, it has in this context a great practical value.

KEY WORDS:

- IT security
- guidelines
- elementary school
- open source software
- Open School Server

KAZALO

1 UVOD

1.1 Predstavitev problema

Uporaba informacijsko - komunikacijske tehnologije (v nadaljevanju IKT) na področju šolstva je danes praktično neizbežna. Ta tehnologija odpira številne nove možnosti in priložnosti za poučevanje in izobraževanje. Na drugi strani pa ima njena uporaba tudi slabosti, izmed katerih izstopajo številne nevarnosti njene uporabe.

Kljub znanemu problemu informacijski varnosti namenjamo vse premalo pozornosti. Šole po Sloveniji so pri zagotavljanju informacijske varnosti prepuščene lastnimi interesom, zato je temu primerno urejeno tudi to področje. Vsaka šola zagotavlja informacijsko varnost po svoje, zato ni sprejete oz. niti ne predlagane enotne rešitve. Zato veliko šol tega problema niti ne more obvladovati, bodisi zaradi pomanjkanja znanja, časa ali sredstev.

K izboljšanju informacijske varnosti v osnovnih šolah bi lahko veliko pripomogla tudi sama država. Prvi problem nastaja zaradi slabe sistemizacije delovnega mesta skrbnika IKT. Delež njegove zaposlitve je odvisen od števila oddelkov, zato je na nekaterih osnovnih šolah njegova prisotnost minimalna. Ponekod pa to delo opravljajo kar drugi učitelji.

Poleg boljše sistemizacije bi nujno potrebovali tudi državno institucijo, ki bi skrbela pa pomoč in podporo na tem področju. Po Sloveniji sicer deluje nekaj institucij, ki pa največ pozornosti namenjajo varni uporabi interneta. Nedvomno gre za pomembno področje, toda šole bi potrebovale konkretne rešitve ter z njimi povezana izobraževanja.

Država se v zadnjem času sicer trudi, da bi v okviru projekta E-šolstvo šolam zagotovila pomoč in podporo na področju IKT, vendar je področje zagotavljanja informacijske varnosti trenutno zelo slabo podprto.

Svetla izjema, ki se dejansko trudi skrbeti za informacijsko oz. natančneje omrežno varnost v osnovnih šolah po Sloveniji, je Arnes. Arnes s svojo že preizkušeno infrastrukturo šolam zagotavlja dokaj varno povezavo do interneta ter obenem skrbi za varnost omrežja znotraj šole. Poleg tega njihovi strokovnjaki nudijo tudi pomoč in podporo na tem področju.

Zdi se, da bodo morale šole same največ postoriti na tem področju. Najprej je potrebno oblikovati in sprejeti varnostno politiko, saj največji problem pogosto predstavljajo slabo ozaveščeni uporabniki. Pri iskanju rešitve ne smemo pozabiti, da je šola specifična organizacija. Njeni uporabniki namreč pogosto nastopajo z različnimi interesi in nimajo pretirano širokega tehnološkega znanja. Zato mora biti rešitev enostavna za implementacijo in uporabo, ampak še vedno dovolj učinkovita pri zagotavljanju informacijske varnosti.

1.2 Cilji in namen naloge

Povod za raziskavo je zaznana premajhna skrb za informacijsko varnost na osnovnih šolah po državi. S pomočjo izkušenj in raziskav smo prišli do ugotovitve, da je za varnost na osnovnih šolah v Sloveniji bolj slabo poskrbljeno. Informacijska varnost je problem, ki se ga mora zavedati celotna organizacija in ne samo skrbnik IKT, kot je to na številnih šolah po Sloveniji navada. Delo skrbnika IKT velikokrat opravljajo kar učitelji, ki običajno niti nimajo ustreznega znanja oz. izkušenj v zvezi z zagotavljanjem informacijske varnosti ali pa se problema informacijske varnosti niti ne zavedajo.

Opravičila za neurejeno informacijsko varnost so danes brez pomena. Vsaka šola se mora problematike zavedati in ustrezno ukrepati.

Pogosto so težave povezane s pomanjkanjem finančnih sredstev, kljub temu pa lahko s pravo voljo in z zanimanjem poskrbimo za primerno informacijsko varnost tudi z minimalnimi sredstvi.

Izgovori v zvezi s pomanjkanjem znanja so prav tako odveč. Sodobna informacijska tehnologija nam ponuja odgovore na vsa vprašanja.

Edini možen sprejemljiv odgovor bi lahko bil pomanjkanje časa. Delovno mesto skrbnika IKT je namreč zelo slabo sistematizirano, zato je potrebno marsikaj postoriti tudi izven delovnega časa.

V nalogi bomo najprej preučili teoretične osnove za zagotavljanje informacijske varnosti.

Nato bomo preučili in primerjali stanje informacijske varnosti v osnovnih šolah doma in po svetu.

S pomočjo raziskave, ki jo bomo izvedli med skrbniki informacijskih sistemov v slovenskih osnovnih šolah, bomo oblikovali smernice za izboljšanje informacijske varnosti. Usmeritve za oblikovanje smernic za izboljšanje informacijske varnosti s strani uporabnikov bomo pridobili s pomočjo raziskave, ki jo bomo izvedli med učitelji in učenci.

Za konec bomo v skladu s predlaganimi smernicami prenovili informacijski sistem v osnovni šoli Neznanih talcev Dravograd.

Izsledki raziskave bodo dober povod za razumevanje informacijske varnosti, hkrati pa bo pristop pri zagotavljanju informacijske varnosti v osnovnih šolah lahko dobra popotnica tudi za ostale šole.

1.3 Predpostavke in omejitve

Zagotavljanje informacijske varnosti je zelo široko področje. V nalogi se bomo omejili zgolj na področja in rešitve, ki so blizu organizacijam, kot so osnovne in srednje šole ter druge javne ustanove.

Pri analizi obstoječega stanja v osnovnih šolah po Sloveniji se bomo opirali na rezultate, pridobljene iz raziskave ter na lastno znanje, poznavanje in izkušnje.

V raziskavo bomo skušali vključiti osnovne šole po celotni Sloveniji. Zavedamo se, da vseh šol v raziskavo ne bomo mogli zajeti, zato lahko pride do nekaterih odstopanj. Kljub vsemu upamo, da bodo rezultati raziskave dober približek realnega stanja glede informacijske varnosti v osnovnih šolah po Sloveniji.

Uvajanje predlaganih smernic v prakso bomo prikazali le na primeru osnovne šole Neznanih talcev Dravograd. Predpostavljamo, da bo pristop z nekaterimi spremembami odgovarjal tudi ostalim osnovnim in srednjim šolam ter nekaterim drugim organizacijam.

1.4 Metode dela

Pri raziskavi bomo uporabili več različnih raziskovalnih metod. Pri opisovanju teoretičnih osnov bomo uporabili predvsem deskriptivno metodo. Uporabili bomo domačo in tujo literaturo ter prispevke, objavljene na internetu.

Preizkusili, opisali in primerjali bomo nekaj praktičnih rešitev, ki se uporabljajo za zagotavljanje informacijske varnosti v osnovnih šolah po svetu.

V empiričnem delu bomo raziskali, kakšno je stanje informacijske varnosti v osnovnih šolah po Sloveniji. V raziskavo bomo vključili uporabnike in skrbnike šolskega informacijskega sistema.

Raziskali bomo, katere državne iniciative delujejo na tem področju ter na kakšne načine se trudijo izboljšati informacijsko varnost v osnovnih šolah.

Na podlagi splošnih ugotovitev in analize trenutnega stanja, pridobljenega s pomočjo raziskave, bomo oblikovali smernice za zagotavljanje informacijske varnosti v osnovnih šolah.

Nato pa bomo v skladu s predlaganimi smernicami prenovili informacijski sistem v osnovni šoli Neznanih talcev Dravograd.

2 OSNOVE INFORMACIJSKE VARNOSTI

2.1 Pomen informacijske varnosti

Področje zagotavljanja informacijske varnosti je postalo z naglim razvojem IKT zelo pomembno. Za zagotavljanje informacijske varnosti so potrebni številni varnostni ukrepi, ki se morajo izvajati tam, kjer IKT uporabljamo, kar pomeni skoraj povsod.

Kljub ukrepom, ki jih izvajamo v praksi, se pogosto pokaže, da še nismo povsem dojeli pravega pomena informacijske varnosti, saj ta tematika pogosto naleti na gluha ušesa. Pogosto za načrti manjkajo ustrezna dejanja ali pa le-ta niso ustrezna.

Rezultati raziskave vodilne analitske družbe IDC (International Data Corporation) kažejo, da je področje varnosti po pomenu preraslo domala vsa druga področja, toda največji problem se kaže v dojemanju varnosti. Vse preveč ljudi naivno verjame, da je mogoče varnost preprosto kupiti v obliki izdelka, ki ga namestimo, malo preizkusimo in se tako zaščitimo pred vsemi nevarnostmi. Najbolj očiten plod takega razmišljanja so varnostne naprave (angl. security appliances), ki vsaj v reklamah obljubljajo odstranitev vseh nevšečnosti, ne da bi morali na odjemalce namestiti dodatno programsko opremo in s tem potencialno porabiti kar nekaj časa. So kot nekakšno "univerzalno zdravilo", ki brez truda odpravi vse tegobe tega časa, pa naj gre za viruse, nezaželeno pošto, vohunske programe, poskuse vdora in še kaj (Djurdič, 2004).

Varnostne naprave in druga sodobna programska oprema so dobrodošla orodja, ki pa lahko pogosto pustijo napačen vtis. Občutek dajejo, da je s tem vse rešeno in se lahko posvetimo drugim stvarem, medtem ko se varnostni mehanizmi samodejno posodabljajo in skrbijo za "varnost". Ta občutek je pogosto celo bolj usoden, kot če bi imeli računalniški sistem povsem nezaščiten. Varnost seveda niso samo orodja, temveč tudi postopki in pravila, ki so zgrajena, usklajena na ravni celotnega podjetja in kar se da dosledno uporabljena v praksi. Zmotno je tudi pogosto razmišljanje, da je varnost računalniških sistemov zgolj naloga službe za informacijsko tehnologijo. Varnost informacij v najširšem pomenu besede je namreč stvar vsakega zaposlenega, celo tistih, ki morda sploh ne uporabljajo računalnikov. Lep zgled za ponazoritev tega so nevarnosti, ki pravzaprav prihajajo iz samega podjetja, ne pa nekje od zunaj, z interneta. Kaj nam pomaga, če imamo še tako sodobne računalniške varnostne mehanizme, ko pa nam lahko nekdo mimo vratarja brez težav odnese cel fascikel papirja. Ali pa prenosni disk velikosti MP3 predvajalnika, na katerem je dovolj prostora, da lahko naredimo domala celotno kopijo poslovnega informacijskega sistema. Statistike kažejo, da večina zlorab računalniških sistemov pravzaprav prihaja iz samega podjetja ali pa so bile opravljene s pomočjo informacij, ki so prišle od "znotraj" (Djurdič, 2004).

2.2 Varnost informacijskega sistema

Pojem informacijska varnost ali varnost informacijskega sistema lahko definiramo kot sposobnost informacijskega sistema, da pri določenih pogojih zadovoljivo opravlja zahtevane funkcije brez neželenih dogodkov, ki bi lahko negativno vplivali na razpoložljivost, celovitost ali zaupnost njegovih dobrin (Brezavšček, 2007).

Osnovne komponente zagotavljanja informacijske varnosti so torej zagotavljanje

- razpoložljivosti,
- celovitosti.
- zaupnosti.

Zagotavljanje razpoložljivosti pomeni prizadevanje, da so vse dobrine informacijskega sistema v stanju zadovoljivega delovanja in na voljo uporabnikom vedno, ko jih ti potrebujejo. Zagotavljanje celovitosti pomeni varovanje dobrin informacijskega sistema pred nepooblaščenimi spremembami ali uničenjem, zagotavljanje zaupnosti pa pomeni zaščito občutljivih informacij pred nepooblaščenim razkritjem ali protipravnim prestrezanjem.

Neželene dogodke ali dejavnosti, ki lahko negativno vplivajo na komponente informacijske varnosti, imenujemo grožnje varnosti.

Informacijski sistem je varen toliko, kolikor je varen njegov najšibkejši člen.

Informacijska varnost ne pomeni le zagotavljanje sistemske varnost, varnost omrežja, varnost podatkov idr., ampak tudi zavedanje in skrb uporabnikov na tem področju (Kizza, 2009).

Iz navedenih definicij o varnosti informacijskega sistema lahko sklepamo, da je za zagotavljanje varnosti informacijskega sistema potrebno nenehno zagotavljati razpoložljivost vseh komponent sistema. Pri tem zahteva posebno pozornost skrb za varovanje podatkov, ki morajo biti na voljo vedno, v pravi obliki in biti morajo konsistentni. Za določene podatke moramo zagotavljati večletno obstojnost, druge spet po pretečenem času nadzorovano uničiti. Ob vsem tem pa moramo biti pazljivi še na namerne ali nenamerne dogodke, ki ne smejo poškodovati ali kako drugače vplivati na te podatke.

Da bi dosegli vse to, je potrebno vpeljati dovolj visoko stopnjo kakovosti strojne in programske opreme ter v podjetju vzpostaviti primerno kulturo varnosti. Podjetja morajo biti pripravljena na dejstvo, da je za zagotovitev primerne strojne in programske opreme z redundanco potrebno zagotoviti finančna sredstva. Samo tako je možno vzpostaviti dovolj varno delovno okolje, ki zagotavlja neprekinjeno poslovanje in ustrezno ščiti komponente sistema pred različnimi grožnjami. Za namen dviga kulture varnosti zaposlenih vzpostavljajo podjetja varnostne portale, na katerih informirajo svoje delavce o vseh vidikih varnosti. Nenehno opozarjanje na različne grožnje varnosti bo pripomoglo k temu, da bo zavest o potrebni varnosti zlezla zaposlenim pod kožo in postala del njihovega vsakdanjega delovnega procesa. Vsebina takšnih portalov se ne nanaša samo na varnost informacijskega sistema, temveč podpira vzpostavitev in

ohranjanje določenega nivoja varnosti na različnih področjih poslovanja in tudi na splošno (Klančnik, 2007).

2.3 Grožnje informacijske varnosti

Grožnja je neželen dogodek ali dejavnost, ki privede do izgube celovitosti, zaupnosti ali razpoložljivosti informacij in onemogoča zadovoljivo delovanje informacijskega sistema.

Grožnje lahko delimo glede na:
- izvor grožnje,
- naravo dobrine, na katero grožnja deluje,
- učinek grožnje na informacijski sistem in njegove dobrine.

Glede na izvor grožnje ločimo naslednje skupine:
- človeški dejavniki,
- izredni dogodki,
- naključni dogodki.

Glede na naravo dobrine, na katero grožnja deluje, ločimo:
- fizične grožnje: delujejo neposredno na otipljive in posredno na neotipljive dobrine,
- logične grožnje: delujejo na neotipljive dobrine informacijskega sistema.

Glede na učinek grožnje na informacijski sistem in njegove dobrine ločimo:
- aktivne grožnje: kadar se le-ta realizira, poškoduje ali celo uniči dobrino informacijskega sistema (npr. nepooblaščena sprememba podatkov),
- pasivne grožnje: kadar se le-ta realizira, povzroči določeno škodo, vendar dobrine informacijskega sistema ne spremeni (npr. nepooblaščeno razkritje oziroma kraja zaupnih podatkov).

V nadaljevanju si bomo najbolj pogoste grožnje podrobneje ogledali.

2.3.1 Škodljiva programska oprema

Škodljiva programska oprema obsega viruse, črve, trojanske konje, vohunske in druge škodljive programe.

Namen piscev takšnih programov je povzročanje škode, izgube podatkov, vohunjenje. Uporabniki porabijo veliko časa za odstranitev takšnih programov in ponovno vzpostavitev normalnega delovanja (Klančnik, 2007).

Najlažji način okužbe so napake v operacijskih sistemih pa tudi v aplikacijah. Za okužbe so zanimivi tudi vsi servisi, še posebej, kadar tečejo s pravicami sistema ali (lokalnega/domenskega) administratorja.

Pogosto se sprašujemo o varnosti operacijskega sistema in pri tem prepogosto pozabljamo na varnost ostale programske opreme, ki jo na računalnik namestimo, vključno z npr. gonilniki za tiskalnik, ki se namestijo kot del jedra. V primeru, da operacijski sistem v določenem okolju ni ranljiv, pa morda lahko

uporabimo kakšno ranljivost v aplikacijah, ki so v nekem okolju nameščene. Znano je, da je kar nekaj proizvajalcev programske in strojne opreme na tržišče poslalo produkte, ki so bili okuženi z virusi (Pihler, 2007).

V zadnjih nekaj letih se je število velikih izbruhov virusov precej zmanjšalo. Razlogov za to je več. V tem času se je močno povečala varnostna osveščenost že pri samem razvoju operacijskih sistemov. Ne smemo pa pozabiti tudi na končne uporabnike, ki so se navadili rednega nameščanja popravkov ter uporabe varnostih mehanizmov, kot so požarne pregrade ter protivirusna zaščita. Omeniti moramo tudi druge razloge. Vedno več napadov na omrežja je naročenih in pri napadih, kjer je cilj kraja podatkov, so svojo novo vlogo našli avtorji virusov, ki so se prelevili v avtorje rootkitov, ob tem pa, ne le da povzročajo kaos na internetu, celo zaslužijo (Pihler, 2007).

Računalniški virus

Računalniški virus je program, ki se lahko „samodejno“ prekopira na druge sisteme. Samodejno pomeni brez privoljenja oz. brez vednosti uporabnika računalnika. Prvi virusi so se širili s pomočjo izmenljivih medijev. S pojavom interneta so virusi postali bolj gibljivi. Virus je lahko na izmenljivem mediju oz. na računalniku shranjen na več načinov:

- v boot sektorju medija oz. v MBR na disku tako, da se požene vsakič, ko
- priklopimo medij oz. ko prižgemo računalnik;
- kot podaljšek izvršilnega programa tako, da se izvede vedno, ko izvedemo okuženi program;
- kot skripta, ki se izvede, ko uporabnik uporabi določen ukaz iz lupine;
- kot makro v dokumentih, ki podpirajo makroje in se izvede vedno, ko odpremo okužen dokument;
- kot skripta na strežniku, ki se izvede vedno, ko z brskalnikom brskamo po straneh na okuženem strežniku.

Računalniški virusi so tem bolj nevarni, čim bolj dolgo ostanejo skriti. Virus, ki takoj ko poženete okuženi računalnik, zbriše ves sistem, v splošnem ni preveč nevaren, saj se ne uspe dovolj razširiti. Po drugi strani pa virus, ki se npr. do določenega datuma samo širi in šele nato začne delati škodo, predstavlja dosti večjo nevarnost. Znano je, da je operacijski sistem Microsoft Windows bolj občutljiv na viruse kot sistem Linux. Res pa je tudi, da so skoraj vsi najbolj znani virusi pisani za okolje Windows. Na sistemu Linux poznamo manj virusov, kar je posledica tega, da je Linux manj razširjen in uporabljen kot Microsoft Windows. Linux je predvsem v domeni tehnično bolj podkovanih in varnostno bolj osveščenih uporabnikov. Ravno zaradi tega platforma Linux ni plodna za širjenje virusov. Velik pomen ima pri širjenju virusov človeška površnost, neizkušenost in neizobraženost oz. neosveščenost. Konec koncev večina ljudi uporablja računalnik le kot orodje, s katerim opravljajo določeno opravilo. In če jim tehnika pomeni le sredstvo, s katerim dosegajo svoje cilje, se po večini niso sposobni ali ne želijo spuščati v podrobnosti, kar bi na koncu grenilo življenje virusom. Linux uporablja tudi čedalje več navadnih uporabnikov računalnikov, zato je pričakovati porast virusov tudi za Linux. Nič kaj težko ni imeti slabo vzdrževan sistem Linux. Tak sistem je lahko idealen gostitelj virusov, kjer se razmnožujejo in iz katerega se širijo (Meolic, 2009).

Večina današnjih virusov izkorišča katero od varnostnih lukenj v določeni programski opremi (ne nujno v operacijskem sistemu). Dober administrator redno spremlja dogajanje na varnostnem področju in takoj nadgradi progam, v katerem je bila odkrita in odpravljena varnostna luknja. Vendar od navadnih uporabnikov ne moremo pričakovati, da se bodo obnašali kot dobri administratorji. Povečini nimajo niti časa niti znanja, da bi to počeli. Tak uporabnik ima lahko tudi na sistemu GNU/Linux precej dolgo časa nameščen program, ki omogoča preživetje in širjenje določenemu ali celo več virusom. V začetku osemdesetih let prejšnjega tisočletja so se pojavljale prve teorije o računalniških virusih. Celo ob prvih delujočih konceptualnih virusih je večina ljudi zamahnila z roko, češ te zadevščine so čista znanstvena fantastika, ki nima veze z realnostjo. Danes številni virusi za operacijski sistem Windows in nekateri za Linux potrjujejo, da tudi ta operacijski sistem ni sam po sebi nanje imun. Zato se je bolje zaščititi preden nam kak virus prekriža načrte (Šuc, 2002).

Črv

Računalniški črv je program, ki se širi po omrežju in ne okuži datotek, lahko pa jih zbriše oz. pokvari. Črv torej vsebuje dva mehanizma:

- zna se prekopirati na drugi računalnik,
- na ciljnem računalniku se zna samodejno pognati oz. preslepiti uporabnika da ga požene.

Predvsem drugi cilj je dokaj težko doseči. Običajno se izrabijo napake v strežniških programih, ki tečejo na računalniku. Še bolj uspešen način za širjenje črvov pa je v obliki priponke k elektronski pošti. Priponka ima zanimivo ime (npr. I love you) in zato jo uporabnik odpre, s tem pa požene črva. Ker se računalniški črv ne shrani na ciljnem računalniku v splošnem, ob okužbi pomaga, da računalnik enostavno ugasnemo in potem spet prižgemo. Problem pa je v tem, da se lahko računalnik takoj po vklopu in povezavi v internet spet takoj okuži.

Trojanski konj

Trojanski konj je podoben računalniškemu črvu, le da se ne zna sam prekopirati na drug računalnik. Prenašajo ga uporabniki sami, ker jih z imenom zavede in mislijo, da so prenesli nekaj drugega.

Posebna oblika trojanskega konja je potegavščina (angl. hoax). Gre za nevarna oblika napada na računalnike v obliki lažnega sporočila o računalniškem virusu, ki ga dobimo preko elektronske pošte. Ker je sporočilo napisano zelo čustveno, ga uporabniki množično razpošiljajo naprej, lahko pa po navodilih v sporočilu celo sami poškodujejo svoj računalnik. Leta 2000 je bilo npr. razširjeno sporočilo, ki je eno od sistemskih datotek na sistemu MS Windows (sulfnbk.exe) opisovalo kot nevarni virus, ki ga naj uporabniki čim prej zbrišejo.

Vohunski programi

Vohunski programi (angl. spyware) so danes pogosta oblika škodljivih programov, ki so napisani z namenom zaslužka. Ko se poženejo na ciljnem gostitelju, začnejo zbirati podatke o uporabnikovem obnašanju in ga prepričevati, da obišče

določene internetne strani oz. kupi določene izdelke. To naredijo tako, da mu prikazujejo reklamna sporočila ali pa spremenijo obnašanje brskalnika tako, da se pri iskanju na spletu na začetku pojavijo povezave do določenih strani. Še bolj nevarni so key loggerji, ki sledijo tipkanju uporabnika in zbirajo gesla ter npr. številke bančnih kartic.

»Rootkit«

Rootkit je posebna oblika škodljivih programov, ki se vgradijo v operacijski sistem in tako v celoti prevzamejo nadzor nad računalnikom.
Primarna naloga rootkitov ni uničevalne narave ali neposredno povzročanje kaosa. Naloga rootkitov je nepridipravom omogočiti kar se da dolgo neopazen dostop in nadzor nad sistemi, kamor jim je uspelo rootkit namestiti.
Rootkiti so si zelo različni in obstajajo za vse sisteme. Lahko počnejo karkoli, na primer:

- na računalniku odprejo stranska vrata,
- onemogočijo dostop do določene strojne opreme, npr. DVD enote,
- skrijejo posamezne datoteke in cele imenike, tako da jih uporabnik ne vidi.

V praksi rootkit programi niso omejeni na eno od naštetih funkcij, ampak počnejo vse in še kaj drugega. Še posebej je nevarna funkcija skrivanja datotek, saj lahko skrijejo sami sebe ali pa druge škodljive programe tako dobro, da jih niti protivirusni programi ne morejo najti. Rootkit programi se pogosto širijo v obliki računalniških črvov in trojanskih konjev. Svojega cilja ne dosežejo tako, da ukradejo ali ponaredijo administratorsko geslo. To namreč niso običajni programi, ki se izvajajo z administratorskimi pravicami, ampak zmorejo več. Izvajajo se kot del operacijskega sistema in prilagodijo njegovo obnašanje. Na računalniku jih najdemo v različnih, tudi nenavadnih oblikah: lahko so v ROMu strojne opreme, ki je instalirana v računalniku, npr. v kakšnem čipu na matični plošči ali v kakšni razširitveni kartici. V tem primeru jih ni mogoče izbrisati, lahko se izdajajo za jedro operacijskega sistema in uporabijo postopek virtualizacije, da naložijo pravo jedro. Na ta način popolnoma nadzirajo dostop do strojne opreme. Veliko rootkit programov se izdaja za gonilnike oz. module operacijskega sistema in tako pridobijo moč, da spreminjajo obnašanje operacijskega sistema. Lahko se izdajajo za sistemske knjižnice in tako prilagodijo obnašanje sistema, lahko se izdajajo za običajne programe, ki jih uporabnik izvaja z administratorskimi pravicami in tako v tem primeru lahko počnejo vse, kar lahko naredi administrator.

Glede na to, da na okuženem računalniku spreminjajo datoteke, so rootkit programi podobni računalniškim virusom. Glavna razlika je v tem, da se rootkit program ne trudi razmnoževati, ampak bolj skrbi za to, da vse njegove funkcije delujejo pravilno (npr. da ima nepooblaščena oseba ves čas dostop do računalnika). Razlika je tudi v tem, da namen rootkit programa ni delati neposredno škodo na računalniku (npr. brisanje datoteke), saj mu je v interesu, da je sistem delujoč in da čim dlje ostane neopažen.

Znana afera z uporabo rootkit programov se je zgodila leta 2005, ko je podjetje Sony BMG, ki je velik založnik glasbenih zgoščenk, na njih sistematično razširjalo rootkit program za operacijski sistem Windows. Ta se je instaliral na računalniku, na katerem ste poslušali glasbo in preprečeval nelegalno kopiranje. Imel pa je

napake in je med drugim omogočal nepooblaščenim osebam, da prevzamejo nadzor nad vašim računalnikom (Meolic, 2009).

2.3.2 Vdori v sistem

Vdori ali poskusi vdorov v omrežja so vse bolj pogosti načini napadov »heckerjev«, »crackerjev«, detektivov, nadobudnih študentov in vohunov. Prizadeta niso samo velika pomembna podjetja, ampak je potencialna žrtev teh napadov lahko katerokoli podjetje ali posameznik.

Motivi takšnih napadalcev so zelo različni, od političnih razlogov, radovednosti, samopotrjevanja, vojaških interesov, denarja, do kriminalnega ozadja. Cilji napadov so pridobitev, spreminjanje ali prilagajanje pomembnih podatkov, finančno okoriščanje, maščevanje ali pa samo povzročanje škode.

Zaradi visoke povezljivosti, ki so jo sistemi dosegli z rastjo in razvojem interneta, se je verjetnost za vdore še povečala. Sistem organizacije ni ogrožen samo od napadalcev, ki so v fizični bližini organizacije ali v sami organizaciji, temveč lahko informacijski sistem organizacije postane žrtev storilca, ki se lokacijsko nahaja na drugi strani planeta in je zaradi tega težko izsledljiv. Tovrstne storilce je za njihova kazniva dejanja težko kazensko ovaditi, kar daje napadalcem občutek varnosti in nedotakljivosti. Da bi se podjetje uspešno ubranilo tovrstnih napadov, je edina učinkovita obramba primeren sistem zaščite informacijskega sistema in visoka ozaveščenost vseh zaposlenih. Prvotnega pomena pri vzpostavitvi varnosti je visoka strokovna usposobljenost skrbnikov sistemov, bistveno pa je tudi, da je vodstvo primerno seznanjeno s tovrstnimi nevarnostmi in podpira vzpostavitev varnostne politike ter s tem primernega nivoja varnosti, ki zahteva visoke finančne vložke in se tega zaveda. Če je informacijski sistem že v osnovi slabo zasnovan, lahko posledično prihaja do preobremenitev in odpovedi sistema. Ne smemo pozabiti, da predstavljajo poleg potencialnih zunanjih napadalcev veliko nevarnost za podjetje zaposleni sami. Zaposleni v organizaciji poznajo njeno delovanje, strukturo in lahko namerno ali nenamerno povzročijo veliko škodo informacijskemu sistemu (uničijo ali poškodujejo pomembne datoteke, ovirajo delovanje sistema, ukradejo ali ponaredijo podatke (Klančnik, 2007).

Fizični in logični vdori

Logični vdori so vdori preko informacijskega sistema podjetja, običajno preko internetne povezave ali preko brezžičnega omrežja. Tak vdor je posledica napak v programski opremi, t.j. operacijskem sistemu, aktivnih strežniških programih, nato napak pri nastavitvi (konfiguraciji) programske opreme ali pa napačnega ravnanja uporabnika (Bratuša, Verdonik, 2005).

Logični vdor v računalniško omrežje pomeni nepooblaščen dostop preko računalniške opreme, ki ga izvede zaposleni ali tuja oseba z uporabo nezakonitih postopkov in metod, kot so razkritje uporabniških gesel s prisluškovanjem omrežju, odkrivanje enostavnih gesel in gesel, ki jih pozna večja skupina ljudi in se ne spreminjajo periodično z različnimi postopki. S takšno zlonamerno dejavnostjo si napadalec pridobi dostopne pravice do dobrin organizacije, do katerih sicer nima dostopa, s čimer pa lahko pride do nepooblaščenih sprememb, razkritja ali uničenja dobrin (Klančnik, 2007).

Fizični vdor je vlom ali katerikoli nepooblaščeni fizični dostop do informacijskega sistema podjetja.

Čeprav sta si obe vrsti vdora na videz zelo različni, so njune posledice podobne: uničenje ali odtujitev dela informacijskega sistema.

Kraja in nezakonito razmnoževanje intelektualne lastnine, kot so znanje, načrti, podatki o kupcih in cenah, predstavlja za podjetje resno grožnjo varnosti. Podjetje mora storiti vse, da takšne podatke zaščiti pred zlorabami in ne sme dopustiti, da takšni podatki »pricurljajo« v javnost, do konkurentov, saj bi to lahko ogrozilo obstoj, integriteto podjetja ali mu povzročilo veliko poslovno in finančno škodo. Organizacijske pomanjkljivosti, kot so npr. slaba, nepopolna ali napačna navodila in dokumentacija, so lahko posledica za nepravilno upravljanje dobrin ali izvajanje delovnih postopkov, zaradi česar pride do spreminjanja, poškodbe ali odpovedi dobrin organizacije. Tovrstne pomanjkljivosti je težko odkriti, poraba časovnih in finančnih virov pri odpravi le-teh pa zelo velika (Klančnik, 2007).

Vlom razumemo kot zelo resno grožnjo varnosti, saj lahko uresničitev te grožnje prizadene vse dobrine organizacije, posledice pa so kraja, uničenje ali poškodba dobrin, delna ali popolna nedosegljivost sistema, poškodbe ljudi, itd. Da bi organizacija ustrezno zaščitila svoje dobrine pred tovrstno grožnjo varnosti, je priporočljivo, da uvede primerne varovalne ukrepe, kot so: z mrežo zaščitena okna v prostor, dostop skozi vhodna vrata pod neposrednim nadzorom varnostnega osebja, celotno območje dostopa do prostora pod nadzorom varnostnega osebja preko nadzornih kamer, omejeno območje gibanja strank, prostor pod stalnim nadzorom ali opremljen z alarmnimi napravami.

V mnogih primerih so dejanja računalniške sabotaže in izsiljevanja, npr. nasilje na delovnem mestu, izvedena s strani nezadovoljnih zaposlenih, ki so jezni zaradi odpuščanja ali premestitev na drugo delovno mesto. Spet drugi primeri zajemajo zaposlene, ki želijo izkoristiti svoj položaj z namenom finančnega okoriščanja, nato hekerje, ki so zaposleni v organizaciji in sodelujejo pri nepooblaščenih raziskovanjih po omrežju in pridobivanju kritičnih informacij ali pa dobro motivirane zaposlene, ki trdijo, da nepooblaščene posege opravljajo v najboljšem interesu organizacije.

Grožnjo predstavljajo tudi povzročitelji, ki jih imenujemo »krti«.To so posamezniki, ki v organizacijo pridejo izključno z namenom povzročitve prevare in vohunstva.

Število groženj, ki jih izvedejo zaposleni je vsako leto večje. Takšne grožnje zelo težko preprečiti s kakršnokoli tehnologijo. Brez temeljite raziskave notranjih groženj in razvoja novih metod upravljanja tveganja znotraj organizacije, kot je nepravilen pristop do upravljanja varnosti informacijskega sistema, pridemo do spoznanja, da so kritične, pomembne informacije ranljive na grožnje varnosti, kot so prevare, vohunstva ali sabotaže s strani tistih, ki poznajo sistem najbolje, in to so zaposleni (Klančnik, 2007).

Napadalec

Napadalec je oseba ki poskuša oz. dejansko izvede napad z uporabo naučenih mehanizmov ali intuicije na računalniški sistem. Napad lahko označimo kot:

- poskus vdora ali dejanski vdor v sistem,
- vdor v zasebnost posameznika ali združbe,
- izsiljevanje posameznika ali združbe,
- poskus onemogočanja storitve in
- lokalni ali oddaljeni dostop do naprave ter zlonamerna manipulacija skozi njene vhodno/izhodne vmesnike.

Napadalci imajo različna imena in so odvisni od dejanj, ki jih povzročajo.

- Heker (angl. hacker) je računalniški zanesenjak, ki uživa v raziskovanju. Sam navdušeno, celo obsedeno programira in spoštuje lastna etična pravila, ki pravijo, da mora biti dostop do računalnikov mogoč vsakomur, informacije pa svobodno dostopne, da nam računalniki izboljšujejo življenje, oblasti (politiki, vojski in pravosodju) pa ne gre zaupati. Heker je lahko tudi oseba, ki je zelo vešča v neračunalniški panogi, dokler jo ubiranje nedokumentiranih ali neuveljavljenih poti vodi do hitrejšega rezultata z manj truda. V praksi lahko takšno delovanje pripelje do nevarnih posledic, zato so potrebna etična in varnostna načela. Ločimo med sekači (angl. white-hat) in lomači (ang. black-hat) hekerji. Sekači spoštujejo nekatera etična pravila, ki jih ločijo od lomačev, ki svoje znanje in sposobnosti uporabljajo za krajo podatkov in povzročanje škode. Sekači delujejo zgolj zaradi ljubezni do računalništva in morebitne slave - brez kakršnekoli denarne motivacije. Večina hekerjev je še mladoletnih, vendar kljub svoji starosti predstavljajo veliko nevarnost za vse vrste, saj s svojim razmišljanjem nikakor ne zaostajajo za ostalimi izkušenimi računalničarji. Nekateri izmed njih delujejo v posebno organiziranih skupinah, katerih cilji so vdiranje v sisteme in medsebojna izmenjava informacij. Dejavnost hekerjev imenujemo hekanje (angl. hacking).

- Kreker (angl. cracker) je oseba, ki svoje znanje uporablja za razbijanje zaščitnih mehanizmov različnih sistemov (ne samo računalniških). Nekateri označujejo krekerje kot neetične hekerje, ki svoje znanje uporabljajo za nelegalna dejanja, kot so kraja podatkov, vdori v računalniške sisteme in podobno. Kreker imenujemo tudi računalniške strokovnjake z zelo dobrim poznavanjem strojnega jezika in ustreznih metod, s pomočjo katerih odstranjujejo zaščitne mehanizme različnih programskih paketov in jih s tem pripravijo na neokrnjeno in nemoteno delovanje brez potrebne registracije ali aktivacije. To najpogosteje dosežejo s postopkom, imenovanim obratno inženirstvo (angl. reverse engineering).

Vzrok za napade so motivi napadalcev, ki jih lahko delimo na načrtovane in priložnostne napade. Načrtovani napadi so napadi na tarčo s točno določenim namenom. Motivi za takšno obliko napadov so lahko zelo različni: iskanje podatkov ali informacij za lastne potrebe, napad po naročilu druge osebe z namenom finančne koristi (industrijsko vohunjenje), izkazovanje moči in znanja o tehnologiji, zabava in ostalo. Če k motivu iskanja podatkov ali informacij za lastne potrebe pripišemo še razlog izključne želje po znanju o tehnologiji, dobimo enega izmed zelo razširjenih motivov za napade. Kot opravičljiv razlog za svoja dejanja v

okviru računalniških napadov bo veliko število napadalcev navedlo ravno iskanje znanja, ki drugače ni dostopno širši javnosti. K motivu iskanja podatkov ali informacij za lastne potrebe lahko dodamo še razloge, kot so radovednost, kraja identitete, kraja zaupnih podatkov, s katerimi se želijo napadalci hvaliti med vrstniki in podobno.
Zelo pomembno je, da napad skrbno analiziramo in preučimo. Analizirati moramo naslednje stvari:

- zaradi koga ali česa se je napad zgodil,
- kdo je neposredno odgovoren, da je napadalec lahko uspešno izvedel napad,
- ocena nastale škode po napadu,
- stopnja ogroženosti zaradi napada in
- verjetnost, da se bo napad ponovil.

Lokalni napad

Napad z lokalnim dostopom je napad, kjer ima napadalec neposreden stik s tarčo, se pravi, da je prisoten znotraj omrežja ali pa direktno na sistemu, kjer ga napada. Takšne vrste napadov je zelo težko zaznati, še posebej, če napad izvaja oseba, ki je dejansko zaposlena tam. Takšna oseba namreč bolj ali manj pozna sistem in njegovo varnostno zaščito.

Steve Stasiukonis je v članku Social Engineering, the USB way opisal naslednjo metodo lokalnega napada. V podjetju Secure Network Technologies Inc. so za znanega naročnika izvedli napad. Napisali so trojanskega konja, ki ob zagonu zbere podatke o računalniku, jih zakodira in pošlje na izbran elektronski poštni naslov. Aplikaciji so zamenjali prvotno ikono s takšno, ki poskuša prikazati datoteko, kot da je ta tipa JPEG, torej slika. Ob tem so se zanašali na privzeto lastnost operacijskega sistema Microsoft Windows, da ne prikazuje končnic tipov datotek. Tako uporabnik mislil, da gre dejansko za sliko, privlačno ime le-te pa bo sigurno sprožilo njen zagon. Tako prirejeno datoteko so posneli na večje število USB ključev. Te so zgodaj zjutraj namestili na različne lokacije v območju podjetja, ki je bil naročnik preizkusa. Pričakovali so, da bodo mimoidoči, predvsem zaposleni v tem podjetju, te ključe našli in si jih seveda prilastili. Od skupaj 20 nameščenih USB ključev, so jih 15 našli zaposleni. Ko so sedli na svoje delovno mesto, so iz radovednosti vklopili USB ključ v svoj računalnik ter kliknili na datoteko, ki je bila videti kot slika z zanimivim imenom. S tem so ročno pognali trojanskega konja, ki je zbral podatke o računalniku in jih poslal na izbran elektronski poštni naslov. Zanimivo je, da so prav vsi zaposleni vklopili najden USB ključ v službeni računalnik. Vzrok za veliko uspešnost te vrste napada je slabo zastavljena varnostna politika v podjetju ali zgolj njeno nespoštovanje med uslužbenci. Ta metoda napada je zanimiva predvsem zato, ker gre dejansko za obliko napada z lokalnim dostopom, čeprav napadalec ne vzpostavi stika s tarčo, ampak ta opravi delo namesto njega (Žagar, 2006).

Oddaljeni napad

Danes je največ napadov izvršenih na daljavo, na računalniške sisteme, ki so priklopljeni v svetovni splet.

Pri tej vrsti napada ni neposrednega stika med napadalcem in tarčo. Napad poteka

preko vmesnika, ki je v največ primerih kar napadalčev lasten osebni računalnik. Dostop do tarče ni omogočen preko njenih osnovnih vmesnikov (tipkovnica, miška, zaslon), pač pa preko njenega vmesnika za komuniciranje z ostalimi sistemi (modem, mrežni vmesnik, bluetooth ipd.). Dostop do tarče je omogočen skozi izbrane komunikacijske poti, žične ali brezžične.

Napad na sistem, zaščiten z geslom

Na sistem, do katerega dostop je zaščiten z geslom, poznamo več tehnik in metod napadov. Najpogostejša je metoda ugibanja gesel, kjer bo napadalec ob prvem stiku s sistemom poskušal uporabiti nekaj najpogostejših gesel, kot so »admin«, »password« in podobno. Zelo pomembno vlogo igra tukaj identifikacija sistema, s katerim pride napadalec v stik. Če ga uspe identificirati, ga lahko poskusi locirati v seznamu sistemov z njihovimi privzetimi gesli, ki jih po svetovnem spletu kroži kar lepo število. Prav tako lahko sedaj pri ugibanju gesel uporabi podatke v navezi z nazivom sistema.

Naslednja metoda vključuje poznavanje uporabnikov sistema. Napadalec lahko ob znanju, kdo je uporabnik sistema, izvede navzkrižno iskanje med njimi in poskuša dobiti podatke o podatkih, potrebnih za overjanje iz drugih sistemov, ki so slabše varovani. Ni potrebno posebej poudarjati, da uporabljajo povprečni uporabniki isto geslo za vse vrste overjanj, on-line in o-line. Če se je ugibanje gesel pri napadalcu izkazalo za neuspešno, lahko sedaj poskuša uporabiti katero izmed orodij, ki nadaljuje delo namesto njega. Pri svojem delovanju lahko uporabi besedne sezname, ki vsebujejo obsežno zbirko najpogosteje izbranih gesel ali pa izvede napad z uporabo grobe sile, kjer bo enostavno preizkusil vse možne znakovne kombinacije. Na z geslom zaščiten sistem lahko napadalec izvede tudi drugačno vrsto napada. Poiskati poskuša poti, pri katerih bi lahko zaobšel mehanizem za overjanje.

V grobem delimo napade na z geslom zaščitene sisteme na lokalne in oddaljene.

Pri lokalnih napadih imamo navadno dostop do zgoščenih vrednosti gesel ali vsaj do mehanizma za overjanje, na katerem lahko izvedemo tudi inverzno inženirstvo.

Pri oddaljenih napadih nimamo dostopa do zgoščenih vrednosti gesel in lahko dostopamo samo do mehanizma za overjanje, skozi katerega izvajamo napad.

Napad s preizkušanjem vseh možnih kombinacij

Napad s preizkušanjem vseh možnih kombinacij (angl. brute force attack) velja za najmočnejše orodje pri razbijanju sistemov, ki so varovani z gesli. Napadalec skuša z namenskim orodjem izvršiti prijavo na sistem za overjanje z uporabo vseh možnih kombinacij izbranega nabora znakov in številk.

Napad s preizkušanjem vseh možnih kombinacij je lahko izveden na daljavo ali lokalno, v obeh primerih pa se napada program za overjanje, ki teče na napadenem sistemu. Časovna zahtevnost takšnega napada je odvisna predvsem od nabora znakov in dolžine niza, ki naj bi predstavljalo geslo ter od hitrosti delovanja mehanizma za overjanje. Če je napad izvršen na daljavo, moramo k časovni zahtevnosti dodati še hitrost komunikacijske poti in možnost paralelnega

napada.

V času starejših operacijskih sistemov Unix je proces generiranja zgoščene vrednosti DES algoritma trajal več kot sekundo. Ta lastnost je zelo omejila možnost tega napada. Za napadalca je bila tehnika skoraj neuporabna, saj je preverjanje gesel trajalo predolgo.

Danes je moč pri nekaterih mehanizmih za overjanje opaziti namensko zakasnitev pri napačno vnesenih geslih. Napad s preizkušanjem vseh možnih kombinacij je 100% uspešen, če predpostavimo, da imamo na voljo neomejeno časa, kjer lahko uporabimo celotni možni nabor znakov, ki jih uporablja napadeni sistem (Wack, Tracy, Souppaya, 2003).

Privzeta gesla

Privzeta gesla oz. privzeti podatki za overjanje so del privzetih tovarniških nastavitev. Naprava, ki ni delana za znanega naročnika, bo ob prihodu na prodajne police vsebovala že vnaprej izbrane splošne nastavitve, ki bodo uporabniku omogočale njeno čimprejšnjo uspešno vzpostavitev. Te nastavitve lahko med drugim vključujejo tudi v konstrukcijskem procesu izbrana privzeta gesla. Ta gesla so namenjena enkratni uporabi, zgolj za namestitev naprave, po tem pa naj bi se zamenjala s poljubno izbranim novim geslom. Nespretni uporabniki tega gesla po namestitvi ne bodo spremenili in bodo tako svojo napravo nevede izpostavili napadalcem. Ohranjanje tovarniških nastavitev, kjer ni nujno govora samo o podatkih za overjanje, je lahko zelo tvegano dejanje. Napadalci bodo ob stiku s sistemom vedno preizkusili, če morda na njem deluje še kakšno privzeto, tovarniško nastavljeno in nikoli spremenjeno geslo. Privzeta gesla je mogoče s pomočjo spletnega iskalnika poiskati za katerokoli napravo.

Napad z uporabo besednega seznama

Napad z uporabo besednega seznama (angl. dictionary attack) je oblika napada z uporabo metode grobe sile, le da tu za geslo ne preverimo vse možne vrednosti, ampak zgolj tiste, ki smo jih pripravili vnaprej. Te vrednosti oz. izraze napadalec združi v datoteko, ki tvori besedni seznam. Besedni seznami so že zelo stara tehnika napada in vsebujejo izraze, ki so bili statistično ugotovljeno največkrat uporabljeni kot geslo za različne sisteme. Vsebujejo tudi privzeta gesla. Napadalec bo pred napadom na z geslom zaščiten sistem pripravil ustrezen besedni seznam. Najpomembneje je vedeti, katere narodnosti je večina uporabnikov. Uporaba besednega seznama, ki vsebuje izraze v ustreznem jeziku, je zelo pomembna za večjo uspešnost. Za angleško govorečega uporabnika je manj verjetno, da bo za geslo izbral nemško besedo.

Zanimiva je analiza nekega seznama okrog 100.000 gesel iz nemške strani za zmenke Flirtlife.de, objavljena na nemški spletni strani heise.de. Izvemo, da so uporabniki v 1375. primerih (1,4%) za geslo izbrali niz 123456 in da se 2,5% izbranih gesel začne z nizom 1234 (Heise online, 2006).

Ti podatki so zelo dobrodošli napadalcem pri sestavljanju njihovih lastnih besednih seznamov, ki jih lahko nato uporabljajo pri svojih nadaljnjih napadih.

Na internetu je bil pred časom objavljen tudi slovenski besedni seznam, ki naj bi vseboval najpogosteje uporabljena gesla slovenskih uporabnikov (Žagar, 2006).

Napad z mavričnimi tabelami

Napad z mavričnimi tabelami (angl. rainbow tables) je oblika napada na gesla, ki so shranjena v sistemu. Operacijski sistemi gesel ne shranjujejo neposredno v datoteko, temveč se uporabljajo t. i. zgoščevalne funkcije, s katerimi naredimo "prstni odtis" gesla, ki ga nato shranimo.

Pri shranjevanju odtisa gesel se v grobem uporabljata dva sistema:

- Zgoščevalno funkcijo se izvede na nespremenjenem geslu ali pa je sprememba taka, da je za vsako geslo unikatno določena in znana.
- Geslu se doda naključna vrednost - sol (angl. salt) in nad tako spremenjenim geslom izvedemo zgoščevalno funkcijo. Dodano seme ni tajno, saj ga potrebujemo kasneje.

Na prvi pogled sta oba sistema enako varna, vendar je bistvena prednost drugega sistema v tem, da odtis gesla ni možno vnaprej določiti, ker je odvisen od neke naključne vrednosti, ki jo dodamo geslu. Na ta način postane napad z mavričnimi tabelami zelo otežen ali pa praktično nemogoč.

Če napadalcu uspe dobiti datoteko z gesli, ne more ugotoviti gesel preostalih uporabnikov, saj so v datoteki shranjene samo zgoščevalne vrednosti gesel. Velja, da če nekdo pozna zgoščevalno vrednost, ne more ugotoviti izvirnega gesla, razen tako, da poskusi vse možne kombinacije besed oz. gesel, nad njimi izvede zgoščevalno funkcijo ter zgoščevalno vrednost, ki jo dobi, primerja z zgoščevalno vrednostjo v datoteki.

Napad z mavričnimi tabelami temelji na izračunanih vseh možnih kombinacijah znakov in njihovih zgoščevalnih vrednosti. Tako dobimo velikansko tabelo "gesel" in pripadajočih zgoščevalnih vrednosti. Napad je podoben metodi z uporabo z grobo silo, s tem, da moramo pri napadu z grobo silo vnesti vsako geslo v program, ki preverja geslo (npr. pri prijavi v sistem Windows). Pri napadu z mavričnimi tabelami pa v tabeli poiščemo ustrezno zgoščevalno vrednost in že imamo geslo. Mavrične tabele so vnaprej izračunane in tako napadalcu prihranijo veliko časa, saj samo poišče ustrezno vrednost v velikanski tabeli. To pa je precej hitreje, kot če poskuša vsa gesla in čaka na odziv, ali je geslo pravilno. Lahko bi rekli, da je napad kombinacija napada z grobo silo in napada s slovarjem, pri katerem imamo zelo velik slovar, v katerem so gesla in pripadajoče zgoščevalne vrednosti.

Napad zavrnitve storitve

Napad zavrnitve storitve (angl. Denial of Service Attack - DoS) deluje tako, da pošlje veliko zahtev na oddaljeni sistem, ki zaradi preobremenitve ohromi njegovo delovanje. Napade lahko izvajamo posamično, tako da napadamo sistem samo z enega računalnika ali pa množično, napad z več računalnikov hkrati.

Priljubljena tarča napadalcev so domenski in spletni strežniki, v bistvu pa se lahko na takšen način ohromi delovanje katerekoli omrežne naprave.

Preden se napadalec pripravi na DoS napad, lahko po internetu pošlje malware, program, ki okuži ostale računalnike in na njegov poziv vsi računalniki pošljejo zahtevek na napadalno stran.

Lahko naredimo tudi ping napad, tako da pošiljamo velike pakete sporočil na žrtvin računalnik in ga tako preobremenimo.

Obstaja tudi tretja opcija – SYN flood. SYN flood pošlje poplavo TCP/SYN paketov, običajno s ponarejenim naslovom pošiljatelja. Vsak paket je obravnavan kot zahtevek za novo povezavo, zaradi česar sistem pošlje nazaj paket TCP/SYN-ACK, in čaka odgovor, saj bi se z odgovorom povezava vzpostavila. Odgovor napadalca ne pride, zahtevki se pa še kar pošiljajo dalje in čakajoči odgovori se vrstijo. Navadni uporabnik, ki čaka na paket TCP/SYN-ACK, ga ne sprejme, saj čaka v vrsti. Sprejme ga šele, ko je napada konec.

Napad s posrednikom

Napad s posrednikom (angl. man in the middle - MITM) je napad, kjer se napadalec oz. njegov računalnik nahaja med dvema napravama v omrežju. Cilj napadalčeve akcije je prestrezanje paketov v komunikaciji med tema napravama ter naknadno posredovanje na legitimni cilj, brez vednosti sodelujočih entitet. Primer MITM napada je zastrupljanje ARP tabele.

Pojavljata se dve obliki MITM napadov, prisluškovanje in manipulacija. Pri prisluškovanju napadalec preprosto posluša sporočila med uporabnikom in ponudnikom storitve. V primeru, ko napadalec manipulira povezavo, le-ta nadomesti legitimnega uporabnika in sam uporablja storitev. Napadalec običajno uporablja protokole, kot so UDP, TCP, ICMP in SYN.

Seveda je tak napad najučinkovitejši, kadar poskušamo prestreči komunikacijo protokolov, ki so prosto berljivi (npr. Telnet, Rlogin, FTP, SMTP, LDAP...). Vztrajen in izkušen napadalec pa lahko prestreže tudi komunikacijo šifriranega protokola, npr. SSH in Kerberos (Strosar, 2006).

Socialno inženirstvo

Socialni inženiring (manipulacija) je najenostavnejši in najcenejši način napada, ki s pridom izkorišča človekovo nevednost, lahkomiselnost in zaupljivost. Zaposleni postane žrtev napada zunanjega napadalca, ki se izdaja za neko drugo osebo (npr. serviserja, ki opravlja nujni poseg) in si z navajanjem resničnih dejstev pridobi zaupanje zaposlenega, ki napadalcu zaupa informacije, ki jih le-ta želi. Ob takšni obliki napada odpovejo vsa klasična orodja varovanja. Edino orožje proti takšnim oblikam napadov je stalno izobraževanje in ozaveščanje zaposlenih (Klančnik, 2007).

Socialno inženirstvo prav gotovo obstaja že dolgo časa, frikerji pa so bili tisti, ki so ga konec 60. let prejšnjega stoletja na široko uporabljali. Najpogosteje so se izdajali za tehnike ali operaterje, zaposlene pri telefonskem podjetju. Pri socialnem inženirstvu se pooseblja predvsem kredibilne osebe, ki imajo ustrezne avtorizacije in dostop do podatkov, katerih se želi napadalec polastiti. Sogovornika poskuša prepričati, da mu razkrije zaupne podatke ali celo sam za

njega opravi naloge, za katere sam nima avtorizacije.

Kevin Mitnick je v svoji knjigi The Art of Deception poudaril, da požarne pregrade in postopki kodiranja podatkov ne bodo odvrnili nadarjenega socialnega inženirja od poskusa manipulacije z ljudmi, ki so v neposrednem stiku s tehnologijo. Če želi napadalec napasti sistem, je najučinkovitejši pristop izkoriščanje najšibkejšega člena. To niso računalniški sistemi, ampak ljudje. Socialno inženirstvo je ena izmed tistih metod, kateri velikokrat posvečamo premalo pozornosti. Moramo se zavedati, da je v končni fazi človek tisti, ki nosi največjo odgovornost in tisti, ki potrebuje ustrezno izobraževanje (Mitnick, 2002).

Naprednejša metoda socialnega inženirstva je inverzno socialno inženirstvo. Napadalec ustvari osebo z ustrezno kredibilnostjo in povzroči, da drugi (zaposleni) povprašujejo njega po podatkih. Ta metoda socialnega inženirstva zahteva več priprav, raziskav in verjetno tudi ostale oblike predhodnih napadov. Če je izvedena pravilno, obeta napadalcu večjo možnost pridobitve uporabnih podatkov. Obstajajo tri oblike inverznega socialnega inženirstva: sabotaža, oglaševanje in nudenje pomoči (Granger, 2010).

Obratno inženirstvo

Obratno inženirstvo (angl. reverse engineering) je postopek iskanja tehnoloških načinov mehanskega sistema skozi analizo njegove strukture, funkcionalnosti in operativnosti. Postopek običajno zajema razstavitev nekega stroja, komponente ali programske opreme na manjše dele, katerih delovanje postane tako razumljivejše. Napad na računalniški sistem lahko vključuje obratno inženirstvo katere izmed komponent sistema ali bolj verjetno programske opreme. Obratno inženirstvo programske opreme lahko izvedemo na več načinov: z analizo podatkovnih tokov, razstavitvijo delujoče programske kode na nivo strojnega jezika in razstavitvijo delujoče programske kode na nivo programskega jezika, v katerem je bil prvotno pisan.

Analiza je skozi opazovanje izmenjave podatkov prevladujoča pri obratnem inženirstvu protokolov. Tehnike in metode, ki se uporabljajo, so predvsem analiziranje vodila in prisluškovanje podatkovnemu toku. Vohljači (angl. snifers) omogočajo vpogled v prenos podatkov, kar omogoča opazovalcu analiziranje protokola. Če pozna njegovo delovanje, lahko naredi programsko opremo, ki simulira delovanje neke druge naprave ali programske opreme. Protokol Samba je bil razvit tako, da so razvijalci analizirali protokol NetBIOS v operacijskem sistemu Microsoft Windows in izdelali njegovo različico za operacijski sistem Linux. Analizo podatkovnih tokov je možno preprečiti tako, da se podatki pred prenosom kodirajo.

2.3.3 Naključni dogodki

Odpovedi strojne in programske opreme, napake uporabnikov in napake v podatkih lahko resno ogrozijo delovanje in s tem varnost informacijskega sistema. Da bi zmanjšali verjetnost odpovedi strojne opreme, je priporočljivo vzpostaviti sistem podvojenih komponent na delih, ki so za delovanje celotnega sistema kritični, z namenom, če pride do odpovedi komponente, njeno nalogo prevzame nadomestna komponenta. Komponento, ki odpove, pa v čim krajšem času

popravimo ali nadomestimo. Težava lahko nastane, če pride do degradacijske odpovedi komponente. V takšnem primeru sistem in komponenta še delujeta, vendar lahko pride do napačnih obdelav in posledično do napačnih končnih rezultatov. Da se takšna tveganja zmanjšajo, so priporočljivi in potrebni preventivni pregledi sistema in njegovih delov ter nenehno spremljanje in nadzor nad obdelavami. Na zelo podoben problem naletimo na področju programske opreme, ki je še pomembnejši in občutljivejši del informacijskega sistema. Da bi odkrili napačno delovanje ali odpoved programske opreme, je potrebno v same programe vgraditi večstopenjska preverjanja, ki na vsako napačno delovanje ustrezno reagirajo (Klančnik, 2007).

Uporabniki napake najpogosteje povzročijo zaradi neupoštevanja navodil, pravil ali predpisov. Informacijski sistemi uporabnike in skrbnike na takšne napake sicer opozarjajo, pa vendar lahko ti kljub temu izvedejo opravilo, ki predstavljajo grožnjo delovanju informacijskega sistema. Zato je zelo pomembno, da se zaposleni povežejo s skrbniki informacijskih sistemov z namenom odprave tako odkritih groženj.

2.3.4 Izredni dogodki

Naravne nesreče kot so npr. požar, potres, izliv vode ali poplava predstavljajo veliko potencialno nevarnost za informacijski sistem. Na takšne grožnje moramo biti pripravljeni z ustreznimi varnostnimi mehanizmi, kot so npr. oddaljena varnostna kopija podatkov, dokumentacija postopkov za ponovno vzpostavitev delovanja, seznam odgovornih delavcev in zunanje podpore. V primeru izpadov električne energije (udar strele, tehnične težave), pa moramo z ustreznimi napravami poskrbeti, da bo informacijski sistem nemoteno deloval naprej.

2.4 Zagotavljanje informacijske varnosti

Informacijska varnost je zelo obsežno in zapleteno področje. Samuelle (2009) navaja, da moramo zagotavljati informacijsko varnost vsaj na naslednjih področjih:

- sistemska varnost,
- varnost podatkov,
- omrežna varnost,
- fizična varnost,
- organizacijska varnost.

2.4.1 Sistemska varnost

Sistemska varnost igra zelo pomembno vlogo pri zagotavljanju informacijske varnosti. Vse grožnje in nevarnosti so bolj ali manj povezane s sistemsko varnostjo oz. varnostjo samega operacijskega sistema. K sistemski varnosti lahko uvrstimo tudi varnost pripadajoče programske opreme, saj lahko njene varnostne pomanjkljivosti prav tako ogrozijo sistemsko varnost.

Operacijski sistem je najpogosteje odskočna deska za napadalce, ki »luknje« v operacijskem sistemu izkoriščajo za nadaljnje napade in povzročanje škode.

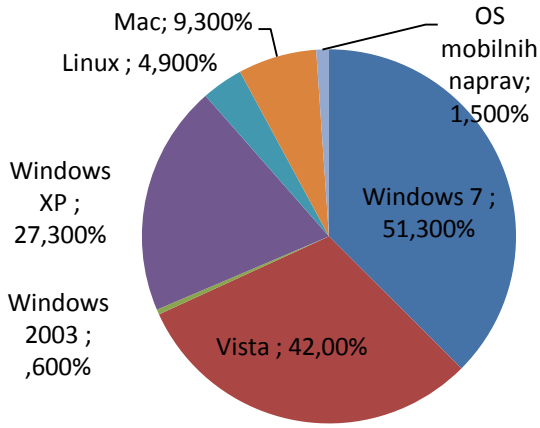
Največkrat omenjena grožnja sistemske varnosti je nedvomno škodljiva programska oprema, h kateri spadajo virusi, črvi, trojanski konji in podobno. Kljub temu, da novi operacijski sistemi s seboj prinašajo tudi nove varnostne mehanizme, nevarnosti še ostajajo, kar lahko sklepamo po neprestanih varnostnih popravkih in posodobitvah operacijskih sistemov pa tudi druge programske opreme. Kateri so glavni razlogi za vse varnostne pomanjkljivosti, verjetno ne bomo nikoli izvedeli. Verjetno je vzrok tudi v tem, da je razvoj programske opreme izredno hiter in posledično tudi pomanjkljiv.
Nekateri celo menijo, da gre za sodelovanje med avtorji protivirusne in škodljive programske opreme.

Veliko grožnjo predstavljajo tudi sami uporabniki operacijskega sistema. Domači uporabniki običajno dobijo računalnik z nameščenim operacijskim sistemom, varnost pa jih ne zanima. V organizacijah je situacija drugačna. Te se morajo sistemske varnosti zavedati in o tem poučiti tudi svoje zaposlene. Takšni uporabniki lahko znatno pripomorejo k izboljšanju informacijske varnosti.

Operacijski sistem

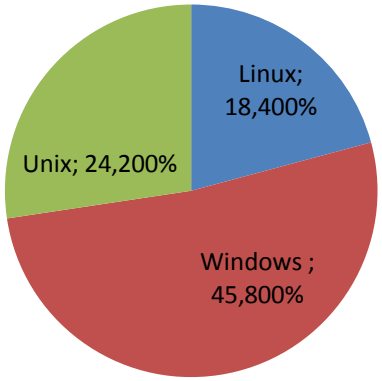
Zapisali smo že, da je za zagotavljanje sistemske varnosti potrebno najprej poskrbeti za varnost operacijskega sistema samega, kamor spadajo tudi varnostni popravki in posodobitve sistema. Kljub nenehnim varnostnim popravkom pa stopnja varnosti, ki jo nudi sam operacijski sistem, običajno ni povsem dovolj. Imeti moramo nameščeno tudi ustrezno zaščitno programsko opremo. Pod to opremo mislimo predvsem na protivirusne programe, na programe za preprečevanje vdorov in podobno. Zelo pomembno vlogo pri zagotavljanju sistemske varnosti ima programska oprema in storitve, ki tečejo na operacijskem sistemu. Velikokrat je ravno programska oprema tista, ki povzroča ranljivosti operacijskega sistema. Pri vsem tem moramo omeniti tudi uporabnike, saj so oni tisti, ki operacijski sistem uporabljajo in nam lahko z nepremišljenimi dejanji ogrozijo informacijsko varnost. Zaradi tega moramo poleg ustreznih varnostnih mehanizmov poskrbeti tudi za ustrezno ozaveščanje uporabnikov.

Na osebnih računalnikih oz. delovnih postajah prevladuje operacijski sistem Microsoft Windows. Raziskava spletne strani w3schools.com, ki je bila opravljena aprila 2012, kaže, da se največ uporabljajo operacijski sistemi Windows 7, Windows Vista ter Windows XP. Delež uporabe operacijskih sistemov prikazuje slika 1.



Slika 1: Najpogostejši operacijski sistemi osebnih računalnikov (Vir: w3schools.com, 2012)

Najpogosteje prisoten operacijski sistem strežnikov je prav tako Windows. Raziskava družbe International Data Corporation (IDC) iz leta 2011 kaže, da ima Windows 45,8% delež na trgu, sledita pa mu Unix in Linux. Rezultate omenjene raziskave prikazuje slika 2.



Slika 2: Najpogostejši operacijski sistemi strežnikov (Vir: IDC, 2012)

Microsoft Windows

Microsoft Windows je najbolj priljubljen operacijski sistem osebnih in prenosnih računalnikov, marsikje pa je uporabljen tudi kot strežniški operacijski sistem. Iz statistike o uporabi smo ugotovili, da se na delovnih postajah največ uporabljata operacijska sistema Windows XP in Windows 7.

Izid operacijskega sistema Windows XP sega v leto 2001, tako da ne gre za najnovejši operacijski sistem, kljub temu pa se še vedno pojavlja na največ računalnikih. Zaradi priljubljenosti je Windows XP pogosto tarča napadalcev, ki hitro najdejo varnostne pomanjkljivosti. Najbolj izstopajo slabosti v navezi s

spletnim brskalnikom Internet Explorer. Kljub dokaj dolgemu obstoju na trgu pa Microsoft še vedno skrbi za varnost sistema s številnimi varnostnimi popravki. Verjetno zato, ker je ta operacijski sistem še vedno največ v uporabi, saj nadgradnja in prehod na novejšo različico ni tako enostavna.

Danes zelo priljubljena verzija operacijskega sistema je Windows 7. Windows 7 vsebuje številne varnostne izboljšave in nove varnostne mehanizme. Seveda pa bomo pravo varnostno podobo dobili šele po daljšem časovnem obdobju uporabe.
Operacijski sistem Windows Server je strežniška različica operacijskega sistema. Gre za večnamenski operacijski sistem, primeren za številne različne strežniške vloge in potrebe uporabnikov, tako v centraliziranih kot v distribuiranih sistemih. Nekatere od teh strežniških vlog so:

- datotečni in tiskalni strežnik,
- spletni strežnik in strežnik za spletne aplikacije,
- poštni strežnik,
- terminalski strežnik,
- strežnik za oddaljeni dostop in navidezna zasebna omrežja (VPN),
- strežnik za imeniške storitve, DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol) in WINS (Windows Internet Naming Service).

Operacijski sistem Windows ima vgrajene številne varnostne mehanizme in orodja, ki ob ustrezni uporabi zagotavljajo višjo varnost sistema. Razumljivo je, da se z razvojem operacijskega sistema izboljšuje tudi njegova varnost. Varnost sistema pa je odvisna tudi od namena njegove uporabe.

Če teče sistem na delovni postaji, potem na sistemu ne potrebujemo dodatnih procesov, ki bi lahko ogrozili varnost operacijskega sistema. V primeru, da sistem deluje na strežniku pa je situacija drugačna, saj mora sistem poleg osnovnih storitev zagotavljati tudi strežniške storitve, kar pomeni tudi večje nevarnosti. Zaradi tega se tudi priporoča, da postavimo ločene strežnike za različne storitve.

Kljub različnim varnostnim značilnostim lahko potegnemo nekaj vzporednic, ki so bolj ali manj enake vsem aktualnim verzijam operacijskih sistemov Windows. Prvič se z varnostjo srečamo že, ko se prijavimo v sam sistem. V sistem se moramo v dokaz svoje istovetnosti prijaviti z uporabniškim imenom in geslom. Seveda se lahko v sistem prijavimo tudi brez gesla, kar pa seveda ni varno.

Gesla so shranjena v obliki prstnega odtisa v lokalno SAM datoteko ali pa v aktivni imenik domene. Starejši Windows sistemi (Windows XP) uporabljajo dva načina za shranjevanje gesel, imenovana LM in NTLM. LM način je starejši in manj varen, ranljiv je na tako imenovane "brute force" napade. Za overjanje v omrežju se uporabljata NTLM in NTLMv2 protokola, slednji pa je tudi varnejši. Priporočljivo je, da se v domeni, kjer nobeden od odjemalcev ni starejši od različice Windows 2000, z uporabo skupinskih politik prepove LM shranjevanje gesel, kot protokol pa se uporabi NTLMv2.

V operacijskem sistemu Windows ima najvišje pravice uporabnik, imenovan administrator. Priporočeno je, da ta uporabniški račun preimenujemo ali pa ga onemogočimo in ustvarimo novega. Nekateri operacijski sistemi Windows imajo ob namestitvi omogočen račun za goste, kar pomeni prijave v sistem brez gesla, zato moramo takšen račun nujno onemogočiti.

Če smo administrator na sistemu, lahko izvajamo vsa opravila na sistemu, brez kakršnih koli omejitev. Operacijski sistem Windows 7 na tem področju prinaša novost. S t.i. nadzorom nad uporabniškimi računi (angl. user account control) imajo vsi uporabniki sistema uporabniške pravice, tudi administrator. V primeru izvajanja določenih opravil nas sistem z obvestilom predhodno opozori.

Vsi aktualni operacijski sistemi Windows imajo privzeto vgrajeno požarna pregrado. Operacijska sistema Windows XP in 2003 nam ponujata dokaj malo varnostnih nastavitev požarne pregrade. Lahko ga zgolj vklopimo in izklopimo ali pa dodamo pravila za dohodni promet.

Windows 7 prinaša na tem področju izboljšavo. Poleg boljšega nadzora nad dohodnim prometom lahko spremljamo in nadzorujemo tudi odhodni promet. Seveda pa lahko pravila za odhodni in dohodni promet urejamo tudi po svoje. Poleg tega Windows 7 omogoča nastavitev požarne pregrade na 3 vrstah omrežij, in sicer na omrežju z domeno, domačem omrežju in javnem omrežju. Omrežju primerno se spremenijo tudi varnostne nastavitve.

Varnostni popravki in posodobitve imajo pomembno vlogo pri zagotavljanju sistemske varnosti. Pomembno je, da posodabljamo tudi ostalo programsko opremo. Posodobitve različnih operacijskih sistemov Windows se med seboj kaj dosti ne razlikujejo. Izbiramo lahko med samodejnim posodabljanjem in posodabljanjem ob določenem času. Določimo lahko tudi možnost, da posodobitve prenesemo in jih namestimo sami. Seveda lahko posodobitve tudi izključimo.

Veliko varnostnih nastavitev lahko določimo s pomočjo tehnologij Group Policy in Local Group Policy. V Windows strežniškem okolju uporabljamo Group Policy, ki nam omogoča, da preko aktivnega imenika (angl. Active Directory – AD) centralno administriramo uporabnikovo delovno okolje, dostop do aplikacij in njihovo namestitev, nadzor nad dogodki in sredstvi v AD in varnostnimi nastavitvami. Na domenskem strežniku lahko do najbolj uporabnih nastavitev Group Policy dostopamo preko dveh administracijskih orodij: Domain Security Policy in Domain Controller Security Policy. Prva določa nastavitve vseh računalnikov v domeni, druga pa samo domenskih strežnikov.

Na lokalnih računalnikih lahko varnostne nastavitve določimo s pomočjo Local Group Policy, izbiramo lahko med varnostnimi nastavitvami na nivoju uporabnika in na nivoju računalnika.

Za šifriranje podatkov na nivoju datotečnega sistema se v Windows okolju uporablja Encrypting File System – EFS. Tehnologija nudi transparentno shranjevanje in dostopanje do kodiranih datotek na datotečnem sistemu NTFS. EFS uporablja kriptografijo javnih ključev, kar je sicer dober faktor zaščite, vendar lahko napadalec še vedno uporabi napad z uporabo grobe sile pri razbijanju zaščite uporabniškega računa za dostop do računalnika. Deluje tako, da uporabnik v raziskovalcu označi datoteke ali imenik, ki ga želi zakodirati in mu doda atribut kodirano (angl. Encrypt contents to secure data). Sistem sicer uporablja kriptografijo javnih ključev, a le za shranjevanje simetričnega ključa, ki se uporablja za dejansko šifriranje in dešifriranje podatkov.

Še ena varnostna funkcija, ki jo prinaša Windows 7 in jo velja omeniti, je BitLocker. BitLocker omogoča večjo zaščito vsega, tudi dokumentov in gesel, tako da šifrira celotni pogon, na katerem so nameščeni sistem Windows in naši podatki. Če je funkcija BitLocker vklopljena, se vse datoteke, ki jih shranimo v zaščiteni pogon, samodejno šifrirajo. BitLocker To Go pa omogoča zaklepanje prenosne naprave za shranjevanje, kot so pogoni USB in zunanji trdi diski, ki jih lahko mimogrede izgubimo.

V Windows 7 najdemo še eno varnostno novost, to je biometrična zaščita. Windows 7 namreč podpira bralnike prstnih odtisov, ki omogočajo uporabniku na podlagi njegovega prstnega odtisa varno prijavo v sistem. Novost je še posebej dobrodošla za uporabnike prenosnih računalnikov, ki so danes v kar veliki meri opremljeni s temi bralniki.

Vsi operacijski sistemi Windows pa tudi ostali imajo možnost oddaljenega dostopa do sistema in upravljanja z njim. Sama funkcionalnost sicer nima neposredne zveze z varnostjo, razen v primeru, ko določene varnostne nastavitve urejamo na daljavo. So pa številne nevarnosti, v primeru, da oddaljenega dostopa nimamo urejenega na varen način. Najlažje se teh nevarnosti izognemo tako, da oddaljen dostop izključimo, kar pa v nekaterih primerih ni izvedljivo.

Če želimo v Windowsih omogočiti oddaljen dostop, moramo to storitev najprej omogočiti in jo dodati med izjeme v požarni pregradi. Takoj ko to storimo, pa postane sistem tudi bolj ranljiv, saj s tem odpremo tudi določena vrata (angl. port) za izvajanje storitve. Napadalec potem skuša preko tega vdreti v naš sistem. Za karseda varno prijavo je priporočljivo, da za dostop določimo uporabnika, ki ni administrator. Privzeta vrata, na katerih storitev »posluša«, je dobro spremeniti, saj običajno napadalci preizkušajo ravno ta. Prav tako je dobro, da nastavimo zaklepanje računa v primeru »brute force« napada. Še dodatno lahko oddaljen dostop zaščitimo tako, da dovolimo dostop le iz določenega IP naslova. To lahko storimo v sami požarni pregradi operacijskega sistema ali pa na usmerjevalniku. Varnost lahko še dodatno izboljšamo, če povezavo do oddaljenega računalnika šifriramo. Za šifriranje lahko uporabimo SSL protokol. Na oddaljenih računalnikih z novejšimi operacijskimi sistemi (Windows 2008 in Windows 7) lahko omogočimo tudi povezavo z uporabo certifikata, s pomočjo katerega se lahko prepričamo, da se povezujemo na pravi oddaljeni računalnik.

Linux

Razvoj Linuxa sega v leto 1991, ko je takrat 21-letni študent računalništva Linus Benedict Torvalds iz Helsinkov, pripadnik švedske manjšine na Finskem, začel pisati (najprej kot hobi) Minixu podoben operacijski sistem. Kasneje je v novičarski skupini comp.os.minix najavil svojo namero in nato na internetu objavil prvo različico operacijskega sistema, ki so ga po njem poimenovali Linux. Takoj so mu priskočili na pomoč številni zanesenjaki z vsega sveta in operacijski sistem je postajal iz dneva v dan zmogljivejši in bolj priljubljen.
Uporaba Linuxa se je naglo povečala, njegova priljubljenost pa narašča še danes. Skorajda vsako podjetje, ki na področju informacijske tehnologije kaj pomeni, ga jemlje zelo resno.

Razlogi za hitro širitev in priljubljenost so naslednji:

- cena (Za Linux običajno ne potrebujemo plačati licence, so pa tudi izjeme.),
- varnost, stabilnost in zanesljivost (Milijoni ljudi po svetu Linux redno izboljšujejo, zato je Linux zelo varen in zanesljiv operacijski sistem.),
- podpora (Lastnik operacijskega sistema Linux ni eden sam, zaradi česar je tudi podpora toliko večja in učinkovitejša. Obstaja posebna lista, namenjena uporabnikom Linux-a (angl. Linux users groups), kamor lahko pošljemo el. sporočilo v primeru težav.),
- združljivost (Linux podpira širok nabor strojne opreme in deluje praktično na vseh osebnih računalnikih.),
- orodja in aplikacije (Pester je tudi izbor programov in najrazličnejših orodij za operacijski sistem Linux, veliko jih je na voljo tudi brezplačno.).

Sistemski administratorji Linux še posebej cenijo zaradi enostavnosti administriranja sistema in manjše možnosti povzročitve nepopravljive škode. Uporaba vmesnika se ne spreminja bistveno, z izjemo lepotnih popravkov. To pomeni, da lahko uporabnik prvih distribucij Linuxa brez večjih težav preide na novejšo. Linux v nasprotju z Windowsi dejansko omogoča delo več uporabnikom hkrati. Po drugi strani pa drži, da je do uporabnika bolj neodpustljiv kot Windows, ne uživa podpore proizvajalcev strojne opreme v tolikšni meri. Prav zaradi tega pa na njem ne delujejo nekatere profesionalne aplikacije.

Operacijski sistem Linux imamo na voljo v različnih distribucijah. Skupno vsem je to, da temeljijo na enaki arhitekturi jedra, medtem ko se vsebina nekoliko razlikuje. Vsaka distribucija ima namreč svoj skupek programov, inštalacijskih paketov in ostalih aplikacij. Distribucije se razlikujejo tudi v podpori, saj imajo nekatere ob doplačilu vključeno sistemsko podporo, medtem ko druge tega nimajo. Vsaka distribucija je posledično prilagojena tudi različnim namenom uporabe. Nekatere so namenjene strežniškim sistemom, nekatere delovnim postajam, obstajajo pa tudi takšne, ki so prilagojene specifični funkciji delovanja. Najpogosteje najdemo Linux, ki je prilagojen delovanju kot strežnik, nekaj je namenjenih tudi delovnim postajam, ki pa se trenutno še ne morejo enakovredno kosati z operacijskim sistemom Windows, vsaj kar se tiče prisotnosti in priljubljenosti med uporabniki. Naslednja razlika je v različnih lokacijah datotek na disku, posledično pa tudi namestitveni paketi med distribucijami niso povsem združljivi. Omeniti velja še eno razliko. To je razlika v podpori in pri ponudniku operacijskega sistema. Nekatere distribucije so plod dela različnih prostovoljcev iz celega sveta, medtem ko so druge v lasti podjetja. Temu primerno se razlikuje tudi cena podpore uporabnikom. Med različnimi distribucijami velja omeniti sledeča imena:

- Red Hat Enterprise Linux,
- CentOS,
- The Fedora Project,
- Debian Linux,
- Ubuntu,
- Gentoo,
- Suse Linux.

Red Hat Linux je zelo razširjen med uporabniki in obstaja v različnih verzijah. Najbolj poznani sta Red Hat Enterprise Linux (poznan kot RHEL) in Red Hat

Enterprise Linux Advandced Platform (poznan kot RHELAP). Največja razlika med njima je v številu procesorjev, ki jih podpirata. RHEL podpira največ 2 procesorja, medtem ko RHELAP podpira neomejeno število procesorjev. Red Hat Linux v veliki meri uporabljajo podjetja.

Operacijski sistem CentOS izhaja iz Red Hat Linuxa. Izvorna koda je povsem enaka, dosegljiv pa je povsem brezplačno. CentOS je zato znan kot zelo zanesljiv in zaradi cene tudi priljubljen med uporabniki. Skrb za njegovo delovanje je prepuščena zgolj administratorjem, saj CentOS nima podpore uporabnikov, kot jo ima Red Hat Linux.

Tudi distribucija Fedora izhaja iz Red Hat Linux-a. Razvijajo jo prostovoljci, ki so predhodno skrbeli za Red Hat Linux. Za Fedoro je značilno, da vsebuje novosti, ki jih izda Red Hat in tako deluje kot neke vrste testni operacijski sistem, iz katerega potem nastane nova različica Red Hat Linux-a.

Projekt Debian GNU/Linux je organiziral Ian Murdock leta 1993. Najprej pod pokroviteljstvom projekta GNU ustanove Free Software Foundation (FSF), pozneje pa se je Debian ločil od FSF. Debian je rezultat prostovoljnih naporov za izdelavo prostega, visokokvalitetnega operacijskega sistema, zasnovanega na jedru Linuxa in združljivega z Unixom s popolnim naborom aplikacij. Skupnost Debiana je skupina več kot 150 neplačanih prostovoljcev z vsega sveta, ki sodelujejo preko Interneta. Ustanovitelji projekta so oblikovali organizacijo Software in the Public Interest (SPI), ki sponzorira nadaljnji razvoj sistema Debian GNU/Linux. Software in the Public Interest je neprofitna ustanova, ki so jo ustanovili, ko je FSF umaknil svoje pokroviteljstvo nad Debianom. Naloga organizacije je razvijati in razširjati prosto programsko opremo. Njeni cilji so zelo podobni ciljem FSF in spodbuja programerje.

Podobno kot Windows ima tudi Linux vgrajene številne varovalne funkcije. Linux običajno deluje kot strežnik, kar pomeni 24 ur na dan in 365 dni na leto. Zaradi tega je še bolj izpostavljen nevarnostim kot sistemi, ki se uporabljajo zgolj na delovnih postajah.

Ob namestitvi sistema lahko izbiramo med številnimi storitvami. Priporočljivo je, da izberemo samo tiste, ki jih zares potrebujemo. Vse dodatne storitve namreč samo ogrožajo varnost sistema.

Ob namestitvi sistema moramo določiti tudi uporabniško geslo za najvišjega uporabnika, to je root. Priporočeno je, da zanj določimo močno geslo ter da račun uporabljamo samo v primeru, ko je to nujno potrebno.

Geslo se podobno kot v ostalih sistemih shranjuje v obliki prstnega odtisa. Pri shranjevanju se geslu doda 12 bitna »sol«, nad katerim se nato izvede zgoščevalna funkcija. Tako lahko ima katerokoli geslo 4096 različnih možnosti, kar pomeni 4096 različnih odtisov in posledično tudi višjo varnost. Poleg tega so odtisi gesel shranjeni v ločeni datoteki (običajno /etc/shadow), ki je dostopna samo uporabniku root in določenim procesom.

Ob zagonu sistema Linux se najprej srečamo z datoteko /etc/inittab, v kateri je nastavljen nivo izvajanja sistema (angl. run level). Poznamo naslednje nivoje izvajanja:

- 0: Ustavljen sistem (pripravljen na izklop)
- 1: Enouporabniški režim
- 2: Večuporabniški režim brez mrežnih datotečnih sistemov
- 3: Večuporabniški režim z mrežo
- 4: Navadno ni v uporabi
- 5: Večuporabniški sistem z GUI
- 6: »Reboot« režim

Za sisteme, ki delujejo kot strežniki, se običajno uporablja nivo 3. Če pa želimo grafično podporo, uporabimo nivo 5. Izbira stopnje je povezana tudi z varnostjo in zanesljivostjo sistema. Višji nivo namreč pomeni več storitev, obenem pa porabi tudi več strojnih kapacitet.

Za sam zagon jedra sistema skrbi zagonski nalagalnik (npr. GRUB, LILO). V zagonskem nalagalniku je določeno, katero jedro se bo zagnalo in kje se to nahaja. Priporočljivo je, da zagonski nalagalnik zaščitimo z geslom in s tem preprečimo nepooblaščeno zaganjanje in spreminjanje sistema ob zagonu.

Vse varnostne nastavitve v sistemu Linux lahko izvajamo iz ukazne lupine. Nekatere distribucije pa imajo poleg tega vgrajene še grafične vmesnike (GUI). Seveda obstaja tudi cela vrsta dodatnih aplikacij (npr. Webmin), kjer lahko varnostne pa tudi ostale nastavitve nastavljamo preko uporabniku prijaznega vmesnika.

Linux ima vse nastavitve, vključno z varnostnimi, shranjene v obliki datotek, ki se običajno nahajajo v imeniku /etc.

Vse Linux distribucije imajo vgrajeno požarno pregrado. Požarna pregrada v sistemu Linux deluje podobno kot filter na usmerjevalniku. Promet lahko filtriramo na podlagi IP naslova izvora in cilja, na podlagi protokola, številk vrat ter tipov in kod ICMP sporočil. Pravila požarne pregrade se primerjajo s paketi, nato pa program bodisi zavrne (angl. deny) bodisi sprejme (angl. accept) paket. Najbolj poznana sta programa ipchains in novejši iptables. Priporoča se uporaba iptables, ker ima vgrajen mehanizem, s katerim lahko ugotovimo, ali je nek vhodni IP paket del seje, ki jo je vzpostavil odjemalec na tem sistemu, ali pa gre za nek »tuj« IP paket, ki prihaja iz zunanjega sistema. Ta mehanizem imenujemo tudi statefull. Seveda poznamo tudi ostale programske pakete, ki lahko v veliki meri nadomestijo komercialno požarna pregrado.

Podobno kot v sistemu Windows imamo tudi v Linuxu opravka z oddaljenim dostopanjem do sistema. Priporočljivo je, da omogočimo dostop samo določenim uporabnikom iz določenega IP naslova ter da pri tem uporabimo protokol SSH.

Na varnost sistema lahko pomembno vplivamo z rednim posodabljanjem sistema, pri čemer moramo paziti, da posodobimo vse dodatne aplikacije in ne samo osnovni sistem.

Upravljanje z uporabniškimi računi

Sistemsko varnost lahko izboljšamo tudi z ustrezno varnostno politiko uporabnikov. Priporočljivo je, da omejimo pravice na nivo, ki uporabnikom še omogoča nemoteno delo, ne dovoli pa jim izvajanja višjih nivojskih opravil. S tem smo uporabnikom preprečili, da bi hote ali nehote nameščali programsko opremo, onemogočeno pa jim je tudi spreminjanje sistemskih nastavitev. Z omejevanjem pravic lahko vsaj delno preprečimo izvajanje škodljive programske opreme, ki bi se v primeru, da imajo vsi uporabniki administratorske pravice, izvedla brez posebnih omejitev.
Omejevanje uporabniških pravic ima tudi določene slabosti. Tukaj mislimo predvsem na dodatno delo sistemskega administratorja, ki mora voditi uporabniške račune, več dela pa ima tudi s programsko opremo, saj jo lahko namešča le on. Seveda se da to z ustrezno organizacijo omrežja znatno poenostaviti. V nadaljevanju si oglejmo organizacijo uporabniških računov v operacijskem sistemu Windows in Linux.

Microsoft Windows

V sodobnih operacijskih sistemih Windows se varnostne pravice (prijava v sistem, dostop do dokumentov, tiskalnikov) določajo na nivoju uporabniških računov. Uporabniški račun enolično določa posameznega uporabnika in mu dovoljuje pravice, vezane na njegovo uporabniško ime. Da nepooblaščena oseba ne more uporabljati drugega uporabniškega imena, so le-ta zaščitena z geslom. Pri določitvi gesel moramo biti še posebej pozorni pri uporabniških računih, ki imajo večje privilegije. Če izberemo enostavno geslo (ali če gesla sploh ne določimo) za npr. administratorjev uporabniški račun, smo potencialnemu hekerju močno olajšali delo in na široko odprli vrata.

Uporabniški račun predstavlja enolično identifikacijo uporabnika (ID) in mu omogoča prijavo tako na lokalno delovno postajo kakor tudi prijavo v domeno. Vsak uporabniški račun je zaščiten z geslom. S prijavo v domeno dobi uporabnik žeton, s katerim so določene pravice dostopa do virov v omrežju.

Lokalni račun omogoči uporabniku prijavo na računalnik in uporabo lokalnih virov (dokumentov, map, tiskalnikov...). Uporabniški račun je shranjen v lokalni bazi (SAM).

Domenski račun omogoča, da ima uporabnik dostop do domenskih virov v celotni domeni. Uporabnik se lahko prijavi iz poljubnega računalnika, razen če mu je ta pravica eksplicitno prepovedana. Uporabniški račun je shranjen v Active Directory bazi.

Vgrajeni račun Windows ustvari pri namestitvi dva uporabniška računa (administrator in gost). Administratorski račun nam daje vse pravice nad računalnikom in je namenjen za administracijo. Račun za goste (angl. guest) služi uporabi naključnim uporabnikom in običajno temu računu dodelimo najmanj pravic. Poleg teh Windows ustvari še druge uporabniške račune, ki ne služijo lokalni prijavi.

Skupine (angl. groups) vsebujejo uporabniške račune. Uporabniške račune združujemo v skupine z namenom lažje administracije in učinkovitejšega dodeljevanja pravic. Član skupine pridobi vse pravice, ki pripadajo skupini. Na vsakem računalniku z Windows sistemom obstajajo lokalne skupine, ki jih lahko uporabljamo le na tistem računalniku. Na domenskem strežniku pa imamo domenske skupine, ki so vidne znotraj cele domene.

Lokalne skupine lahko ustvarimo na vseh računalnikih Windows, razen na domenskih strežnikih. Lokalni skupini lahko dodeljujemo pravice samo na računalniku, kjer je bila skupina ustvarjena. Namen lokalnih skupin je dovoliti uporabnikom določene pravice, ki jih pridobijo s članstvom v določeni lokalni privilegirani skupini. Sistemi Windows pri instalaciji avtomatično zgradijo privilegirane lokalne skupine.

Značilnosti lokalnih skupin:

- Vsebujejo lahko globalne skupine in račune domene.
- Ne morejo vsebovati lokalnih skupin.
- Lokalni skupini se lahko dodelijo pravice samo na računalniku, kjer je bila ustvarjena.
- Lokalna skupina ne more biti članica nobene druge skupine.

Tabela 1 prikazuje najpomembnejše privilegirane lokalne skupine in njihove bistvene administracijske pravice.

Tabela 1: Skupine uporabnikov v OS Windows
(Vir: B2,2004)

SKUPINA	OPIS	ZAČETNI ČLANI
Account operators	Člani lahko upravljajo uporabniške račune in skupine uporabnikov.	
Administrators	Popolna administracija stroja.	Administrator oz. Domain Admins
Backup operators	Skupina ima možnost ustvarjanja rezervnih kopij.	
Guests	Skupina z zelo omejenimi možnostmi dela.	Domain Guests
Print operators	Upravljanje tiskanja.	
Replicator	Skupina, ki lahko podvaja datoteke med različnimi računalniki.	
Server operators	Delna administracija strežnika, ne more pa upravljati nobenih varnostnih nastavitev (uporabniki, skupine, sistemska pravila …).	
Users	Vsak nov uporabnik se avtomatično doda v to skupino.	Globalna skupina: Domain Users
Network Configuration	Člani imajo nekatere administracijske pravice za nastavitve omrežja (ni na	

SKUPINA	OPIS	ZAČETNI ČLANI
Operators	voljo v Windows 2000).	
Remote Desktop Users	Imajo pravico za prijavo na oddaljen računalnik (ni na voljo v Windows 2000).	
HelpServicesGroup	Skupina za "Help and Support Center".	

Domenske skupine so vidne v celotni domeni in na vseh delovnih postajah, ki so vključene v domeno. Ustvarimo jih lahko samo na domenskem strežniku. S pomočjo domenskih skupin si omogočimo lažjo administracijo vseh računalnikov v domeni. Vsak nov uporabniški račun, ki ga ustvarimo na domenskem strežniku, postane avtomatično član skupine domenskih uporabnikov. Število domenskih skupin ni konstantno, temveč se spreminja glede na servise, ki jih imamo nameščene na strežniku. Tabela 2 prikazuje seznam bistvenih domenskih skupin.

Tabela 2: Seznam domenskih skupin v OS Windows
(Vir: B2, 2004)

SKUPINA	OPIS	ZAČETNI ČLANI
Domain Admins	Člani lahko administrirajo domeno, domene, ki tej domeni zaupajo ter delovne postaje.	Administrator domene
Domain Users	Navadni uporabniki domene.	Vsi novi uporabniki v domeni
Domain Guests	Globalni račun: Guest.	
Domain Computers	Vsi računalniki (razen Windows 9x).	
Domain Controlers	Vsi domenski strežniki v domeni.	

V strežniškem sistemu Windows obstajata dve vrsti domenskih skupin:

- »Security groups« - so običajne skupine, katerim dodeljujemo dovoljenja in pravice dostopov do virov.
- »Distribution groups« - so namenjene programom za pošiljanje elektronske pošte. Če naslovimo distribucijsko skupino, dobijo elektronsko pošto vsi člani skupine. Distribucijsko skupino ne moremo uporabiti za dodeljevanje pravic in dovoljenj.

Domenske skupine ločimo glede na doseg in namen uporabe v tri vrste: domenske lokalne skupine, globalne skupine in univerzalne skupine. Razlika med temi vrstami skupin se pokaže šele, če imamo v gozdu več domen.

- Globalne skupine – lahko vsebujejo samo domenske uporabnike in globalne skupine iz domene. Uporabimo jih lahko za določanje pravic v vseh domenah. Vidna je v celotnem gozdu v vseh domenah.
- Domenske lokalne skupine - vsebujejo lahko vse uporabnike in skupine iz vseh domen. Uporabimo jih lahko za določanje pravic samo v domeni, v kateri je bila ustvarjena. In vidna je samo v domeni, v kateri je bila ustvarjena.

- Univerzalne skupine – lahko vsebujejo vse uporabnike in skupine iz vseh domen. Uporabimo jih lahko za določanje pravic v vseh domenah. Vidna je v celotnem gozdu v vseh domenah.

Zelo pomembna je strategija uporabniških skupin in uporabnikov. Le-ta je odvisna od nivoja varnosti in nadzora, ki ju želimo imeti. Zelo moramo biti pazljivi na pravice posameznih skupin. Pravilna strategija uporabe domenskih skupin igra bistveno vlogo pri administraciji domene. Delo in nadzor si bistveno poenostavimo s pravilnim gnezdenjem skupin. Pri Microsoftu predlagajo postopek A-G-DL-P. Uporabniški račun (angl. account) uvrstimo v globalno skupino (angl. global group), globalno skupino uvrstimo v domensko lokalno skupino (angl. domain local group) in nazadnje domenski lokalni skupini določimo pravice ter dostop do virov (angl. permission).

Uporabnik dobi pravice s članstvom v privilegirani lokalni skupini. Lahko pa se zgodi, da članstvo v skupini dodeli uporabniku preveč privilegijev, ker se pravice dodelijo v svežnju. Preko »Domain Security Policy« lahko uporabnikom dodajamo posamezne pravice.

Linux

Linux je večopravilni in večuporabniški operacijski sistem, kar pomeni, da lahko več ljudi hkrati poganja več različnih aplikacij na enem samem računalniku. V sistem se moramo podobno kot v Windowsih prijaviti z uporabniškim imenom in geslom, ki je naš osebni ključ za prijavo v naš račun.

Sistemski administrator na sistemu Linux je imenovan root. Za uporabnika root ni omejitev. Lahko bere, spreminja ali pobriše katerokoli datoteko na sistemu, spreminja dovoljenja in lastništvo katerekoli datoteke in poganja posebne programe, kot so tisti, ki razdelijo trdi pogon ali ustvarijo datotečne sisteme. Osnovna zamisel tega je, da se oseba, ki skrbi za sistem, prijavi v sistem kot root ter izvaja opravila, ki jih ne bi mogla izvajati kot običajni uporabnik. Ker lahko root naredi karkoli, je mogoče narediti napake s katastrofalnimi posledicami. Če navaden uporabnik nenamenoma poskuša pobrisati vse datoteke v imeniku /etc., mu sistem tega ne bo dovolil, medtem ko za uporabnik root to ni ovira.

Za normalno uporabo ni priporočljivo uporabljati tega uporabniškega računa, saj lahko zaradi neomejenih pravic, hitro storimo kakšno nepopravljivo napako.

Uporabniške račune za ostale uporabnike operacijskega sistema lahko izdela le administrator. Nadzor dostopa se vrši na podlagi pravic, ki jih je administrator dodelil uporabnikom. V sistemu pa obstajajo tudi uporabniki, ki so bili kreirani za točno določene storitve. Tako se recimo ob namestitvi poštnega strežnika (angl. mail server) ustvari uporabnik z imenom mail. Uporabniki operacijskega sistema pripadajo eni, lahko pa tudi več uporabniškim skupinam.

Uporabniku pripadajo pravice, ki so določene za skupino, v kateri se nahaja. Koncept uporabnikov in uporabniških pravic je podoben tistemu v operacijskem sistemu Microsoft Windows. Ob kreiranju uporabniškega računa dobi vsak uporabnik tudi svoj imenik v katerem ima dodeljene vse pravice..

Dovoljenja datotek so urejena tako, da običajni uporabniki ne morejo brisati ali spreminjati datotek v določenih imenikih. Večina uporabnikov ščiti svoje lastne datoteke z ustreznimi dovoljenji, da drugi uporabniki ne morejo dostopati do njih ali jih spreminjati.

Spremljanje sistemskih procesov in dogodkov

Definicija pravi, da je računalniški proces aktivno delujoči izvod programa, torej vsak program, ki smo ga morebiti pravkar pognali (Kranjčič, 2004).

Vsakemu procesu operacijski sistem ob kreiranju ali izvrševanju procesa dodeli določene vire, kot so čas CPE, pomnilnik, datoteke in vhodno/izhodne naprave.

Proces je lahko sistemski ali uporabniški. V skladu s to lastnostjo so mu dodeljene tudi pravice za dostop do virov računalniškega sistema. Velikokrat proces ni enovit, ampak je sestavljen iz niti (angl. threads). Nit si lahko predstavljamo kot določen del procesa. Vzemimo za primer poljuben urejevalnik besedil. Glavna nit skrbi za prikaz tipkanega besedila, druga nit lahko skrbi za preverjanje črkovanja med tipkanjem, tretja pa lahko istočasno tiska del dokumenta, ki ga urejamo itd. (Harej, 2008).

Procesi tečejo v ozadju operacijskega sistema, zato jih niti ne opazimo oz. jim ne posvečamo pozornosti. So pa procesi tisti, ki nam kažejo, kaj točno se s sistemom dogaja. Procese je potrebno spremljati tudi zaradi varnostnih razlogov, saj lahko iz njih točno vidimo, kateri uporabnik poganja kateri proces. Če smo sistemski administratorji, poznamo procese, ki na našem sistemu tečejo in tudi njihove uporabnike. Posledično lahko iz tega vidimo, če je v tem delu kaj narobe. S procesi lahko prav tako spremljamo obremenitev in posledično tudi zanesljivost delovanja sistema. Zanesljivost delovanja sistema je še kako pomembna, ko govorimo o informacijski varnosti.

Pri zagotavljanju varnosti je pomembno tudi redno spremljanje podatkov o določenih dogodkih. Ti podatki nam med drugim lahko povedo, kdaj je želel nekdo vdreti v naš računalnik, kdaj se je uporabnik prijavil in kdaj odjavil ter podobno.

Microsoft Windows

Operacijski sistem Windows vsebuje kar nekaj orodij, ki omogočajo nadzor nad delovanjem sistema. Napake, ki se pojavijo, lahko pravočasno zaznamo in poiščemo odgovor nanje.

Upravitelj opravil (angl. task manager) je izredno uporaben program, s katerim lahko spremljamo aktivne programe in procese. Z njim lahko spremljamo zasedenost pomnilnika in aktivnost procesorja. Za zagon tega programa lahko uporabimo naslednje načine:

- kombinacija tipk CTRL+SHIFT+ESC,
- desni miškin klik na opravilni vrstici in ukaz zaženi upravitelja opravil,
- kombinacija tipk CTRL+ALT +DELETE in ukaz zaženi upravitelja opravil,
- v ukazni vrstici ga lahko izvedemo z ukazom taskmgr.exe.

V opravilni vrstici na desni strani se prikaže aktivnost upravitelja opravil. Program je sestavljen iz štirih oz. petih zavihkov (programi, procesi, učinkovitost delovanja, omrežje in uporabniki). Zavihek uporabniki je na voljo le, če je naš računalnik v delovni skupini.
V zavihku programi vidimo vse programe, ki so trenutno aktivni. Iz statusa lahko vidimo, ali se programi trenutno izvajajo (angl. running). Kadar se nek program preneha odzivati, se izpiše »not responding«. Z ukazom končaj opravilo trenutni izbrani program zaustavimo, z ukazom preklopi izberemo nov aktivni program in z ukazom novo opravilo zaženemo nov program.

V zavihku procesi lahko podrobno spremljamo vse procese. Računalnik potrebuje za svoje delovanje tudi sistemske procese.

Zavihek učinkovitost delovanja nam prikazuje uporabo pomnilnika in procesorja. Uporaba CPE nam prikazuje trenutno zasedenost procesorja, zgodovina uporabe procesorja pa hrani nekaj trenutkov zgodovine. Enako velja tudi za pomnilnik.

Zavihek omrežje grafično prikazuje delovanje omrežja. Predstavlja enostaven indikator, ki prikazuje stanje omrežne povezave našega računalnika.

V zavihku uporabniki vidimo vse trenutno prijavljene uporabnike. To so lokalno prijavljeni uporabnik in vsi uporabniki, prijavljeni preko terminalskega servisa. Uporabnike lahko tu tudi odklopimo ali odjavimo.

»Performance Monitor« je sistemski program, s katerim ugotavljamo obremenjenost procesorja, zasedenost navadnega in navideznega pomnilnika, obremenitev omrežnih protokolov, obremenjenost diskov ... Na podlagi njegovih rezultatov se odločimo za določene optimizacijske postopke. »Performance Monitor« lahko zaženemo iz administrative tools /performance ali pa neposredno z ukazom perfmon.msc. Za prikazovanje rezultatov imamo na razpolago tri načine: dva grafična načina in obliko poročil (številčni prikaz). Za katero obliko se odločimo, je odvisno od števca, ki ga želimo prikazovati. Tako v primeru merjenja obremenjenosti procesorja izberemo grafični način, pri merjenju omrežnega prometa bit/sek pa je boljše izbrati obliko poročil.

Orodje »Event Viwer« najdemo v administrativnih orodjih. Z njegovo pomočjo spremljamo aktivnosti na lokalnem ali omrežnem računalniku. Omogoča pa nam tudi zbiranje informacij o strojnih in programskih napakah in preobremenjenosti komponent ter podobno. Servis za spremljanje dogodkov se zažene avtomatično pri zagonu računalnika. Dogodki se beležijo v posebnih dnevniških datotekah (angl. log files). Dogodki, ki jih »Event Viewer« beleži, so odvisni od operacijskega sistema. V operacijskem sistemu Windows XP so zabeleženi naslednji dogodki:

- Sistemski dogodki, ki jih ustvari operacijski sistem, se zapišejo v system log.
- Programski dogodki, ki jih ustvarijo programi, se zapišejo se v application log.
- Varnostni dogodki, ki jih ustvari operacijski sistem, ko so se sprožili določeni varnostni mehanizmi, ki smo jih nastavili.

Beleženje sistemskih dogodkov lahko nastavimo v orodju »Local Computer Policy«. V mapi »local policies« imamo tri podprograme, in sicer »audit policy«, »user

rights assignment« in »security options«. Kar se tiče varnosti na lokalnem računalniku, je v teh treh mapah večina varnostnih nastavitev. Mapa user »rights assignment« je namenjena določanju sistemskih pravic uporabnikov in skupin. V mapi »audit policy« lahko določamo, katere dogodke bomo spremljali. Mapa »security options« je namenjena številnim varnostnim nastavitvam uporabniških računov, varnostnim omejitvam pri delu v omrežju, omejitvam pri uporabi strojne opreme in podobnim.

V tabeli 3 je prikazanih nekaj primerov uporabe »audit policy« orodja.

Tabela 3: Primer uporabe audit policy orodja
(Vir: Orbanić, 2005)

Težava	**Ukrep**
Poskus vdora z naključnim preskušanjem gesel	Vključimo spremljanje neuspešnih dogodkov pri »audit account logon events« in »audit logon events«.
Vdor z ukradenim geslom	Vključimo spremljanje uspešnih dogodkov pri »audit account logon events«. V zabeleženih dogodkih bomo težko razlikovali med prijavami pravih in lažnih uporabnikov. Poskušamo iskati nenavadno obnašanje, kot so prijave ob nenavadnih urah, ko ne pričakujemo prijav na sistem.
Napačna uporaba administrativnih pravic s strani uporabnikov, ki jih imajo	Vključimo spremljanje uspešnih dogodkov »audit account managment«, »audit policy change«,«audit privileged use«, »audit object access«in »audit system events«.
Izbruh virusa	Najbolje je, če uporabimo protivirusne programe. Sicer pa lahko opazujemo sumljive dogodke tako, da opazujemo dostope do datotek s končnicami EXE in DLL. Vključeno mora biti spremljanje uspešnih in neuspešnih dogodkov »audit object access« in »audit process tracking«. Potem poženemo sumljive programe in iz obvestil poskušamo najti sumljivo obnašanje, kot je nenavadno ustvarjanje in popravljanje datotek, nenavadno zaganjanje procesov in drugo nenavadno obnašanje. Ker se pri tem beleži veliko dogodkov, uporabljajmo ta način le, ko aktivno pregledujemo sistem. Če pustimo beleženje vklopljeno tudi med uporabo sistema, ga s tem lahko znatno upočasnimo.
Neustrezni dostopi do datotek	Če želimo spremljati neustrezne dostope do datotek, vključimo spremljanje uspešnih in neuspešnih dogodkov pri »audit object access«. Na datotekah/mapah pa nastavimo, katere uporabnike/skupine bomo dejansko spremljali.

Linux

Za Linux kot večopravilni operacijski sistem je razumljivo, da bo na njem teklo več procesov hkrati.

Za spremljanje in upravljanje s procesi je v operacijskem sistemu na voljo kar nekaj pripomočkov, nekaj pa je tudi ukazov, ki jih lahko izvajamo iz ukazne lupine in so skupni večini različic operacijskega sistema Linux. Takšni ukazi so npr. ps, top, nice, kill.

Ukaz ps nam na zaslonu izpiše seznam procesov. Za vsak proces se izpiše njegov pid - številka procesa, imena terminalov, s katerih so bili procesi pognani. Za vsak proces se potem izpiše še čas, ki ga je procesor porabil in ukaz.
Več informacij dobimo z uporabo parametra -l (ps -l); npr. informacijo o roditelju procesa (ppid) in prioriteti, s katero se proces poganja. Temu stikalu lahko dodamo stikalo -a, ki izpiše tudi procese drugih uporabnikov in -x, ki izpiše procese, ki jih je pognal sam sistem (procesi brez nadzornega terminala). Ukaz iz kombinacije vseh parametrov bi se nato glasil ps –auxl.

Za porabo procesorskega časa lahko uporabimo ukaz top. Ta ukaz nam v realnem času prikazuje seznam najbolj aktivnih procesov. Za vsak proces podaja tudi odstotek uporabljenega pomnilnika in procesorskega časa.
Ukaz nam poda tudi informacijo o količini uporabljenega fizičnega in navideznega pomnilnika, število vseh procesov itd. Z uporabo tipkovnice lahko prikaz poljubno priredimo. S pritiskom na tipko u lahko prikažemo samo procese določenega uporabnika in s pritiskom na tipko c se nam izpiše tudi ukaz, s katerim je bil proces pognan ipd. Seznam in opis možnosti dobimo s pritiskom na tipko h. Stanje se osveži vsako sekundo. Iz programa gremo s pritiskom na tipko q.

Z ukazom nice lahko uravnavamo, koliko bo določen proces obremenjeval sistem. Primer: ukaz nice -n vrednost_nice.
Vrednost nice lahko zavzema vrednosti od -20 do 19, pri čemer -20 pomeni največje obremenjevanje sistema, vrednost 19 pa pomeni, da bo ukaz dobil najmanj procesorskega časa.

Za prekinitev procesa obstaja več načinov. Eden od načinov je pritisk na kombinacijo tipk Ctrl + c med samim izvajanjem programa.
Več se uporablja ukaz kill. Ukaz uporabimo na način kill [-sig] pid. Kjer je sig ime signala, pid pa identifikacijska številka procesa.
Z zaustavljanjem starševskega procesa se prenehajo izvajati tudi vsi procesi, izpeljani iz tega procesa. Izhod iz lupine praviloma prekine vse procese, ki smo jih zagnali v tej lupini.

Obstajajo tudi številna druga orodja, ki se razlikujejo najbolj po tem, da so uporabniku prijaznejša za uporabo.

Vsi dogodki v operacijskem sistemu Linux se beležijo v obliki datotek. Te datoteke so običajno shranjene v imeniku /var/log. Te datoteke lahko enostavno pregledujemo kar s preprostimi tekstovnimi urejevalniki, med katerimi je najbolj priljubljen urejevalnik vi. Vsebina log datoteke se razlikuje glede na to, za katero

storitev je namenjena. V glavnem pa log datoteke vsebujejo datum nastanka dogodka, povzročitev dogodka in njegov izvor.

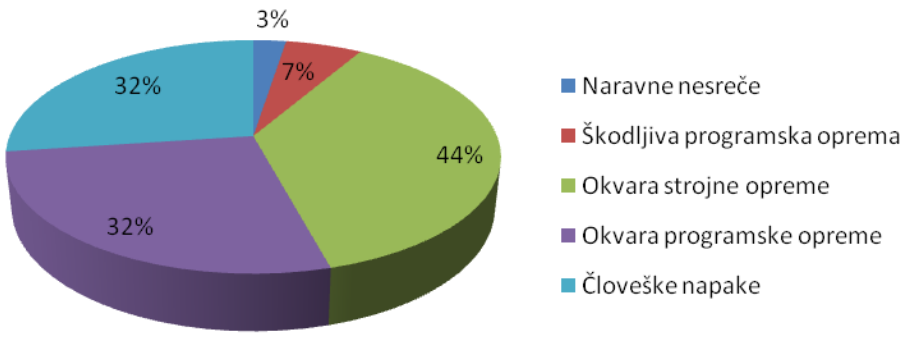
2.4.2 Varnost podatkov

V današnji informacijsko usmerjeni družbi sta varnost in ohranjanje razpoložljivosti računalniških podatkov ključnega pomena. Vedno večja vloga, ki jo imajo digitalne informacije, zahteva povečan nadzor nad tem, kako so ti podatki hranjeni in zaščiteni. Varovanje digitalnih podatkov je zahtevna naloga, še posebno, če se podatki nahajajo na več strežnikih, na delovnih postajah, v oddaljenih pisarnah po vsem svetu in na številnih prenosnikih (istor.net).

Podatki so najpomembnejši del vsakega informacijskega sistema. Varovanje podatkov je izziv, s katerim se srečujemo vsi uporabniki, posebej pa podjetja. Zaradi hitrega ritma življenja in prepričanja, da te vrste stroškov ne potrebujemo, velikokrat podatke varujemo neredno oziroma nekakovostno. Tega dejstva se običajno zavemo šele takrat, ko jih izgubimo. Na njihovo izgubo ali okvaro lahko vplivajo človeški, tehnični in naravni oziroma okoljski vzroki.

Na sliki 3 so prikazani najpogostejši vzroki izgube podatkov. Na prvem mestu so tehnične okvare, sledijo okvare in napake programske opreme in napake, ki jih povzročajo ljudje s svojimi dejanji. Med nekoliko manj pogostejše vzroke za izgubo podatkov, prištevamo še škodljivo programsko opremo in naravne nesreče.

Kljub temu, da so naravne nesreče najmanj pogoste, jih lahko predvidimo. Velikokrat si mislimo: nam se to ne bo zgodilo. To je na žalost največja iluzija, s katero živimo in mnogokrat to ne velja samo za varovanje podatkov. Če optimistično verjamemo, da se nam naravna nesreča ne bo zgodila, pa vselej lahko predvidimo nesreče zaradi malomarnosti ali nerodnosti (Telemach).



Slika 3: Najpogostejši vzroki za izgubo podatkov
(Vir: Online Data Backup Solutions)

Nekaj dejstev v zvezi z izgubo podatkov:

- 94% podjetij, ki utrpi večjo izgubo podatkov, propade, 43% jih po izgubi podatkov sploh ne nadaljuje s poslovanjem, 51% podjetij pa zaprejo v dveh letih.

- 7 od 10 malih in srednje velikih podjetij, kjer je prišlo do večje izgube podatkov, propade v enem letu.

- 93% podjetij, kjer je prišlo do nedosegljivosti podatkov za 10 dni ali več, propade v manj kot 12 mesecih.

- 77% tistih podjetij, ki testirajo varnostne kopije na trakovih, je ugotovilo težave s trakovi.

Oblikovanje kakovostnega varnostnega načrta za varovanje podatkov ni tako enostavno, kot se zdi na prvi pogled. Načrtovanja in izvajanja varnostnega kopiranja podatkov se moramo lotiti načrtno in sistematično. Velikokrat se pomembnosti tovrstnega početja ne zavedamo, saj podatkov iz varnostnih kopij ne potrebujemo, vse dokler se z njimi kaj ne zgodi.

Večje organizacije izziv sprejmejo brez velikih težav. Za manjše organizacije in končne uporabnike pa stroški hitro postanejo obsežnejši, kot smo sprva predvidevali. Vzrokov za to je več. Potrebno je narediti primerno raziskavo in izbrati opremo, s katero bomo varovali podatke ter vlagali v nakup ustrezne strojne in programske opreme.

Namestitev opreme zahteva strokovni kader, kupljeno opremo moramo ustrezno fizično varovati, uporabnike pa ustrezno izobraziti ter spremljati, ali se varnostno kopiranje opravlja redno. Če smo se odločili za varovanje podatkov na prenosljivih medijih, moramo zagotoviti ustrezna sredstva za njihovo nabavo ter s časom ustrezno menjavati opremo zaradi zastarelosti. Stroški, povezani z vzdrževanjem in popravili opreme so nepredvidljivi.

Poleg vzpostavitve rešitve na lokaciji moramo za kakovostno varovanje podatkov nujno poiskati rezervno lokacijo. Podatki morajo biti varovani na razpršenih dislociranih lokacijah, da so povsem neodvisni od stanja naše opreme. Požar, poplave, potresi, kraja opreme ne ogrožajo naših podatkov. Rešitev moramo zasnovati na podlagi preizkušene in strogo namenske opreme z redundantnimi povezavami, redundantnimi energetskimi viri ter zrcaljenjem podatkov na dveh dodatnih oddaljenih lokacijah. Oprema in podatki morajo biti pod nadzorom 24 ur na dan, vse dni v tednu. To v največji možni meri onemogoči izgubo podatkov zaradi okvare oziroma poškodbe opreme. Vsako nepravilno delovanje strojne in programske opreme se odkrije in prične odpravljati takoj. Zaradi okvar strojne in programske opreme storitev varovanja nikakor ne sme biti motena. Oprema ter lokacije morajo imeti status varovanih območij, kar pomeni, da so nenehno pod nadzorom varnostne tehnične opreme in varnostnega osebja. Varovanje moramo izvajati v skladu s standardi ISO 27001. Opremo, s katero opravljamo varnostno kopiranje, moramo redno vzdrževati in nadgrajevati. Le tako lahko uporabnikom zagotovimo, da so podatki varovani z zadnjimi najboljšimi, svetovno preizkušenimi in priznanimi rešitvami. Priporočljivo je tudi, da podatke šifriramo in zavarujemo s pristopnim geslom, tako da so dostopni samo pooblaščenim osebam (Jančigaj, 2007).

Varnostno kopiranje in arhiviranje podatkov

Pomena varnostnega kopiranja in arhiviranja podatkov se zaveda sleherni uporabnik osebnega računalnika, a nanj pogosto pomisli šele takrat, ko je že prepozno. Zagotovo k temu pripomore zamudnost in kompleksnost tega sicer zelo pomembnega opravila. Malo pa tudi neznanje, saj lahko z nekaj truda ta proces v celoti avtomatiziramo (Lampret, 2009).

Pogosto zamenjujemo oz. enačimo pojma varnostno kopiranje in arhiviranje podatkov. Pri varnostnem kopiranju (angl. backup) podatke ščitimo pred spremembami, pretvorbami, brisanjem ali koruptiranjem, medtem ko gre pri arhiviranju (angl. archive) za dolgoročno hrambo podatkov, ki se več ne spreminjajo.

Načela varnostnega kopiranja podatkov se v zadnjih letih niso bistveno spremenila. Vidnejši spremembi sta shranjevanje podatkov na naprave z naključnim dostopom (angl. disk based backup) in tehnologija za kontinuirano zaščito podatkov (angl. continuous data protection). Tračne knjižnice z zaporednim dostopom do podatkov so najbolj razširjen način shranjevanja podatkov. Dosegajo lahko visoke hitrosti in veliko kapaciteto. Slabost te tehnologije je zanesljivost robotike, pogonov in medijev ter zaporedni dostop do podatkov, kar velikokrat onemogoča hitro vračanje podatkov. Zato jih počasi že nadomeščajo naprave z naključnim dostopom do podatkov, ki jih imenujemo diskovne ali virtualne tračne knjižnice. Slednje so zanesljivejše in omogočajo hitrejše shranjevanje ali restavriranje podatkov.

Diskovno tehnologijo lahko pri varnostnem kopiranju podatkov uporabimo na več načinov. Prvi je uporaba tehnologije JBOD (Just a Bunch Of Disk), kar pomeni uporabo običajnih trdih diskov, ki so priklopljeni direktno na strežnik za centralizirano varnostno kopiranje podatkov. Drugi je uporaba diskovne knjižnice (angl. Disk Library ali Virtual Tape Library), ki se priklopi direktno na podatkovno omrežje SAN. Posebnost diskovne knjižnice je v tem, da se je programska oprema za varnostno kopiranje podatkov ne zaveda. Proti njej se predstavlja za tračno knjižnico. Kljub vrsti ključnih prednosti diskovne tehnologije pred tračno moramo razmišljati tudi o varovanju podatkov za primer katastrofe na primarni lokaciji (požar, poplava, potres, itd.). Ker podatkov z diskovne knjižnice ne moremo iznašati, je potrebno za iznos uporabiti tračne medije ali zagotoviti replikacijo oziroma kopiranje med diskovnimi knjižnicami, ki se nahajajo na ločenih lokacijah.

Varovanje v realnem času oz. kontinuirano varnostno kopiranje podatkov (angl. continuous data protection) omogoča varovanje podatkov v realnem času. To pomeni, da se v realnem času zajame vsaka sprememba na pomnilniškem podsistemu, kar kasneje omogoča vzpostavitev v poljuben čas, do sekunde natančno. S pomočjo posebnih naprav lahko zagotavljamo kontinuirano zaščito vseh operacijskih sistemov ali aplikacij. Tak način zaščite podatkov je primeren za strežnike in aplikacije, ki jih zaradi varnostnega kopiranja podatkov ne smemo obremenjevati, zanje pa potrebujemo kontinuirano zaščito podatkov in možnost instantne vzpostavitve v poljuben čas. Drug način uporabe CDP je na nivoju operacijskih sistemov. Ideja teh posebnih agentov izhaja iz prepričanja, da varnostno kopiranje enkrat dnevno preprosto ne zadostuje. Na določenih

dokumentih se spremembe lahko dogajajo zelo pogosto, cilj pa je, da se zaznajo takoj ter se hkrati tudi ustrezno zavarujejo.

Testiranje integritete je bistvenega pomena, saj varnostne kopije potrebujemo predvsem v neugodnih situacijah. Načrti za okrevanje so pomemben del načrta za neprekinjeno poslovanje organizacij. Načrt za okrevanje natančno določa vse postopke in aktivnosti, ki jih je potrebno v kritičnih situacijah izvesti.

V IT okolju se za varnostno kopijo običajno omenja le tista, ki je narejena na tračno enoto in pod točno določenimi pogoji. Domači uporabniki in manjša podjetja, ki si ne morejo privoščiti investicije v drage sisteme varnostnega kopiranja podatkov, se zato najpogosteje poslužujejo enega od sledečih načinov:

- varnostno kopiranje podatkov, prenesenih na disk v drugem računalniku,
- varnostno kopiranje podatkov na zunanji mrežni disk (po možnosti vsaj 2 diska v RAID polju),
- arhiviranje podatkov na CD/DVD medije,
- varnostno kopiranje na USB ključke ali zunanje USB trde diske.

Pri shranjevanju podatkov na medije je problematična tudi življenjska doba zapisa na njih, ki je med drugim odvisna od samega shranjevanja medijev, kakovosti medijev in rokovanja z njimi. Priporočljivo je, da berljivost medijev vsake toliko časa preverimo ter čez čas podatke prekopiramo tudi na nove medije.

Nobena od teh metod ne zagotavlja visoke stopnje varnosti podatkov. Problem je predvsem v fizični lokaciji medija z varnostno kopijo. Danes se veliko uporabljajo metode, kjer se podatki shranjujejo na oddaljene lokacije. Zelo priljubljeno je t.i. hranjenje podatkov v oblaku. Podatki so v primeru, da govorimo o »javnem« oblaku shranjeni na lokaciji oz. na več različnih lokacijah izven podjetja. Lahko pa postavimo tudi »zasebni« oblak, če želimo podatke hraniti v podjetju. Seveda imajo tudi te tehnologije določene slabosti. Problematično je recimo samo pošiljanje in vračanje podatkov iz oddaljenih lokacij, kjer moramo poleg varnosti podatkov zagotoviti tudi varno povezavo med prenosom le-teh. Problem lahko nastane tudi pri pošiljanju in vračanju velike količine podatkov, saj sam prenos traja običajno dlje kot v lokalnem omrežju. Vprašati pa se moramo tudi, če lahko ponudniku zaupamo svoje podatke (Merljak, 2009).

Varnost podatkov v operacijskem sistemu Windows

V operacijskem sistemu Windows so dovoljenja za dostop do podatkov močno odvisna od datotečnega sistema, ki ga uporabljamo. Trenutno se največ uporablja datotečni sistem NTFS (New Technology File System), ki omogoča tudi največ dovoljenj na mapah in datotekah.

Dovoljenja v NTFS datotečnem sistemu lahko nastavljamo lokalno ali pa za zaščito map in dokumentov v skupni rabi. V primerjavi z dovoljenji skupne rabe nam lokalna nudi številna dodatna dovoljenja. Na voljo so naslednja osnovna dovoljenja:

- poln nadzor (uporabniki lahko vidijo vsebino mape ali datoteke, spreminjajo obstoječe datoteke in mape, ustvarjajo nove datoteke in mape ali zaganjajo programe v mapi);

- spreminjanje (uporabniki lahko spreminjajo obstoječe datoteke in mape, ne morejo pa ustvarjati novih);
- branje in izvajanje (uporabniki lahko vidijo vsebino obstoječih datotek in map ter lahko zaganjajo programe v mapi);
- branje (uporabniki lahko vidijo vsebino mape ter odpirajo datoteke in mape);
- pisanje (uporabniki lahko ustvarjajo nove datoteke in mape ter spreminjajo obstoječe datoteke in mape).

Poleg teh dovoljenj poznamo še posebna dovoljenja:

- poln nadzor, ki omogoča dodeljevanje dovoljenj tudi ostalim uporabnikom;
- prečkanje mape omogoča ali prepoveduje premikanje preko omejene mape do posameznih datotek in map v okviru omejene mape v hierarhiji map. Izvajanje mape omogoča ali zavrača delovanje programske (izvršljive) datoteke;
- naštevanje map in branje podatkov omogoča ali zavrača ogled imena datotek in podmap znotraj mape ter ogled in branje podatkov v datotekah;
- atribut za branje omogoča ali prepoveduje ogled osnovnih atributov;
- branje razširjenih atributov omogoča ali prepoveduje ogled razširjenih atributov datoteke ali mape;
- ustvarjanje datotek omogoča ali prepoveduje ustvarjanje datotek znotraj mape;
- pisanje podatkov omogoča ali prepoveduje spreminjanje datoteke in pisanje čez obstoječo vsebino;
- ustvarjanje map omogoča ali prepoveduje ustvarjanje podmap znotraj mape. Dodajanje podatkov omogoča ali prepoveduje spreminjanje končnega dela datoteke;
- atributi za pisanje in razširjeni atributi se nanašajo na pravice spreminjanja teh atributov;
- brisanje podmap in datotek dodeljuje pravico za brisanje podmap in datotek, tudi v primeru, če dovoljenje za brisanje določeni podmapi oziroma datoteki ni bilo dodeljeno;
- dovoljenje za branje omogoča ali prepoveduje dovoljenje za branje datotek ali map;
- spreminjanje dovoljenj omogoča ali prepoveduje spreminjanje dovoljenj nad določeno datoteko ali mapo;
- prevzem lastništva omogoča ali prepoveduje prevzem lastništva nad določeno datoteko ali mapo.

Datoteke podedujejo dovoljenja od mape. Mape podedujejo nastavitve od nadrejene mape. Uporabnik lahko dostopa do mape le, če ima dovoljenje ali pripada skupini, ki ima dovoljenje za mapo. Dovoljenja so kumulativna. Prepoved ima največjo prioriteto in prednost tudi pred polnim nadzorom. Uporabnik, ki ima dodeljen poln nadzor nad mapo, lahko izbriše vse podmape in datoteke, ne glede na njegova dovoljenja do podmap in datotek. Uporabnik, ki ustvari datoteko ali mapo, postane tudi njun lastnik. Lastništvo je največje dovoljenje, ki mu omogoča spreminjanje dovoljenj. Tudi če administrator uporabnika odstrani iz seznama dovoljenih uporabnikov datoteke oziroma mape, lahko ta še vedno popravi dovoljenja. Administrator in člani privilegirane lokalne skupine administrators

lahko vedno prevzamejo lastništvo nad mapo ali dokumentom. Lastništvo lahko tudi dodelijo drugemu uporabniku.

Varnost podatkov v operacijskem sistemu Linux

V operacijskem sistemu Linux je običajno več kot en uporabnik, zato Linux ponuja mehanizem, znan kot dovoljenja datotek, ki ščiti uporabniške datoteke pred pregledovanjem drugih uporabnikov. Ta mehanizem omogoča datotekam in imenikom, da so »last« točno določenega uporabnika. Uporabnik, ki je ustvaril datoteke v svojem domačem imeniku, je tudi njihov lastnik in ima do njih dostop.

Linux tudi dovoljuje delitev datotek med uporabniki in skupinami uporabnikov. Če lastnik datotek želi, lahko onemogoči uporabnikom dostop do svojih datotek. Na večini sistemov je drugim uporabnikom dovoljeno branje svojih datotek, ne pa tudi njihovo spreminjanje ali brisanje.

Vsako datoteko si lasti določen uporabnik. Vendar so datoteke tudi last določene skupine (angl. group) uporabnikov sistema. Vsak uporabnik se ob kreiranju uporabniškega računa dodeli vsaj v eno skupino. Sistemski administrator lahko podeli uporabniku dostop do več kot ene tovrstne skupine.

Skupine navadno določa vrsta uporabnikov, ki dostopajo do računalnika, na primer na šolskem sistemu Linux so lahko uporabniki razdeljeni v skupine učenci, učitelji, administrativni delavci in gostje. Obstaja tudi nekaj sistemsko definiranih skupin (kot sta skupini bin in admin), ki jih uporablja sam sistem za nadzor dostopa do virov. Dovoljenja so razdeljena v tri glavne oddelke: branje, pisanje in izvajanje. Ta dovoljenja so lahko dana trem razredom uporabnikov: lastniku datoteke, skupini, kateri pripada datoteka in vsem uporabnikom, ne glede na skupino.

Dovoljenje za branje pusti uporabniku brati vsebino datoteke ali v primeru imenikov izpis vsebine imenika. Dovoljenje za pisanje dovoljuje uporabniku pisanje ali spreminjanje datoteke. Pri imenikih dovoljenje za pisanje dovoljuje uporabniku ustvarjanje novih datotek ali brisanje starih datotek v tem imeniku. Končno, dovoljenje za izvajanje dovoljuje uporabniku pogon datoteke kot programa ali skripta ukazne lupine.

Poglejmo primer, ki demonstrira dovoljenja datotek. Z uporabo ukaza »ls – l« se prikaže »dolgi« izpis imena datoteke, vključno z dovoljenji za uporabo te datoteke.

drwxr--r-- 5 ucenec users 16384 Apr 20 12:58 besedilo.doc

Prvo polje v izpisu predstavlja dovoljenja za uporabo datoteke, tretje polje vsebuje lastnika datoteke (ucenec), četrto je skupina, kateri datoteka pripada (users) in zadnje polje je mapa z imenom (besedilo.doc). To datoteko si lasti učenec, ki pripada skupini »users«. Niz drwxrwxr-x po vrsti našteva dovoljenja, dana lastniku datoteke, skupini datoteke in vsem ostalim.

Prvi znak niza dovoljenj predstavlja oziroma pove, ali gre za imenik ali datoteko. Znak »d« pomeni, da je to datoteka. Naslednji trije znaki (»rwx«) predstavljajo dovoljenja, podeljena lastniku datoteke. Črka »r« pomeni »branje« (angl. read),

črka »w« pomeni »pisanje« (angl. write) in črka »x« izvajanje (angl. execute). Torej, uporabnik učenec ima dovoljenja za branje, pisanje in izvajanje datoteke besedilo.doc.

Naslednji trije znaki (»r--«) predstavljajo dovoljenja skupine do uporabe datoteke. Skupina, ki si lasti to datoteko, se imenuje »users«. Ker se tukaj pojavlja le »r«, lahko vsak uporabnik, ki pripada skupini »users«, bere to datoteko.

Zadnji trije znaki, tudi (»r--«), predstavljajo dovoljenja, podeljena vsem uporabnikom sistema (razen lastniku datoteke in uporabnikom skupine »users«). Prisoten je le »r«, zato lahko drugi uporabniki berejo datoteko, a ne morejo vanjo pisati ali je izvajati.

Dovoljenja za dostop do datoteke so odvisna od dovoljenj za dostop do imenika, v katerem je datoteka. Na primer, če so dovoljenja datoteke nastavljena na rwxrwxrwx, drugi uporabniki ne morejo dostopati do datoteke, razen če imajo bralni ali izvajalni dostop do imenika, v katerem je datoteka.

Če bi želeli omejiti dostop do vseh svojih datotek, bi lahko nastavili dovoljenja svojega domačega imenika na -rwx. Na ta način noben drug uporabnik nima dostopa do našega imenika, datotek in imenikov v njem. Se pravi, če želimo sploh dostopati do datoteke, moramo imeti izvajalni dostop do vseh imenikov po poti datoteke in dovoljenje za branje (ali izvajanje) same datoteke.

Običajni nabor dovoljenj za dostop do datotek je -rw-r--r--, kar omogoča branje datoteke drugim uporabnikom, a brez vsakih sprememb. Običajni nabor dovoljenj za imenike je - rwx r - x r - x, kar omogoča drugim uporabnikom sprehod po imenikih, a brez ustvarjanja ali brisanja datotek v njih. Če želimo obdržati druge uporabnike čim dlje od naših datotek, nastavimo dovoljenje datoteke na –rw, ki bo preprečevala vsem drugim uporabnikom dostop do datoteke. Podobno nastavitev dovoljenj imenika na –rwx prepreči vstop drugim uporabnikom v ta imenik.

Poleg standardnih imamo v Linux sistemih tudi nekaj dodatnih opcij za spreminjanje dovoljenj na datotekah. Najprej so to nastavitveni biti »suid«, »guid« in »sticky bit«. »Suid« (set user id) in »sgid« (set group id) omogočata uporabnikom izvajanje datotek s pravicami lastnika datoteke ali njegove uporabniške skupine. Brez teh nastavitev se pravice na datotekah izvajajo s pravicami uporabnika, ki jih izvaja. Zaradi varnosti je bolje na sistemu imeti čim manj takšnih datotek ali pa vsaj takšnih, katerih lastniki so višje nivojski uporabniki. »Sticky bit« (uporablja se tudi izraz saved text bit) se uporablja za zaščito datotek ali imenikov. Datoteke, ki ima postavljen »sticky bit«, ne more brisati nihče drug razen njen lastnik, lahko pa jo ostali v skladu s pravicami pregledujejo, spreminjajo ter izvajajo. Podobno je, če »sticky bit« postavimo na določen imenik. Uporabniki, ki imajo do njega dostop, lahko vanj pišejo, brisanje pa je omogočeno le lastniku tega imenika.

Tipično je na Linux sistemih lastnik datoteke eden sam, zato se zna pojaviti težava, če želimo to datoteko dovoliti tudi kateremu izmed ostalih uporabnikov. To lahko sicer storimo tako, da dodelimo dovoljenje celotni uporabniški skupini ali pa kar vsem ostalim, ne moremo pa to storiti za posameznega uporabnika. Linux v

ta namen podpira razširjene ACL (access control lists) pravice, ki omogočajo pravice tudi takšnim uporabnikom, ki niso direktno povezani s tisto datoteko ali imenikom.

2.4.3 Omrežna varnost

Zagotavljanje sistemske in podatkovne varnosti je le del v mozaiku procesa zagotavljanja informacijske varnosti. S pojavom računalniškega omrežja, predvsem pa s pojavom interneta, je postalo zagotavljanje informacijske varnosti zelo resen in vsesplošni problem. Ni težko zagotoviti varnosti računalniku, ki nikoli ni bil in nikoli ne bo priključen v takšno ali drugačno omrežje in ga po možnosti uporablja vedno isti uporabnik. Ampak takšne situacije danes ni več. Praktično so vsi aktivni računalniki danes priključeni v lokalno in tudi v globalno omrežje, kjer imajo na voljo vse storitve, ki jih internet ponuja. Zavedati se moramo, da nam uporaba omrežnih storitev, poleg številnih prednosti, prinaša tudi slabosti, kjer so v ospredju predvsem številne nevarnosti.

Grožnje, ki pretijo računalniškemu omrežju, lahko razdelimo na pasivne in aktivne. Pasivne grožnje so tiste, ki niso neposredno vključene v sam proces izmenjave podatkov. Med takšne grožnje štejemo prisluškovanje vsebini omrežnega prometa in analizo omrežnega prometa. Aktivne grožnje aktivno vplivajo na komunikacijski proces in jih zato tudi lažje zaznamo. Aktivne grožnje so npr. maskiranje podatkov, nepooblaščeno podvajanje omrežnega prometa, nepooblaščeno spreminjanje omrežnega prometa, ohromitev strežnika in podobno.

Pri zagotavljanju omrežne varnosti moramo omeniti tudi pojma, kot sta zagotavljanje zasebnosti in verodostojnosti podatkov. Zasebnost podatkov pomeni, da ima vanje vpogled samo tisti, ki so mu namenjeni, vsem ostalim pa je vpogled onemogočen. Verodostojnost dokumenta zagotavljamo s svojim lastnoročnim podpisom. Lastnoročni podpis ima na dokumentu dva različna pomena. Podpis pomeni, da je dokument istoveten, to je tak, kot je bil takrat, ko smo ga podpisali. Pomeni pa tudi, da se strinjamo z njegovo vsebino. Kadar sta izpolnjeni obe funkciji, govorimo o verodostojnosti dokumenta.

Za zagotavljanje omrežne varnosti imamo na voljo številna orodja in pripomočke. Nekatere izmed njih smo opisali v nadaljevanju.

Arhitektura in delovanje omrežja

Večina omrežij je organiziranih kot zaporedje plasti ali nivojev, pri čemer je namen vsake plasti nuditi določene storitve za potrebe plasti na enem nivoju višje. Delovanje plasti lahko opišemo z mehanizmom odjemalec strežnik. Posamezna komunikacijska plast na enem računalniku skrbi za komunikacijo z isto ležečo plastjo na drugem računalniku. Pravila in odgovori, ki se pri tej komunikaciji uporabljajo, se imenujejo komunikacijski protokoli (Brezavšček, 2008).

Največje in najbolj uporabljeno omrežje internet deluje na skupku protokolov TCP/IP, ti pa temeljijo na nekoliko predelanem referenčnem modelu OSI. Podobno kot internet deluje tudi intranet. Intranet je manjša, pogovorno rečeno tudi žepna

različica interneta. Za razliko od interneta lahko v intranetu dostop kontroliramo in je dovoljen le končnemu številu uporabnikov.

Model OSI je sestavljen iz naslednjih sedmih plasti:

- fizična plast ima na skrbi prenos podatkov prek prenosnega medija in zagotavlja standardno strojno priključevanje sistemov na ta prenosni medij;
- povezovalna plast ima poleg glavne plasti dodan tudi rep, kjer so dodane informacije, namenjene odkrivanju napak pri prenosu prek prenosnega medija;
- omrežna plast je zadolžena za usmerjanje paketov skozi topologijo omrežja,
- transportna plast skrbi za storitve, ki omogočajo prestop podatkov od uporabnika v transportni sistem in nazaj;
- plast seje je namenjena storitvam, ki podpirajo logično povezovanje oddaljenih procesov med seboj;
- predstavitvena plast je zadolžena za zaščito in združljivost predstavitve podatkov v različnih računalniških okoljih;
- aplikacijska plast vsebuje standardne aplikacije, brez katerih si težko predstavljamo informacijski sistem.

Model TCP/IP je sestavljen iz štirih plasti, ki so podrobneje opisane v tabeli 4.

Tabela 4: Model TCP/IP

Plasti	**Protokol**	**Opis**
Aplikacijska plast	SMTP, FTP, HTTP, Telnet, TFTP,…	To je sloj, kjer imajo aplikacije dostop do omrežja.
Transportna plast	TCP (Transmission Control Protocol) UDP (User Datagram Protocol)	TCP služi kontroli prenosa podatkov, ter omogoča prenos podatkov med aplikacijami. UDP skrbi za nepovezavno komunikacijo in tako ne zagotavlja, da bodo poslani podatki prispeli. Aplikacije, ki ponavadi uporabljajo UDP, pošiljajo majhno količino podatkov naenkrat. Za zanesljivo pošiljanje podatkov je odgovorna aplikacija.

Plasti	Protokol	Opis
Internetna plast	IP (Internet Protocol) ARP (Address Resolution Protocol) ICMP (Internet Control Message Protocol) IGMP (Internet Group Management) Protocol	V tej plasti protokoli enkapsulirajo okvirje protokolov lokalnih omrežij v internetne datagrame in zaženejo vse potrebne usmerjevalne algoritme. Štirje protokoli so najpomembnejši na internetnem sloju: IP, ARP, ICMP in IGMP. IP je odgovoren za naslavljanje in usmerjanje paketkov med računalniki in omrežji. ARP služi za povezavo med strojnimi in logičnimi (IP) naslovi strojne opreme računalnikov in drugih sistemov v istem fizičnem omrežju. ICMP pošilja sporočila in sporoča napake glede pošiljanja paketa. IGMP uporabljajo računalniki IP, da sporočajo imena skupine za oddajanje več sistemom (angl. multicast), to je računalnikom in
Plast omrežnega vmesnika	Ethernet, FDDI, Token Ring	Je vmesnik med omrežno arhitekturo (kot je na primer Token Ring ali Ethernet) in internetno plastjo. Plast omrežnega vmesnika sestavljajo protokoli lokalnih omrežij (npr. Ethernet, token ring in FDDI), ki jih je TCP/IP zmožen povezati v prostrano omrežje s svojimi protokoli na višjih plasteh.

Požarna pregrada

Požarna pregrada (angl. firewall) je orodje, ki zagotavlja filter za pakete, katere sprejemamo v omrežje ali napravo in pakete, katere pošiljamo iz omrežja oziroma naprave (Kizza, 2009).

Požarna pregrada je lahko samostojna naprava ali programska oprema, ki teče na drugem računalniku in pregleduje omrežni promet, ki prehaja skozenj. Prehod je mogoč na osnovi posebnih pravil, ki dovolijo ali prepovejo prehod.

Osnovna funkcija požarne pregrade je uravnavanje prometa med računalniškimi omrežji z različno stopnjo zaupanja. Tipičen primer je internet kot omrežje, kateremu ne zaupamo in naše interno omrežje z visoko stopnjo zaupanja. Obstaja pa še omrežje z vmesno stopnjo zaupanja, umeščeno med internet in omrežje, kateremu zaupamo in katerega razumemo kot neko varovano oziroma demilitarizirano območje (angl. demilitarized zone DMZ). Pomembna je pravilna konfiguracija požarne pregrade. Običajna varnostna praksa je “privzeto-prepovedano” (angl. default-deny) nabor pravil, kar pomeni, da so dovoljene samo omrežne povezave, katere eksplicitno dovolimo. Takšna nastavitev zahteva detajlno poznavanje in razumevanje mrežnih aplikacij, zato se včasih raje uporabi

praksa "privzeto-dovoljeno" (angl. default-allow) nabor pravil, kar pomeni, da so vse povezave dovoljene, razen eksplicitno prepovedanih. Taka konfiguracija povzroča nenamerne, nenadzorovane oziroma neželjene mrežne povezave.

Poleg običajnih požarnih pregrad poznamo tudi osebne požarne pregrade. Osebna požarna pregrada se od konvencionalnega pojmovanja požarne pregrade razlikuje predvsem po obsegu. Osebne požarne pregrade so tipično razvite in prilagojene za uporabo pri končnih uporabnikih. Uporabljajo se za zaščito osebnega računalnika, na katerem so nameščene.

Mnoge požarne pregrade so primerne za nadzor mrežnega prometa tako, da vsakič ko zaznajo neko zahtevo ali mrežni promet, opozorijo uporabnika in nato ustrezno prilagodijo varnostno politiko. Osebne požarne pregrade lahko tudi zagotovijo nek nivo zaznavanja poizkusov vdorov, programska oprema pa ob sumu poizkusa vdora blokira povezavo.

Osnovne funkcije

Politika sprejmi/zavrni (angl. accept/deny), uporabljena v požarni pregradi, mora temeljiti na varnostnih politikah organizacije. Obstajata dve temeljni varnostni politiki oziroma načina delovanja požarnih pregrad:

- zavrni vse, kar ni eksplicitno dovoljeno, pri čemer požarna pregrada zavrne ves promet in onemogoči vse mrežne storitve, razen tistih, ki so posebej specificirane;
- dovoli vse, kar ni eksplicitno prepovedano, pri čemer je dovoljen ves promet in vse mrežne storitve, razen tistih, ki so na listi prepovedanih.
- Na osnovi teh politik skušamo doseči sledeče cilje:
- ves promet v in iz varovanega omrežja mora prehajati skozi požarno pregrado;
- prehaja lahko samo avtorizirani promet na osnovi organizacijske varnostne politike;
- požarna pregrada mora biti imuna za poizkuse vdorov, kar dosežemo z uporabo varnega sistema z varnim operacijskim sistemom.
- Ko so politike in cilji implementirani v požarno pregrado, je ta sposobna:
- zaščititi varovano omrežje pred vdori in vplivi;
- zavarovati dostop oziroma preprečiti nenadzorovano odtekanje pomembnih informacij preko omrežnih povezav;
- preprečiti nepooblaščeno in nenadzorovano uporabo virov, s katerimi razpolaga organizacija;
- omogočati pooblaščenim razne nadzorovane povezave in načine dostopa, kot je npr. VPN (angl. virtual privat network).

Vrste požarnih pregrad

Požarne pregrade se pogosto uporabljajo tudi za nudenje različnih varnostnih storitev – omogočajo nadzorovane načine dostopa pooblaščenim do določenih virov oziroma uporabo teh virov. Obstajajo različni tipi požarnih pregrad. Za razumevanje teh je najbolje, če pogledamo, katere vrste varnostnih storitev omogočajo požarne pregrade na različnih plasteh (angl. layers) protokola TCP/IP.

Požarne pregrade, razdeljene glede na storitve oziroma tipe storitev, ki jih nudijo na različnih nivojih mrežnih protokolov, prikazuje tabela 5.

Tabela 5: Varnostne storitve požarnih pregrad po posameznih plasteh (Vir: orbit-computer-solutions.com)

Nivo	**Storitev**
Aplikacijski (angl. Application)	Proxy strežnik, encryption, Application level gateways
Transportni (angl. Transport)	Filtriranje paketov (TCP, UDP, ICMP)
Omrežni (angl. Network)	NAT, IP filtriranje
Povezovalni (angl. Data)	Filtriranje na podlagi MAC naslovov
Fizični (angl. Physical)	N/A (may not be available)

Prvi tip požarne pregrade je usmerjevalnik, ki deluje na principu preverjanja oziroma filtriranja paketov TCP, UDP in ICMP (angl. packet inspection or filtering router). Pri tem uporablja zbirko pravil za odločanje o prehodu ali blokadi prehoda paketov. Strojna oprema takega usmerjevalnika je lahko preprost računalnik z več mrežnimi vmesniki – karticami ali pa sofisticiran računalnik z več funkcionalnostmi. Paketi so sprejeti (angl. accept) ali zavrnjeni (angl. reject) na osnovi specifičnih politik, ki temeljijo na varnostnih politikah organizacije. Ta tip požarne pregrade deluje predvsem na omrežnem in povezovalnem nivoju OSI modela. Če paket ustreza nekemu pravilu, potem je glede na to sprejet ali zavrnjen, v nasprotnem primeru pa pošlje ICMP sporočilo pošiljatelju paketa.

Uporabljata se dva tipa filtriranja paketov:

- Statično (angl. static) oziroma »stateless«, ki se uporablja pri full duplex ali dvosmerni komunikaciji. Pri tem tipu se upoštevajo striktna pravila filtriranja. Pravila se nanašajo samo na informacijo, vsebovano v paketih. Kontekst ni pomemben.
- Pri drugem tipu filtriranja – »statefull«, ki se ravno tako uporablja pri »full duplex« komunikaciji, pa je pomemben kontekst. Za vsak paket se preverja čas in stanje, v katerem se nahaja povezava med odjemalcem in strežnikom. Kateri tip bomo uporabili, je odvisno od varnostne politike, sprejete v organizaciji. Princip preverjanja oziroma filtriranja paketov temelji na IP naslovih, številkah vrat, ACK (Acknowledgement bitih) in ISN inicialnih sekvenčnih številkah, na TCP, UDP in ICMP glavah paketov in aplikacijah, ki se lahko pojavijo na katerem koli od protokolnih nivojev.

Drugi tip požarne pregrade je t.i. zastopniški strežnik za preverjanje aplikacij oziroma aplikacijska požarna pregrada (angl. application inspection proxy server). Strežnik uporablja posebno programsko opremo, ki zagotavlja prehod paketov na osnovi posebnih pravil za overjanje. Princip temelji na poznanih storitvah. Namesto filtriranja na osnovi IP naslovov, številk vrat in številk sekvenc, kar lahko povzroči blokiranje nekaterih storitev v sicer varovanem omrežju, če npr. poizkušamo doseči neko specifično storitev, je mogoče filtrirati promet na osnovi poznanih storitev v organizaciji. Filtri so definirani tako, da prepuščajo samo pakete iz dobro poznanih aplikacij iz okolja v omrežje organizacije in zavrnejo vse ostale pakete. Poenostavljeno – proxy strežniki (v nadaljevanju namestniški

strežnik) delujejo tako, da najprej prestrežejo zahtevo računalnika oziroma naprave iz notranjega omrežja po uporabi neke aplikacije in jo posredujejo ponudniku oziroma viru (angl. destination), ki je običajno nekje na spletu. Toda, preden jo posredujejo, zamenjajo IP naslov naprave z nekim drugim (svojim) naslovom in šele potem pošljejo paket naprej. V obratni smeri, pri sprejemu odgovora od spletnega strežnika, pa namestniški strežnik najprej preveri paket, potem pa zamenja lasten IP naslov v paketu z internim IP naslovom računalnika oziroma naprave, katera je poslala zahtevo.

Sodobni namestniški strežniki omogočajo tri osnovne funkcionalnosti:

- »Host IP address hiding« – pri tem gre za zamenjevanje delov paketov (header), ki vsebujejo IP naslove računalnikov v varovanem omrežju.
- »Header destruction« – pri tem gre za avtomatično zaščito, ki jo uporabljajo nekateri namestniški strežniki za ”uničevanje” delov paketov TCP, UDP in IP naslovov v paketih. Vse naslove se zamenja z enim samim – naslovom namestniškega strežnika, ki je edini viden v zunanjem omrežju.
- »Protocol enforcement« – pri tem gre za to, da vsak namestniški strežnik deluje kot strežnik za vsakega uporabnika in to za vsako aplikacijo posebej na svojih vratih (angl. ports). Skupnih vrat se ne uporablja.

Obstajata dva modela oblikovanja aplikacijske požarne pregrade:

- pozitivni varnostni model, ki temelji na pozitivnem vedenju uporabnikov in sprotni vsakokratni verifikaciji uporabniških zahtev in
- negativni varnostni model, ki temelji na vnaprej definirani bazi nesprejemljivih vzorcev oziroma razpoznavnih oblik napadov.

Tretji tip so posebni strežniki za overjanje in strežniki za vzpostavitev virtualnih privatnih omrežij (angl. virtual privat networks - VPN). VPN so posebne kriptirane povezave v privatna – varovana omrežja, za samo povezavo pa kot infrastrukturo uporabljajo javna omrežja. Gre v bistvu za sistem kriptiranja, ki vključuje tudi Point-to-point Tunneling Protocol (PPTP), Layer 2 Tunneling protocol (L2TP) in IPSec kot nosilec Point to Point Protocol (PPP) framov skozi internet. Možne so različne izvedbe VPN. Za povezavo enega oddaljenega računalnika v omrežje organizacije ali pa za povezavo dveh lokacijsko ločenih omrežij. Mnoge požarne pregrade omogočajo VPN zaščito, ki teče vzporedno z ostalimi overjanji in nadzornimi režimi na strežniku.

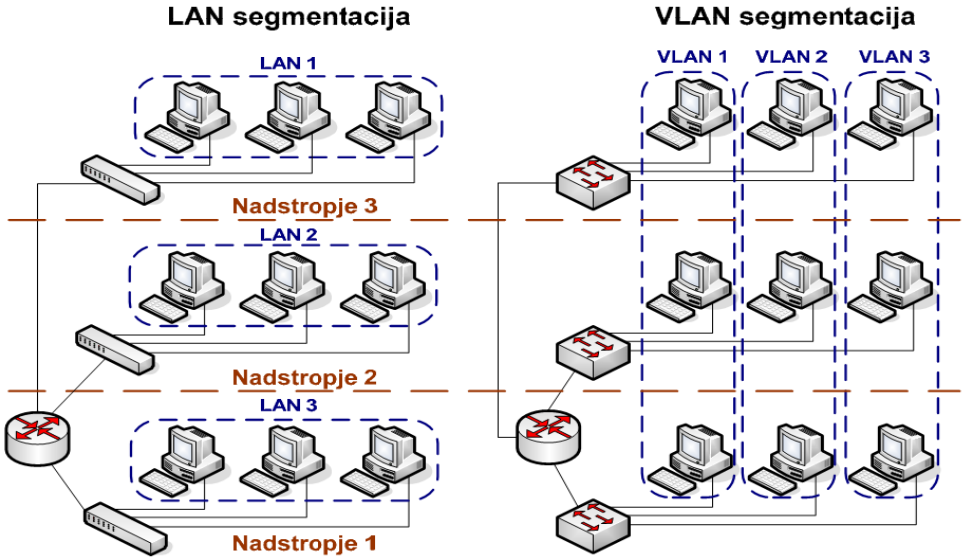
Četrti tip požarnih pregrad so požarne pregrade za mala poslovna ali domača omrežja (angl. small office or home SOHO). To so relativno majhne požarne pregrade, ki povezujejo le nekaj osebnih računalnikov preko HUB-ov, stikal ali celo usmerjevalnikov na eni strani na nek širokopasovni modem (npr. DSL) ali ethernet kabel na drugi strani.

Peti tip pa je NAT filter. V omrežju ima vsak računalnik oziroma vsaka delujoča naprava svoj IP naslov. Če so ti naslovi statični, je za hekerje še posebej enostavno npr. zasesti računalnik in ga uporabiti za določene nadaljnje napade. NAT filtri skrivajo naslove varovanega omrežja pred zunanjim omrežjem. Delujejo podobno kot namestniški strežniki. Vsi notranji strežniki v varovanem omrežju so iz zunanjega omrežja dostopni samo prek enega javnega IP naslova.

Navidezno lokalno omrežje (VLAN)

VLAN je komutacijsko omrežje, ki omogoča logično segmentacijo uporabnikov, ne glede na njihovo fizično lokacijo. Logična topologija omrežja je tako neodvisna od fizične oziroma geografske postavitve. Na primer, vse delovne postaje in strežnike, ki jih za svoje delo uporablja določena delovna skupina, je moč povezati v skupno VLAN omrežje, ne glede na njihovo fizično povezavo na omrežje in morebitno pomešanost te skupine z drugimi delovnimi skupinami. VLAN omrežje se vzpostavi s pomočjo programske opreme in ne s fizičnim preklapljanjem naprav ali povezav. VLAN omogoča logično segmentacijo LAN omrežja v različne domene razpršenega oddajanja (Zorko, 2007).

Zaradi logične segmentacije omrežja ni potrebno, da se delovne postaje nahajajo druga ob drugi. Primer takšne LAN in VLAN segmentacije prikazuje slika 4.



Slika 4: LAN in VLAN segmentacija
(Vir: Zorko, 2007)

Prednosti VLAN omrežja

Ena izmed prednosti VLAN omrežja je njegova hitrost. V omrežjih, kjer visok odstotek prometa predstavlja razpršeno oddajanje (angl. broadcast) ali oddajanje več prejemnikom (angl. multicast), lahko VLAN-i zmanjšajo potrebo po pošiljanju prometa k nepotrebnim destinacijam. Na primer, če je v broadcast domeni, ki jo sestavlja 10 uporabnikov, samo 5 uporabnikov, katerim je dejansko namenjen promet te domene, potem lahko s premestitvijo ostalih petih uporabnikov v ločen VLAN zmanjšamo promet v omrežju. V primerjavi s stikali potrebujejo usmerjevalniki več procesiranja prihajajočega prometa.

S povečevanjem prometa se skozi usmerjevalnik povečujejo tudi prehodni časi v usmerjevalniku, kar se odraža v zmanjšanju zmogljivosti omrežja.

Z uporabo VLAN-ov zmanjšamo število usmerjevalnikov, saj VLAN-i broadcast domeno vzpostavijo z uporabo stikal in ne usmerjevalnikov.

S pomočjo VLAN omrežja lahko kreiramo navidezne skupine za člane delovnih skupin, ki delujejo skupaj. Komunikacija med njimi je običajno zelo visoka, zato je smotrno vzpostaviti VLAN omrežje. Brez VLAN-a bi bila edina pot fizična združitev osebja delovne skupine, kar pa je pogosto nemogoče. Problem, ki se lahko pojavi pri formiranju navideznih delovnih skupin z VLAN-i, je implementacija osrednjega polja strežnikov, ki navadno predstavljajo serijo strežnikov in večjih enot za shranjevanje podatkov na skupni lokaciji, iz katere črpa informacije celotno omrežje. Prednosti skupne lokacije je veliko, saj je učinkoviteje, ceneje in lažje zagotavljati boljšo varnost podatkov, brezprekinitveno napajanje, varnostne kopije in primerno delovno okolje na enem mestu, kot pa imeti vire podatkov, razpršene na več lokacijah. Osrednje polje strežnikov lahko pri formiranju navideznih delovnih skupin povzroči težave, v kolikor strežnikov ni moč »postaviti« v več VLAN-ov hkrati. V tem primeru so strežniki postavljeni v samostojen VLAN in vsi ostali VLAN-i morajo za dostop do strežnikov preko usmerjevalnika, kar zmanjšuje zmogljivost omrežja (Zorko, 2007).

Logično združevanje uporabnikov, ki ni odvisno od njihove fizične ali geografske lokacije, omogoča enostavnejšo administracijo nad omrežjem. Velik strošek v omrežju predstavlja dodajanja, premestitve in spremembe uporabnikov. Z vsakim premikom uporabnika v LAN omrežju je potrebna nova namestitev ožičenja, novo IP naslavljanje in sprememba nastavitev stikal in usmerjevalnikov. Nekaj teh opravil je mogoče z uporabo VLAN omrežij poenostaviti. Če se uporabnik preseli na drugo lokacijo znotraj VLAN-a, ponovna nastavitev usmerjevalnika ni potrebna. V odvisnosti od tipa VLAN omrežja je moč posamezna administrativna dela zmanjšati ali odpraviti. Ob tem pa je treba omeniti, da se z implementacijo VLAN-ov, kljub poenostavitvi določenih opravil, posledično poveča kompleksnost nadzora nad omrežjem, saj VLAN-i dodajo dodaten sloj navideznih povezav, ki morajo biti upravljane v povezavi s fizičnimi povezavami.

Z možnostjo ločevanja uporabnikov v skupine veliko pridobimo tudi na sami varnosti omrežja. S tem lahko vključujemo različne uporabnike v omrežje in jim omogočamo dostop do virov in sredstev omrežja, hkrati pa jim omogočamo popolno avtonomnost znotraj posameznih VLAN skupin. Ker so VLAN-i logično osnovane skupine, ki se obnašajo kot fizično ločene enote, poteka komunikacija med VLAN-i preko usmerjevalnika. Ko pride do tovrstnega komuniciranja preko usmerjevalnika, se lahko uporabijo vse varnostne in filtrirne funkcije, ki jih običajno nudijo usmerjevalniki, ker imajo le-ti možnost »vpogleda« v informacije 3. nivoja OSI modela. V primeru uporabe neusmerjevalnih protokolov ni možna komunikacija med VLAN-i, pač pa le znotraj posameznega VLAN-a. Uporabnike, ki potrebujejo visoko stopnjo varnosti podatkov, lahko združimo v samostojen VLAN in noben uporabnik zunaj tega VLAN-a ne more komunicirati z njimi.

Sistemi za zaznavanje in preprečevanje vdorov

Sistem za zaznavanje vdorov je programska in/ali strojna oprema, namenjena zaznavanju nezaželenih poizkusov dostopa, manipuliranja in/ali onemogočanja računalniških sistemom, običajno preko omrežja.

Vdor je lahko posledica zunanjih ali notranjih napadalcev. Zaželeno je, da se zaznavanje vdorov izvaja v realnem času (Mukherjee, 1994).

Obstaja več vrst sistemov za zaznavanje vdorov, glede na to, kje so senzorji za zaznavanje postavljeni in kaj zaznavajo:

- Mrežni sistemi za zaznavanje vdorov (angl. Network intrusion detection system – NIDS) je samostojna platforma, ki zaznava vdore na osnovi opazovanja in analiziranja mrežnega prometa. Tak sistem lahko hkrati nadzira več naprav, priključenih v omrežje. Dostop do mrežnega prometa za te senzorje je lahko zagotovljen s priklopom na mrežne koncentratorje z uporabo zrcaljenja priključkov na mrežnem stikalu ali z drugo napravo, ki omogoča opazovanje vsega mrežnega prometa.
- Sistem za zaznavanje vdora na nivoju protokola zaznava poizkuse vdora za točno določen protokol (npr. za spletni strežnik). Običajno je nameščen na strežniku, na katerem je ciljni gostitelj za nadzorovani protokol ter nadzira promet med strežnikom in njegovimi odjemalci. Prednost takih sistemov glede na NIDS je, da poznajo protokol, ki ga nadzorujejo in s tem lahko nudijo večjo zaščito.
- Sistem za zaznavanje vdora na nivoju protokola med aplikacijami se od prejšnjega sistema razlikuje po tem, da analizira promet med dvema aplikacijama. Tipičen primer uporabe je komunikacija med spletnim strežnikom in podatkovnim strežnikom.
- Sistem za zaznavanje vdorov na gostitelju je nameščen na gostiteljski napravi, na kateri zaznava vdore z analiziranjem sistemskih klicev, pregledovanjem aplikativnih dnevnikov, spremembe v datotečnem sistemu (spremembe izvršljivih datotek, spremembe datotek z gesli …) in druge aktivnosti na gostitelju.
- Hibridni sistem za zaznavanje vdorov kombinira dva ali več zgoraj naštetih pristopov.

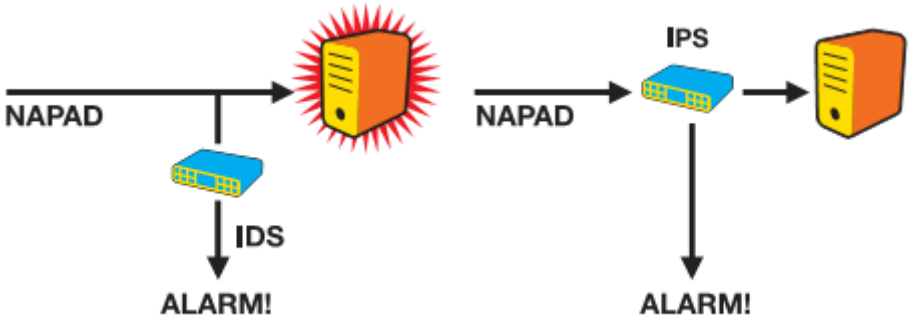
Glede na akcijo, ki jo sprožijo ob zaznavi vdora, imamo dve vrsti sistemov za zaznavanje vdorov:

- pasivni sistem in
- reakcijski sistem.

Pasivni sistem oz. IDS (Intrusion detection system) je sistem, ki spremlja pojav neustreznega ali celo škodljivega prometa v računalniškem omrežju in obvešča skrbnika omrežja o pojavu takšnega prometa. Slabost IDS sistema je ta, da nima možnosti aktivnega odziva. Lahko le resetiramo nezaželeno TCP povezavo, na nezaželene ICMP ali UDP pakete pa se ne moremo odzvati.

Reakcijski sistem oz. IPS (Intrusion prevention system) je sistem, ki odkriva neustrezen ali celo škodljiv promet v omrežju in postopa skladno z vnaprej definirano politiko. IPS natančno pregleduje pakete, prepozna več kot 100 različnih protokolov, povezuje se "inline" in ima možnost blokiranja vseh vrst prometa.

IDS opazuje promet v omrežju in pošilja opozorila o morebitnih napadih, IPS pa se nahaja na taki lokaciji znotraj omrežja, da lahko takoj aktivno blokira promet, kadar zazna poskus napada. Postavitev IPS in IDS sistema v omrežje prikazuje slika 5.



Slika 5: Postavitev IDS in IPS v omrežje
(Vir: Lubej, 2006)

Znana svetovalna hiša Gartner je v svojem poročilu 11. junija 2004 objavila, da so IDS sistemi že v zatonu in da je IPS za prihodnost nepogrešljiv (Antič, 2005).

Varnost brezžičnih omrežij

Brezžična oz. WLAN omrežja trpijo vse nevarnosti žičnih omrežjih in še dodatne nevarnosti zaradi uporabe brezžičnega medija. Signal WLAN omrežij se lahko širi tudi po prostorih, kjer si tega ne želimo. Tako lahko pride do prisluškovanja ali celo do nepooblaščenega dostopa do omrežja. Zato je potrebno poskrbeti za ustrezno overjanje, v posameznih primerih pa tudi za šifriranje podatkov. Pri vstopu v WLAN omrežje se mora uporabnik identificirati, da mu ponudnik omogoči storitev. Seveda tudi uporabnik želi zanesljivo vedeti, kam se je priključil. Ker uporabniki v WLAN omrežjih nimajo fizičnega dostopa do omrežne opreme, se morajo prepričati, da se povezujejo na pravo dostopno točko.

V zvezi z varnostjo v WLAN omrežjih moramo upoštevati tudi ostale varnostne parametre, kot npr. zagotavljanje integritete sporočil, varovanje pred napadi ipd. Če so brezžična omrežja pravilno konfigurirana, lahko zagotavljajo primerno varnost. Njihova slabost je prav gotovo ta, da niso samostojno upravljana, poleg tega pa ne omogočajo zaščite pred napadi z zavrnitvijo storitve DOS (Denial of Service).

Za zaščito v brezžičnih omrežjih se najpogosteje uporabljajo standardi WEP, WPA in WPA2 ter RADIUS protokol.

WEP

Standard IEEE 802.11 v osnovni različici predpisuje za zagotavljanje varnosti uporabo protokola WEP (Wired equivalent privacy). Osnovna značilnost protokola je statičen ključ, ki se uporablja za overjanje in šifriranje podatkov.

WEP zaščita temelji na šifriranju mrežnih paketov na povezovalni plasti (angl. data link layer) s (simetričnim) "skrivnim" ključem, ki mora biti znan vsem

uporabnikom neke točke dostopa (angl. access point - AP). Specifikacija 802.11b določa 40 bitno dolžino uporabniškega dela ključa (ali 5 znakov, 8 bitov × 5 znakov = 40 bitov), ki je nato združen s 24 bitnim inicializacijskim vektorjem (angl. initialization vector - IV). IV je naključno število, ki je del WEP algoritma in se izračuna ob vsakem pošiljanju paketa. Skupaj tvorita 64 bitni ključ. Glavni problem ključa je, da ga je s pasivnim opazovanjem radijskega prometa možno relativno hitro ugotoviti. Kljub podaljšanju ključa iz 40 na 128 bitov te velike pomanjkljivosti ni možno odpraviti, saj se čas, potreben za napad, povečuje linearno in ne eksponentno. Podobno je predpisan 128 bitni WEP ključ, pri katerem 104 biti (ali 13 znakov) pripadajo uporabniškemu delu ključa.

WEP izvaja overitev po naslednjem postopku:

- Odjemalec pošlje dostopni točki zahtevo po overitvi.
- Dostopna točka pošlje nešifrirano besedilo odjemalcu.
- Odjemalec to besedilo šifrira s svojim ključem.
- Dostopna točka dešifrira sporočilo s svojim ključem in na podlagi primerjave dešifriranega besedila z izvirnim overi ali zavrne odjemalca.

WEP uporablja za šifriranje in dešifriranje algoritem RC4, ki ne velja za posebno varnega. Samo dostopno točko je mogoče konfigurirati na tri načine:

- Ne uporabljaj WEP-a.
- Uporabljaj WEP za šifriranje.
- Uporabljaj WEP za overjanje in šifriranje.

Nekatere dostopne točke pa dovoljujejo tudi možnost uporabljaj WEP samo za overitev. Standard ne določa, kako potekajo drugi postopki v zvezi s ključem za overitev in šifriranje. Tako niso podani naslednji vidiki WEP-a:

- Generiranje deljenega skrivnega ključa.
- Distribuiranje teh ključev.
- Največje število ključev, ki jih dostopna točka dovoljuje.
- Življenjska doba ključev.

Zaradi omenjenega posamezne implementacije WEP izvajajo po svoje. Pri nekaterih implementacijah je potrebno vse izvesti ročno, nekatere pa to izvajajo samodejno, kar imenujemo dinamični WEP (angl. Dynamic WEP). Tipični dinamični WEP izvaja na takšen način generiranje in distribuiranje ključev. Ti storitvi običajno temeljita na overitvi, določeni s specifikacijo 802.1X. Ta overitev uporablja metode, kot je EAP-TLS, ki omogoča generiranje skrivnega ključa za vsakega odjemalca kot rezultat overitve.

Ranljivost WEP standarda

WEP uporablja RC4 šifrirni algoritem za generiranje neskončnega pseudo-naključnega ključa iz kratkega skrivnega ključa, ki ga nato uporabi pri XOR operaciji nad vsebino paketa. Tako dobljeno šifrirano vsebino paketa oddajnik pošlje sprejemniku. Ko sprejemnik prejme šifriran paket, se z neskončnim ključem (ki je generiran na prejemnikovi strani z RC4 algoritmom) ponovno uporabi operacija XOR nad šifrirano vsebino in tako dobi prvotno nešifrirano vsebino paketa. Neskončna RC4 ključa sta enaka (simetrična kriptografija) na oddajni in sprejemni strani, saj sta generirana iz istega skrivnega ključa (5 znakov pri 64-bitnem WEP-u). Tak način zaščite je ranljiv pri več vrstah napadov:

1. Če napadalec preseže dva paketa, šifrirana z istim ključem, je možno dobiti XOR obeh nešifriranih vsebin in s pomočjo tega ter statističnih napadov ugotoviti, kakšna je nešifrirana vsebina. Ko je enkrat znana vsebina enega paketa, je trivialno ugotoviti, kakšna je vsebina vseh ostalih.

2. Možno je tudi spreminjati vsebino šifriranega paketa, saj ob zamenjavi bita šifriranega sporočila pride do zamenjave tudi po XOR operaciji oz. v prvotni vsebini ni zagotovljena verodostojnost sporočila.

WEP ima sicer zaščito proti obema prej opisanima vrstama napadov, ki pa sta nepravilno implementirani. WEP za preverjanje verodostojnosti uporablja preverjanje integritete (ang. Integrity Check), natančneje CRC-32, ki je del kriptirane vsebine. CRC-32 je linearna funkcija, kar pomeni, da je možno izračunati bitno razliko dveh CRC-jev glede na bitno razliko med dvema vsebinama, nad katerima sta bila CRC-ja izračunana. To pomeni, da se zamenjava bitov vsebine deterministično odraža v spremembi bitov CRC-ja, ki jih je potrebno zamenjati, da bi zopet dobili pravilno vrednost, kar omogoča napadalcu, da zamenjuje bite vsebine in hkrati popravlja CRC.

Za izogibanje šifriranju vsebine z vedno istim neskončnim ključem pa WEP uporablja inicializacijski vektor, iz katerega v kombinaciji s skrivnim ključem algoritem RC4 generira neskončne pseudo-naključne ključe. Inicializacijski vektor je nato dodan paketu, da je možno dešifriranje na sprejemni strani. Vendar pa majhno število inicializacijskih vektorjev (dobrih 16 milijonov) pomeni, da se bodo ti relativno hitro začeli ponavljati. To omogoča napadalcu, da zbere dva paketa, šifrirana z istim ključem in napravi statističen napad, ki mu vrne nešifrirano vsebino. Razmere so dejansko še slabše, saj je v primeru dveh uporabnikov v omrežju, ki uporabljata isti skrivni ključ, verjetnost pojave paketov, šifriranih z istim ključem, še večja. Torej, z dovolj velikim številom zbranih paketov in uporabo naprednih statističnih algoritmov lahko zelo hitro ugotovimo skrivni ključ. Pred pojavitvijo teh algoritmov je moral napadalec zbrati okoli 10 milijonov paketov, kar je lahko trajalo tudi nekaj dni v omrežjih z majhnim prometom. Danes pa je ta številka precej nižja. V najboljšem primeru 250 tisoč paketov z enoličnim IV za 64 bitni WEP ključ in 500 tisoč do 1 milijon za 128 bitni WEP ključ. Da je zaščita res nična, so prikazali tudi strokovnjaki ameriške agencije FBI v svoji demonstraciji, kjer so z uporabo aktivnega napada razbili 128 bitni WEP ključ v pičlih 3 minutah.
Številne slabosti standarda WEP so bile povod za razvoj novega standarda, imenovanega WPA, ter številnih ostalih varnostnih metod, ki se lahko uporabijo kot dodatni varovalni mehanizem.

Standarda WPA IN WPA2

WPA je zgodnja različica varnostnega standarda 802.11i, ki ga je za nadomestitev WEP razvila WiFi Alliance oktobra 2003. Standard WPA omogoča relativno visoko stopnjo zaščite uporabniških podatkov in dostop do omrežja le avtoriziranim uporabnikom. WPA temelji na algoritmu TKIP (Temporal key integrity protocol) in overjanju po standardu 802.1X. Dolžina ključa v algoritmu TKIP je 128 bitov, pri čemer gre za dinamične ključe, ki se jih distribuira s pomočjo strežnika, ki skrbi za overjanje. Z dodatno uporabo protokola EAP (Extensible authentication

protocol) je omogočena uporaba digitalnih potrdil, unikatnih uporabniških imen, gesel, pametnih kartic ipd.

Šifrirni algoritem TKIP zelo poveča moč in kompleksnost šifriranja, zato je napad na tak sistem zelo zapleten, če ne celo nemogoč. WPA ima vgrajeno tudi zaščito pred zajemanjem in ponovnim pošiljanjem popravljenih podatkov, ki se imenuje MIC (Message integrity check). S pomočjo zahtevne matematične operacije se izvede primerjava MIC na strani oddajnika ter na strani sprejemnika. V kolikor MIC ni enak na obeh straneh, se pošlje zahteva po prekinitvi seje.

Pri razvoju standarda WPA niso pozabili na že obstoječo opremo, ki predhodno tega standarda ni podpirala. Vgradnja je mogoča v večino strojne opreme, ki ima WI-FI certifikat, bodisi z nadgradnjo strojne opreme (angl. firmware) ali samo s programskimi nadgradnjami. Standard WPA je na voljo v 2 oblikah uporabe. Enterprise je namenjena zahtevnejšim uporabnikom, predvsem organizacijam. Druga oblika Personal pa je namenjena manj zahtevnim uporabnikom in je tudi najbolj pogosto uporabljena pri posameznikih. Značilnost omenjenih načinov uporabe je naslednja:

- WPA Enterprise ponuja overjanje na podlagi strežnika RADIUS. Vsakemu uporabniku se dodeli edinstveni ključ, kar poleg visoke varnosti omogoča tudi visok nivo zasebnosti. Za kriptiranje se uporablja kriptirni algoritem TKIP, na podlagi katerega se tvorijo kriptirni ključi.
- WPA Personal za varno povezavo uporablja PSK (Pre-shared Shared Key), ki uporablja 8 do 64 znakovno geslo. Šibka PSK gesla lahko različni programi strejo v manj kot minuti. WPA je varna, kadar za PSK geslo uporabimo poln 64 znakovni šestnajstiški ključ.

WPA2 je ime za dokončan standard 802.11i, ki ga je septembra 2004 predstavila WiFi Alliance. WPA2 je zasnovan podobno kot standard WPA, le da namesto algoritma TKIP uporablja močnejši AES-CCMP (Advanced Encryption Standard - Counter Mode - MAC Protocol) algoritem, kar še dodatno povečuje varnost. Tudi standard WPA2 je na voljo v 2 oblikah uporabe. Prva (Enterprise) je namenjena zahtevnejšim uporabnikom, predvsem organizacijam. Druga oblika (Personal) pa je namenjena manj zahtevnim uporabnikom oz. posameznikom. Nadgradnja na standard WPA2 je odvisna od strojne opreme, pogosto pa je potrebna zamenjava le-te, saj nadgradnja pogosto ni mogoča. Za nadgradnjo na standard WPA2 je na voljo tudi tako imenovan »mešan« način delovanja (WPA2 Mixed Mode), ki podpira tako WPA kot WPA2. Omenjeni način delovanja je še posebej primeren takrat, ko nadgrajujemo, opravljamo prehod iz WPA na WPA2. V WPA2 Mixed Mode načinu delovanja dostopna točka omogoča uporabo algoritma TKIP in tudi algoritma AES. Kateri algoritem bo uporabljen pri komunikaciji, je odvisno od odjemalca, saj le-ta sproži zahtevo po uporabljenem algoritmu.

Kot pa je že za večino varnostnih mehanizmov značilno, da 100% varnosti ni, se je tudi v primeru uporabe standarda WPA pojavila slabost, ki vsaj nekoliko meče slabo luč na omenjeni standard. Govora je o standardu WPA-PSK, ki se tudi največ uporablja. S primernimi orodji je namreč možno prestreči štiristransko rokovanje EAPOL, ki se izvede med odjemalcem in dostopno točko. Nato pa je možno razbijanje ključa, ne da bi bili v stiku z omrežjem (offline) na podlagi ugibanja gesel oz. fraz. Omenjena metoda je uspešna le v primeru, kadar je kot ključ uporabljeno šibko geslo in je sestavljeno iz manj kot 8 znakov. Delo razbijanja

ključa je še toliko lažje, če je uporabljena neka splošno znana beseda, po možnosti še iz slovarja, saj ravno slovar z gesli služi kot podlaga za ugibanje gesel.

Radius

Radius (Remote Authentication Dial-In user Service) je protokol, ki omogoča centralizirano overjanje in avtorizacijo uporabnikov, ki dostopajo do omrežja. Strežnik omogoča tudi urejanje skrbništva nad računi uporabnikov. V prvotni obliki je bil razvit za kontrolo modemskega dostopa, danes pa se uporablja tudi za kontrolo dostopa pri brezžičnih omrežjih.

Uporabnik za dostop potrebuje svoje uporabniško ime in geslo. Te informacije se prenesejo do omrežnega vmesnika NAS (Network access server) preko PPP protokola (Point to Point Protocol). Omrežni vmesnik nato te podatke posreduje RADIUS strežniku. V kolikor so podatki pravilni in je zahteva za dostop odobrena, dodeli RADIUS strežnik uporabniku IP naslov in masko omrežja za protokol PPP ali vrata TCP za telnet.

RADIUS podpira razširjen protokol za overjanje (EAP – Extensible Authentication Protocol). Ta protokol omogoča uporabo različnih shem za overitev, med njimi javne ključe, Kerberos in pametne kartice (smart cards). Dva najpogostejša načina, ki ju omogoča EAP, sta EAP-MD5 in EAP-TLS. EAP-MD5 je običajni protokol izziv in odgovor (challenge-response) z algoritmom MD5.

2.4.4 Fizična varnost

Fizična varnost spada med zelo pomembne gradnike informacijske varnosti. Zagotavljanje fizične varnosti običajno ni ravno naloga skrbnikov informacijskih sistemov, nedvomno pa lahko ti s svojim znanjem in izkušnjami znatno pripomorejo k izboljšanju le-te.

Verjetno tudi ni računalničarja oz. skrbnika informacijskega sistema, ki bi lahko mirno spal, če bi vedel, da se njegov računalnik oz. ostali nahajajo v nezaščitenem prostoru. Še hujše pa je, če je na takšnem področju strežnik.

Varnostna politika na fizičnem nivoju bi nam morala biti najbolj jasna in naj bi povzročala najmanj težav. Na žalost pa se v realnosti izkaže, da je ravno tukaj največ pomanjkljivosti. Pri načrtovanju fizične zaščite moramo misliti o stvareh, kot so:

- Omejevanje vstopa v prostore. Obravnavati moramo tako obiskovalce kot tudi delavce podjetja. Obiskovalci ne smejo imeti nikakršnega dostopa do strežniške sobe, razen pod strogim nadzorom. Prav tako se tudi ne sme zgoditi, da se znajdejo sami v sobi z nezaščitenim računalnikom, ki ima dostop do poslovnih podatkov. Zaposleni naj bi načeloma dostopali samo do stvari in prostorov, ki jih uporabljajo med delom.
- Zaščita prostorov pred fizično škodo. Govorimo predvsem o škodi v primeru nesreče, kot sta požar ali poplava. Čeprav je to v veliki meri rešeno že z drugimi elementi (gradbeno dovoljenje, splošna protipožarna zaščita), moramo razmišljati o teh stvareh tudi v povezavi z delovanjem informacijskega sistema.

- Napotki za obnašanje zaposlenih. Uporabniki ne smejo puščati prazne in odprte pisarne z vklopljenim računalnikom, prijavljenim v sistem. Dokaj pogosta napaka uporabnikov je ravnanje s pomembnimi podatki, med katere sodi tudi ravnanje z gesli, zato uporabnike opozarjamo, naj listka z gesli ne lepijo na vidna mesta. Vsi taki napotki se slišijo smešno, še bolj smešno pa je vedeti, kako pogosto se jih ljudje ne držijo.
- Brezprekinitveno napajanje (UPS). Izpad elektrike in nenormalna zaustavitev računalnikov lahko povzročita izpad dela in napake v podatkih. Na fizičnem nivoju moramo razmisliti o tem, kateri računalniki so kritični in jih je treba priklopiti na naprave UPS. Te poskrbijo za pravilni izklop tudi v primeru izpada elektrike, v nekaterih primerih pa tudi za nemoteno delo v daljšem obdobju brez energije.

2.4.5 Organizacijska varnost

Organizacijsko varnost obravnava kodeks upravljanja varovanja informacij ISO/IEC 17799 in je namenjena organiziranju in upravljanju varovanja informacij v organizaciji.

Za zagotavljanje organizacijske varnosti se predlaga ustanovitev odbora oz. foruma, ki bo poskrbel, da bo stopnja varnosti ostala na želeni ravni. V tej fazi se določijo tudi odgovornosti za zaščito posameznih sredstev in izpeljavo posameznih postopkov. Določijo se tudi pravila za nabavo novih sredstev, potrebnih za obdelavo informacij. Treba je zagotoviti sodelovanje s strokovnjaki: bodisi zunanjimi ali notranjimi in skrbeti za stike z organi pregona, zakonodajnimi organi in ostalimi, tako da se lahko v primeru varnostnega incidenta takoj pridobi nasvet in se ustrezno odzove. Na tem nivoju se določijo tudi pogoji glede dostopa tretjih strank. Prav tako se pripravijo dogovori z zunanjimi organizacijami, ki bodo imele v upravljanju del informacijskega sistema, omrežja ali osebnih računalnikov (Kos, 2004).

Podpora vodstva podjetja je pri zagotavljanju organizacijske varnosti bistvenega pomena. Vodstvo podjetja mora pomagati:

- zagotoviti, da je cilj varovanja informacij jasen in v skladu z organizacijskimi zahtevami,
- oblikovati in pregledovati politiko varovanja informacij,
- pri učinkovitosti izvajanja politike varovanja informacij,
- zagotoviti jasno usmeritev in vidno podporo za upravljanje varnostnih pobud,
- zagotoviti sredstva, potrebna za informacijsko varnost,
- pri dodelitvi vlog in odgovornosti za informacijsko varnost v organizaciji,
- pri izobraževanju, usposabljanju in ozaveščanju o varnosti informacij,
- zagotoviti, da je izvajanje nadzora varnosti informacij usklajeno po vsej organizaciji.

Pomemben del pri obvladovanju organizacijske varnosti predstavlja varnostna politika informacijskega sistema.

Varnostna politika informacijskega sistema je celovit pogled na varnost informacijskega sistema in zajema vse dejavnike, organizacijska pravila in

postopke, ki kakorkoli vplivajo na varno in zanesljivo delovanje celotnega informacijskega sistema. Varnostna politika informacijskega sistema ima več elementov, ki se lahko prilagajajo glede na informacijski sistem organizacije. Nekateri tipični elementi varnostne politike informacijskega sistema so (Štrakl, 2003):

- seznam in varnostna klasifikacija vseh informacijskih virov,
- analiza varnostnega tveganja vsakega informacijskega sistema,
- organiziranost varovanja informacijskega sistema,
- dolžnosti, pristojnosti in odgovornosti za varovanje informacijskega sistema,
- varnostni elementi v povezavi s človeškimi viri (zaposlovanje, ozaveščanje, izobraževanje, usposabljanje…),
- upravljanje z informacijskimi sistemi (postopki in odgovornosti, načrtovanje in prevzem sistema, zaščita pred škodljivo programsko opremo…),
- uporaba elektronske pošte,
- uporaba storitev omrežja internet,
- upravljanje z nosilci podatkov,
- upravljanje omrežij,
- upravljanje z varnostnimi dogodki, incidenti in okvarami,
- dostop do informacijskega sistema (upravljanje dostopa, nadzor nad dostopom, oddaljen dostop…),
- razvijanje, naročanje, prevzemanje in načrtovanje programske in strojne opreme,
- načrtovanje neprekinjenega poslovanja,
- varnostne zahteve zunanjih izvajalcev storitev.

Varnostna politika ni nespremenljiva, saj jo je potrebno prilagajati spremembam v razvoju varnosti. Varnostna politika je od organizacije do organizacije različna, zato mora biti narejena za vsak informacijski sistem posebej. Vsako podjetje lahko varnostno politiko izdela po lastnih kriterijih in lastni metodologiji. Nekoliko lažja pot je, če se podjetje odloči, da bo izdelalo varnostno politiko informacijskega sistema v skladu s standardom ISO 17799, ki vključuje tematiko varnostne politike informacijskega sistema (Štrakl, 2003).

2.4.6 Odgovornosti in naloge sistemskega administratorja

Sistemski administrator ima veliko moči in odgovornosti, zato mora še posebej paziti na varnost sistemskega uporabniškega računa. Nekateri uporabniki namreč izkoristijo prvo priložnost, pri kateri se lahko v sistem prijavijo kot administrator. Ker ima administrator takšno moč nad sistemom, je potrebna določena stopnja zrelosti in samonadzora, da se uporablja sistemski račun, za kar je namenjen – za delovanje sistema.

V raziskavi, opravljeni med sistemskimi administratorji, je kar 67% sodelujočih priznalo, da so dostopali do informacij, ki niso bile povezane z njihovimi delovnimi nalogami. Zlorabo administrativnih gesel pri vohljanju za zaupnimi podatki pa je priznalo 41 % sodelujočih (CIO, 2010).

Kadar imamo opravka z zlonamernimi uporabniki, lahko postopamo na dva načina: lahko smo paranoični ali zaupljivi. Paranoični sistemski administrator navadno povzroči več škode kot koristi. V devetdesetih odstotkih, kadar uporabnik povzroča težave na sistemu (denimo, zapolnjuje uporabniško particijo z velikimi datotekami ali poganja več izvodov velikega programa), se uporabnik preprosto ne zaveda, da ustvarja problem. Kadar imamo opraviti z uporabniki, ki povzročajo potencialne težave, jih ne obtožujmo. Najbolje, da se z njimi pogovorimo in jih povprašamo o težavah, namesto da bi se spuščali v spore. Zadnja stvar, ki jo želimo, je, da bi se zamerili uporabniku. To bi sprožilo veliko sumov o nas, da morda sistema ne upravljamo pravilno. Če uporabnik misli, da mu ne zaupamo ali da ga ne maramo, nas lahko obtoži izbrisa datotek ali kršitve zasebnosti na sistemu. Če ugotovimo, da uporabnik poskuša »vlamljati« ali drugače namenoma škodovati sistemu, ga je potrebno opozoriti. V veliko primerih lahko ujamemo uporabnika »na delu« škodovanja sistemu. V tem primeru mu je treba povedati, da naj se to ne zgodi več. Če uporabnik s početjem ne preneha, smo lahko prepričani, da je bilo to storjeno namenoma. Kljub temu pa izkušnje kažejo, da je največkrat vzrok napaka uporabnika ali sistemska napaka.

Manj kot imamo postavljenih pravil, manj verjetno je, da bodo kršena. Tudi če so naša pravila popolnoma razumna in jasna, jih bodo uporabniki občasno še vedno prekršili, ne da bi to nameravali. To posebej drži za nove uporabnike, ki se uvajajo v sistem. Ko določimo pravila za uporabo našega sistema, se prepričajmo, da je pojasnilo za določen napotek jasno. Če ne, bodo uporabniki iznašli vse sorte ustvarjalnih načinov, da se bodo izognili pravilu in ne bodo vedeli, da ga kršijo.

3 INFORMACIJSKO-KOMUNIKACIJSKA TEHNOLOGIJA V ŠOLSTVU

Razvoj informacijsko-komunikacijske tehnologije je v zadnjih letih strahovito napredoval. Svet je postal odvisen od številnih možnosti, ki jih omenjena tehnologija ponuja. Uporaba računalnikov, interneta, intraneta ter vsega ostalega, povezanega s to tehnologijo, je postalo del našega vsakdana. Kljub temu, da na osnovnih šolah še vedno prevladuje »klasična« oblika pouka in poučevanja, si sodobna tehnologija zelo hitro utira pot tudi na tem področju.

Poleg vpliva na sam didaktični proces tehnologija še močneje vpliva na procese, ki tečejo vzporedno z njim. Med te uvrščamo recimo izdelavo šolskega urnika, elektronsko redovalnico, elektronske dnevnike, izobraževanje na daljavo, proces priprave na pouk in še bi lahko naštevali. Poleg vsega tega pa moramo omeniti tudi poslovni proces, ki je v osnovnih šolah kar nekako potisnjen v ozadje, kar pa seveda ni pravično, saj je njegova vloga prav tako zelo pomembna.

3.1 Informatizacija šolstva v Sloveniji

Slovenija je bila ena izmed prvih evropskih držav, ki je v letu 1993 zagotovila pogoje za dolgoročni sistematični preskok na področju uporabe informacijsko-komunikacijske tehnologije (IKT) pri poučevanju in učenju. Definirana so bila glavna tri področja vlaganja sredstev in izvajanja dejavnosti:

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

Vsa tri področja so bila neločljivo povezana, tj. niso bila obravnavana parcialno (npr. hkrati z dobavo opreme in izgradnjo omrežij je potrebno skrbeti za pripravo gradiv ter izvedbo seminarjev za učitelje itd). Poraba sredstev se ni načrtovala le z vidika porabe sredstev za eno izmed področij, ampak so se porabljala celovito (npr. izobraževanje za opremo, ki je šolam dosegljiva za uporabo).

V letu 1999 je bil ugotovljen vse večji prepad med tistimi učitelji, ki so IKT osvojili kot del življenja in dela šole, ter tistimi, ki IKT niso uporabljali niti za svoje delo, še manj pa pri delu z učenci.

V letu 2000 je bila pripravljena strategija informatizacije šolstva, s katerim bi se s približno 10 krat večjimi sredstvi izvajale široko zaznamovane dejavnosti, ki bi zajele praktično vse vzgojitelje, učitelje in ravnatelje, pa tudi učence in jih motivirale za uporabo IKT pri poučevanju in učenju ter hkrati povzročile nov dvig kakovosti pouka in drugih dejavnosti šole. Poleg tega bi z IKT učenci pridobili znanja in spretnosti za novo kvaliteto življenja (komunikacija, samoizobraževanje oz. vseživljenjsko učenje, iskanje in vrednotenje informacij…). Vendar za preskok niso bila zagotovljena ustrezna sredstva, še manj pa novi organizacijski modeli za izvajanje informatizacije šolstva na višjem nivoju. Bili pa so zagotovljeni pogoji za vzdrževanje stanja na vseh treh področjih.

Veliko rezultatov dosedanje informatizacije se lahko oceni kot uspešne, vendar pa proces informatizacije šolstva v Sloveniji še vedno živi vzporedno z običajnim življenjem vzgojno-izobraževalnih zavodov (v nadaljevanju VIZ) . Posledice tega so, da se informatizacija ne izvaja celovito, ampak v večini primerov le parcialno (šole nimajo potrebnega znanja, želje in ustrezne podpore).

Če primerjamo trenutno stanje VIZ v Sloveniji z ostalimi članicami EU, lahko ugotovimo, da smo primerljivi le na področju opremljenosti. Na področju uporabe in dostopnosti storitev pa je stanje precej slabše. Predvidevamo, da je takšno stanje neposredna posledica nezadostnega sistematičnega pristopa v preteklosti, ki je VIZ prisilil v iskanje in razvoj lastnih rešitev. Tak pristop je nujno vodil do razdrobljenosti, raznovrstnih rešitev, visokih obratovalnih stroškov in pomanjkljive informatizacije VIZ. Ocenjujemo, da bi bilo potrebno in smiselno dvigniti nivo informatizacije na področju podpore delovanja VIZ in prav tako na področju e-gradiv oziroma na področju e-učenja. Že programski svet za informatizacijo šolstva je predlagal, da se pristopi k celoviti informatizaciji VIZ, ker se bo v nasprotnem primeru razvojno zaostajanje v primerjavi z ostalimi državami EU še povečevalo.
Nezadovoljivo stanje informatizacije VIZ kliče k skupnemu sistematičnemu projektnemu pristopu vpletenih državnih organov in drugih akterjev, skupaj z združevanjem kadrovskih in finančnih virov.

Zaradi velikega števila deležnikov, visokih investicijskih vložkov, potrebnih organizacijskih sprememb in zaradi drugih značilnosti področja je problematika zelo kompleksna, zato bo za uspešno vodenje informatizacije VIZ potrebna močna podpora. Poleg nje je ključnega pomena zavezanost akterjev informatizacije VIZ k skupnim razvojnim ciljem. Tu ne gre pozabiti, da govorimo o javnem sektorju, da porabljamo denar državnega proračuna in da se racionalizacija kot proces docela nikoli ne konča.

Večina šol ima svoja lokalna omrežja povezana v omrežje Arnes, ravno tako uporabljajo večino njihovih storitev. Šole so posebna skupina uporabnikov, saj imajo glede na razpoložljiva finančna sredstva in ob različni stopnji znanja razmeroma visoke zahteve po uporabi spletnih tehnologij za dostop do multimedijskih vsebin, videokonferenčnega povezovanja, projektnega sodelovanja, mobilnosti in uporabi porazdeljenih virov ter inovativni uporabi IKT v učnem procesu. Želijo preizkušati in uporabljati nove storitve, pri tem pa potrebujejo zelo veliko podpore (Ministrstvo za izobraževanje, znanost, kulturo in šport, 2006).

3.2 Akademska in raziskovalna mreža Slovenije - Arnes

Akademska in raziskovalna mreža Slovenije, v nadaljevanju Arnes, je javni zavod, ki z zagotavljanjem omrežnih storitev organizacijam s področja raziskovanja, izobraževanja in kulture omogoča njihovo povezovanje ter sodelovanje med seboj in s sorodnimi organizacijami v tujini. Arnes opravlja enake storitve kot nacionalne akademske mreže v drugih državah, ki se danes običajno imenujejo National Research and Education Network – NREN, saj njihovo področje delovanja vključuje poleg raziskovalnega in razvojnega tudi izobraževalni sektor. V omrežje Arnes se povezujejo organizacije s področja raziskovanja, razvoja, izobraževanja in kulture. Skupno število uporabnikov se ocenjuje na približno 200.000. Ti

uporabniki uporabljajo tako storitve lokalnega omrežja svoje organizacije kot tudi posredno ali neposredno storitve omrežja Arnes (Arnes, 2010a).

V nadaljevanju bomo opisali infrastrukturo omrežja in nekaj najpomembnejših storitev na področju varnosti, ki jih Arnes nudi svojim uporabnikom.

3.2.1 Vloga in storitve Arnes-a

Pri uvajanju tehnologij in storitev sodeluje Arnes z Ministrstvom za visoko šolstvo, znanost in tehnologijo ter Ministrstvom za izobraževanje, znanost, kulturo in šport. S projektom računalniškega opismenjevanja, postavitve omrežij in izobraževanja učiteljev se je na terenu oblikovala neformalna skupina strokovno usposobljenih učiteljev, ki poznajo tako tehnologijo kot razmere v šolah posamezne regije. Ti učitelji svetujejo in pomagajo šolam na terenu ter so v nenehnem stiku z Arnes-ovo strokovno ekipo, s katero si izmenjujejo izkušnje in sodelujejo pri načrtovanju šolskih omrežij (Arnes, 2011b).

Med najširše uporabljene storitve, ki jih Arnes nudi svojim uporabnikom, so nedvomno internetne storitve. Precej skrbi in nenehne nadgradnje pa potrebujejo tudi osrednji strežniki, da lahko zagotavljajo varno, stabilno in hitro delovanje storitev. Izmed ponujenih storitev velja izpostaviti storitev gostovanja spletnih strani. Arnesovi uporabniki lahko uporabljajo t.i. gostovanje statičnih spletnih strani in gostovanje dinamičnih spletnih strani. Pri statičnem gostovanju lahko uporabniki spletne strani objavijo v HTML obliki, medtem ko lahko pri dinamičnem gostovanju uporabijo spletna orodja, ki omogočajo aktivno sodelovanje obiskovalcev spletne strani pri oblikovanju njene vsebine. Storitev podpira PHP in podatkovno bazo MySQL. Skrbniki lahko ustvarijo poljubno število podatkovnih baz, dostop imajo z vsemi administratorskimi pravicami. Arnes skrbi za vzdrževanje in posodabljanje operacijskega sistema in strojne opreme, dodeljuje vire, organizacija pa skrbi za svoje aplikacije. Kompleksna tehnična rešitev, ki deluje v ozadju, zagotavlja visoko stopnjo varnosti, uporaba pa ostaja preprosta (Arnes, 2011a).

Podobna storitev je gostovanje virtualnih strežnikov. Storitev je namenjena organizacijam in društvom z večjimi zahtevami, saj je omogočen dostop do strežnika z vsemi uporabniškimi pravicami. Na strežnik je že nameščen operacijski sistem, spletni strežnik, podatkovna baza in orodja za statistiko. Strežnik se lahko upravlja kot običajen Linux strežnik. Uporabnik za celoten strežnik skrbi sam, le strojno opremo vzdržuje Arnes. Poleg zagotavljanja visoke stopnje varnosti omogoča rešitev tudi zagotavljanje strojnih virov.

Osnovna storitev, ki jo Arnes ponuja svojim uporabnikom, je nudenje elektronske pošte. Arnes navaja, da se iz leta v leto veča količina prejetih in poslanih elektronskih sporočil, med katerimi je čedalje več nezaželenih oglasnih sporočil – t.i. vsiljene (angl. spam) pošte. Zaradi tega morajo nenehno nadgrajevati zaščito proti tovrstni pošti. Arnesovi strežniki naj bi v letu 2009 prejeli v obdelavo več kot milijon elektronskih sporočil na dan. Večina prejetih nezaželenih oglasnih sporočil je bila zavrnjena s t.i. tehniko »greylisting«. To je metoda, ki izloči sporočila, ker niso bila poslana v skladu s sprejetimi standardi. Takšne metode uporabljajo »spam« strežniki zaradi hitrejšega pretoka podatkov. Ostala elektronska sporočila so obdelana s sistemom strežnikov za izločanje virusov in nezaželenih sporočil

(AVS), ki sporočila analizira na osnovi nenehno rastoče baze znanja, ki vsebuje informacije o trenutno poznanih virusih in kompleksna pravila za prepoznavanje »spama«. Storitev AVS uporabnikom elektronskih predalov omogoča zavračanje elektronske pošte, ki vsebuje viruse in ponuja možnost izločanja nenaročenih sporočil iz prihajajoče elektronske pošte. Hkrati sistem izloča tudi okuženo pošto, ki jo uporabniki pošiljajo preko Arnesovega strežnika in tako ščiti naslovnike pred okužbami iz omrežja Arnes. Nivo zaščite si lahko uporabniki nastavijo po lastnih željah preko spletnega vmesnika. Storitev AVS je Arnes razvil v sodelovanju z Računalniškim centrom Instituta Jožef Stefan in temelji na odprtokodni programski opremi (Arnes, 2011a).

Arnes omogoča tudi šifriran prenos elektronske pošte. Uporabniki Arnes-a lahko uporabljajo šifriran prenos elektronske pošte med svojim računalnikom in Arnes-ovim sistemom za posredovanje elektronske pošte. Šifriran prenos pomeni, da se vsi podatki, tako uporabniška gesla kot tudi vsa vsebina elektronske pošte, prenašajo v šifrirani obliki, kar onemogoči prestrezanje podatkov. Le-to je še posebej pomembno pri uporabi javnih nezaščitenih brezžičnih omrežij. Pri šifriranem prenosu se uporabljata protokola TLS in SSL. Od leta 2007 naprej lahko uporabniki uporabijo tudi overjanje SMTP za dostop do Arnes-ovega poštnega strežnika in tako pošto pošiljajo preko Arnes-ovega sistema, ne glede na to, v katerem omrežju se nahajajo (Arnes, 2011a).

Zaradi vse večjega števila uporabnikov, ki morajo za uporabo določene storitve (npr. elektronska pošta) izkazati svojo istovetnost, npr. z uporabniškim imenom in geslom, je začel Arnes v letu 2009 pospešeno izvajati aktivnosti za uvajanje avtentikacijske in avtorizacijske infrastrukture (AAI). Omenjena infrastruktura omogoča enotnejši dostop do storitev na osnovi e-identitete, ki jo uporabniku izda domača organizacija (Arnes, 2011a).
Rešitev je zasnovana na naslednjih idejah:

- Uporabnik prejme eno uporabniško ime in geslo, ki je uporabno za dostop do različnih aplikacij, tako do spletnih storitev, ki jih nudi uporabnikova domača organizacija (npr. fakulteta) kot tudi do spletnih storitev, ki jih nudijo druge organizacije (npr. on-line podatkovne baze).
- Uporabnik se v sistem prijavi s pomočjo posebnega sistema na svoji domači organizaciji. Spletna aplikacija nikoli ne vidi njegovega gesla. Posamezne aplikacije dobijo vpogled zgolj v tiste osebne podatke uporabnika, ki so nujno potrebni za delovanje aplikacije. Uporabnik ima polno kontrolo nad prenosom osebnih podatkov.
- Podatke o uporabnikih se vnaša zgolj enkrat, in to v domači organizaciji uporabnika. Enotna infrastruktura za overjanje istovetnosti in avtorizacijo (AAI) vzpostavi okolje, kjer se preverjanje istovetnosti uporabnikov ter hranjenje njihovih osebnih podatkov izloči iz posameznih aplikacij in se izvaja na domači organizaciji uporabnikov.
- Aplikacije ohranijo funkcijo avtorizacije, vendar pri tem uporabljajo podatke, ki jih pridobijo od domače organizacije uporabnika.

Arnes je že od leta 1999 v okviru mednarodne projektne koordinacije European Schoolnet partner v projektih Evropske komisije iz akcijskega načrta Varnejši internet, ki promovira varnejšo uporabo interneta za otroke in mladostnike. Gre za koordinirane aktivnosti v vseh državah članicah EU, v Sloveniji projekte podpira Direktorat za informacijsko družbo na Ministrstvu za visoko šolstvo, znanost in

tehnologijo. V okviru tega akcijskega načrta Arnes od leta 2005 aktivno sooblikuje SAFE-SI, nacionalno točko osveščanja o varnejši rabi interneta. Od oktobra 2008 so vse aktivnosti iz tega načrta v Sloveniji združene v projekt SIP-SI, ki ga izvajajo Fakulteta za družbene vede Univerze v Ljubljani, Arnes in Zveza potrošnikov Slovenije, sofinancirata pa ga Generalni direktorat za informacijsko družbo pri Ministrstvu za visoko šolstvo, znanost in tehnologijo (Arnes, 2010b).

3.2.2 Omrežje Arnes za izobraževalne ustanove

Med pomembnimi varnostnimi storitvami, ki jih Arnes nudi izobraževalnim ustanovam, je tudi varna internetna povezava ter infrastruktura omrežja.

Arnes nudi izobraževalnim ustanovam varno povezavo do interneta, v kolikor je ta povezava na njihovi lokaciji možna. Ponekod namreč Arnes še ne more zagotavljati ustrezne povezave (npr. nekatera optična omrežja). Poleg dostopnosti pa je pogoj še ustrezna omrežna oprema (usmerjevalnik, omrežna stikala), ki jo šolam običajno zagotovi ministrstvo.

Usmerjevalnik, ki je pod nadzorom in upravljanjem tehničnega osebja Arnes, opravlja funkcijo požarne pregrade. Usmerjevalnik filtrira promet na podlagi izvora, od koder prihaja, naslova, kamor je namenjen, tipa prometa (protokola, internetne storitve) in še nekaterih drugih podatkov. Usmerjevalnik ne more nadzorovati vsebine prometa, količine prenesenih podatkov, trajanja sej, imen uporabnikov ipd. Novejši usmerjevalniki nudijo postavitev navideznega privatnega omrežja (angl. VPN), ki omogoča šifriranje prometa in overjanje uporabnikov, ki dostopajo do šolskega sistema.

Filter za šolski usmerjevalnik je definiran na podlagi podatkov o najbolj pogostih storitvah, ki se uporabljajo na šolah. Usmerjevalnik tako prepušča le tisti internetni promet, ki je potreben za delovanje izbranih storitev, ves ostali promet pa je zavrnjen. Tipično so na šolskem usmerjevalniku omogočene naslednje internetne storitve:

- uporaba Arnes-ovih imenskih (DNS) strežnikov,
- elektronska pošta (SMTP, IMAP in POP3),
- svetovni splet WWW (http in https),
- konferenčni sistem NEWS,
- prenos podatkov po protokolu FTP v pasivnem načinu,
- uporaba Arnes-ovih strežnikov za sinhronizacijo časa po protokolu NTP,
- uporaba orodij ping in traceroute,
- in po potrebi multimedijske storitve in »multicast«.

Poleg funkcije požarne pregrade omogoča usmerjevalnik tudi postavitev ločenih omrežij. Arnes priporoča delitev omrežja na pedagoški in administrativni del. S takšno delitvijo ločimo administrativni in pedagoški del omrežja ter s tem zavarujemo administrativni del pred nekaterimi nevarnostmi iz pedagoškega dela omrežja. Tako je npr. onemogočeno prisluškovanje (angl. sniffing) administrativnemu delu omrežja.

Glede na dejstvo, da Arnes zagotavlja internetno povezavo na več kot 500 osnovnih šolah (vseh osnovnih šol v Sloveniji je nekaj čez 800) in posledično skrbi

tudi za zaščito omrežja, lahko upravičeno trdimo, da ima Arnes zelo pomembno vlogo pri zagotavljanju omrežne varnosti v osnovnih šolah.

3.2.3 Eduroam omrežje

V današnjem času je čedalje večja potreba po brezžičnem povezovanju računalnikov in ostalih naprav z omrežjem. Šole lahko v ta namen same postavijo dostopne točke ter omogočijo uporabnikom dostop do omrežnih virov. Seveda je potrebno pri tem poskrbeti za primerno varnost. V primeru, da imajo šole primerno opremo (omrežna stikala, dostopne točke in strežnik), je sploh z vidika varnosti priporočljiva postavitev Eduroam omrežja.

Eduroam je federacija nekomercialnih omrežij WLAN, v katero je združenih 28 držav. Sestavljajo ga samostojna brezžična omrežja izobraževalnih in raziskovalnih ustanov, združena v sistem, ki svojim uporabnikom omogoča gostovanje v brezžičnih omrežjih v drugih (tudi tujih) organizacijah, vključenih v sistem. V Sloveniji je začel Eduroam delovati leta 2002 (Strosar, 2007).

V Eduroam omrežju je poskrbljeno za varnost in zasebnost uporabnikov. Celotno omrežje je zgrajeno z vrhunsko strojno opremo, ki mora zadovoljiti visoke tehnične zahteve. Za preverjanje istovetnosti se uporablja 802.1x protokol EAP-TTLS. Osnovna naloga protokolov 802.1x je, da omogočijo varno preverjanje istovetnosti, samo overjanje in avtorizacija pa se izvedeta v strežniku domače organizacije (npr. šole). Strežniki RADIUS skrbijo predvsem za usmerjanje zahtevkov po overjanju in avtorizaciji med gostujočim uporabnikom in domačim strežnikom.

Protokoli za preverjanje istovetnosti (EAP-TTLS, EAP-TLS, PEAP...) tečejo preden se uporabnik dejansko poveže v omrežje. Šele, ko se istovetnost uporabnika preveri, se odobri povezava na dostopno točko. Odjemalcu se nato dodeli naslov IP prek DHCP (Dynamic Host Configuration Protocol) in promet lahko steče. Po prijavi v omrežje se promet uporabnika pretaka prek brezžičnega omrežja do dostopne točke po protokolu WPA/WPA2 (oz. TKIP/AES), med dostopno točko in usmerjevalnikom pa poteka promet prek ožičenega omrežja (Strosar, 2007).

Pri postavitvi Eduroam omrežja je šolam v pomoč Arnes, ki testira posamezno brezžično opremo, nudi pomoč, vzdržuje vzorčne nastavitve in sistem Eduroam na brezplačni tehnološki osnovi Linux CentOS, OpenLDAP ter FreeRADIUS.

3.3 Državne iniciative na področju ozaveščanja o informacijski varnosti v šolstvu

V Sloveniji deluje kar nekaj institucij, ki ozaveščajo o informacijski varnosti učitelje, učence ter njihove starše. Temeljna naloga teh institucij je ozaveščanje o varni rabi interneta, ozaveščanje na področju varnosti omrežij, tehnična zaščita in varovanje omrežij ter storitev in varovanje osebnih podatkov ter zasebnost uporabnikov.

V nadaljevanju si bomo podrobneje ogledali naslednje projekte, ki skrbijo za ozaveščanje o informacijski varnosti:

- Projekt Center za varnejši internet »SAFE-SI«.
- Projekt »NASVET ZA NET«
- Projekt »VARNI NA INTERNETU«

3.3.1 Projekt »SAFE-SI«

Projekt Center za varnejši internet SAFE-SI izvajajo Fakulteta za družbene vede, Arnes, Zveza prijateljev mladine Slovenije in Zavod MISSS (Mladinsko informativno svetovalno središče Slovenije), financirata pa ga Generalni direktorat Connect pri Evropski komisiji in Ministrstvo za izobraževanje, znanost, kulturo in šport (Safe-si, 2012).

Center za varnejši internet SAFE-SI združuje tri komponente:
- SAFE-SI - ozaveščanje o varni rabi interneta in novih tehnologij,
- TOM TELEFON 116 111 - telefonsko linijo za pomoč mladim in njihovim staršem, ki se znajdejo v težavah, povezanih z uporabo interneta,
- SPLETNO OKO - točka za anonimno prijavo nelegalnih spletnih vsebin - posnetkov spolnih zlorab otrok (otroška pornografija) in sovražnega govora.

Aktivnosti Centra so namenjene štirim ciljnim skupinam: otrokom, mladostnikom, staršem in strokovnim delavcem (učiteljem, socialnim, mladinskim delavcem...). Vizija projekta je, da med izbranimi ciljnimi populacijami s sprotnim zagotavljanjem preverjenih informacij in nasvetov za varno rabo novih tehnologij v Sloveniji doseže visoko stopnjo ozaveščenosti o teh temah.

Tako so v poslanstvo projekta SAFE-SI zajete naslednje aktivnosti:
- vzdrževanje osrednje spletne strani kot baze znanja in pomoči za otroke, najstnike, starše in učitelje,
- izobraževanje učiteljev in drugih strokovnih delavcev za poučevanje in prenos vsebin varne rabe interneta,
- priprava in distribucija izobraževalnih gradiv (zloženk, brošur, didaktičnih iger ipd.) za vse ciljne skupine,
- izvedba delavnic za otroke in mladostnike, predavanj za starše, natečajev za šole,
- organizacija in udeležba na predstavitvah, konferencah, okroglih mizah, seminarjih, dogodkih,
- zagotavljanje medijske prisotnosti, priprava člankov in prispevkov za različne medije,
- organizacija in izvedba dogodkov in aktivnosti ob svetovnem dnevu varne rabe interneta (vsako leto drugi torek v februarju).

Projekt »SPLETNO OKO«

SPLETNO OKO je slovenska spletna prijavna točka, kjer lahko anonimno prijavimo otroško pornografijo in sovražni govor na internetu.

SPLETNO OKO deluje v okviru komunitarnega programa Varnejši internet plus in organizacije INHOPE. Kot člani svetovalnega telesa pri projektu sodelujejo tudi Vrhovno državno tožilstvo Slovenije in Policija ter predstavniki medijev in ostalih organizacij, ki aktivno delujejo na področju varovanja pravic otrok.

Projekt financira Generalni direktorat za informacijsko družbo pri Evropski komisiji, Direktorat za informacijsko družbo v okviru Ministrstva za visoko šolstvo, znanost in tehnologijo in partnerji - Univerza v Ljubljani, Fakulteta za družbene vede, Zveza potrošnikov Slovenije in Akademska in raziskovalna mreža Slovenije. Sodelovanje podobnih točk v Evropi se je izkazalo za učinkovit ukrep v boju za zmanjšanje nezakonitih vsebin na internetu. Slovenski uporabniki interneta lahko zdaj tudi sami z anonimnim poročanjem o obstoju potencialno nezakonitih vsebin prispevate k varnejšemu internetu (Spletno oko, 2012).

3.3.2 Projekt »NASVET ZA NET«

NASVET ZA NET je projekt Zveze potrošnikov Slovenije, sofinancirata ga Evropska komisija - Generalni direktorat za informacijsko družbo ter Ministrstvo za visoko šolstvo, znanost in tehnologijo - Direktorat za informacijsko družbo. Sodi v evropski projekt Varnejši internet plus. V projektu sodelujejo skupaj s Fakulteto za družboslovne vede, ki vodi slovensko točko osveščanj – SAFE-SI in Slovensko akademsko raziskovalno mrežo – Arnes. Projekt izvaja Zveza potrošnikov Slovenije, sodi v program Varnejši Internet Plus.

Projekt NASVET ZA NET je namenjen otrokom in staršem, ki iščejo pomoč ali informacije o tem, kako se zavarovati pred spletnim nadlegovanjem (angl. grooming) ali spletnim nasiljem (angl. cyberbullying), kaj narediti, če naletimo na spletne vsebine, ki nas vznemirijo ali kako ravnati v primeru neprijetne izkušnje pri uporabi interneta (Nasvet za net, 2010).

3.3.3 Projekt »VARNI NA INTERNETU«

Projekt VARNI NA INTERNETU izvaja Slovenski center za posredovanje pri omrežnih incidentih SI-CERT, ki deluje pod okriljem javnega zavoda Arnes. Projekt je zastavljen dolgoročno in naslavlja precej široko področje problematike informacijske varnosti. Aktivnosti projekta so usmerjene k doseganju sledečih ciljev (Varni na internetu, 2010):

- dvigniti stopnjo zavedanja ciljnih javnosti o različnih nevarnostih, katerim so izpostavljeni na spletu,
- informirati o varni uporabi spletnega bančništva,
- informirati o različnih oblikah spletnih prevar in ponuditi praktične rešitve, kako se zavarovati,
- informirati o varstvu osebne identitete v socialnih omrežjih.

3.4 Stanje in dobre prakse po svetu

Naj najprej kot zanimivost povemo, da smo največ prispevkov v zvezi z informacijsko varnostjo v šolah zasledili na področju Velike Britanije. Ugotovili smo, da tam za informacijsko varnost običajno skrbi ekipa ljudi, vsak izmed njih pa je zadolžen za določeno področje. Poleg tega ponekod to področje obvladujejo tudi zunanje organizacije. Sklepamo lahko, da je zaradi tega boljša tudi informacijska varnost. V raziskavi, ki so jo leta 2009 tam izvedli, je bilo namreč ugotovljeno, da ima večina šol že izdelano varnostno politiko oz. je le-ta v fazi izdelave. Izmed varnostnih pomanjkljivosti so izpostavili pomanjkljivo varovanje

podatkov. Ugotovili so, da je večina podatkov nezaščitenih, kar je še posebej nevarno na prenosnih računalnikih in prenosnih medijih (Saunders, 2009).

Dokaj podobno rešujejo težave v zvezi z informacijsko varnostjo tudi na šolah v Avstriji in Nemčiji. Za IKT in varnost skrbijo ekipe ljudi znotraj šole ali pa to delo opravlja zunanja organizacija. Ta postavi in vzdržuje rešitev (informacijski sistem), katerega nato upravljajo učitelji oz. nekdo izmed zaposlenih na šoli. Namenoma nismo uporabili izraza osnovna šola, saj osnovnošolskega izobraževanja v teh državah ne moremo povsem enačiti z našo osnovno šolo. V Veliki Britaniji ločimo obvezno (angl. primary) in srednje (angl. secondary) izobraževanje. V Nemčiji in Avstriji pa se starostna skupina otrok, ki pri nas obiskuje osnovno šolo, tam deli na osnovne (nem. Grundschule) in srednje šole (nem. Hauptschule).

Glede informacijskih sistemov, ki jih uporabljajo v šolah drugod po svetu, nismo zasledili enotne rešitve. Veliko šol uporablja že dokaj standardne in verjetno najbolj uveljavljene rešitve, ki temeljijo na arhitekturi odjemalec strežnik z uporabo operacijskega sistema Windows.

Vedno več je primerov, ko šole preidejo na odprtokodne rešitve - Linux. Tako je Becta leta 2005 opravila raziskavo, v kateri je sodelovalo 9 različnih šol. Becta (British Educational Communications and Technology Agency) ima podobno vlogo kot Arnes v Sloveniji. Organizacijo Becta v Veliki Britaniji financira Ministrstvo za otroke, šole in družine. Becta nadzira nakup vse opreme IKT in strategijo e-učenja za šole, poleg tega pa ima zelo pomembno vlogo pri zagotavljanju informacijske varnosti v šolah. Raziskava je bila opravljena na šolah, kjer že uporabljajo Linux. Analizirali so mnenje zaposlenih, učencev ter staršev. Predstavili so prednosti in slabosti omenjenih rešitev. Raziskali pa so tudi, katera odprtokodna oprema se največ uporablja. Kot največje prednosti navajajo šole znatno znižanje stroškov, brezplačno tehnično podporo, stabilnejše delovanje računalnikov, uporabo tudi manj zmogljivejših računalnikov in za nas zelo pomembno dejstvo, tudi višjo varnost sistema. Edina slabost, ki jo omenjajo, je nezdružljivost nekatere didaktične programske opreme z operacijskim sistemom Linux. Učitelji poudarjajo, da ima uporaba Linuxa in ostale odprtokodne programske opreme prednost tudi za učence. Ti lahko to opremo brezplačno uporabljajo na svojih domačih računalnikih in si obenem pridobijo nova znanja na področju odprte kode. Nekatere šole so z odprto kodo seznanile tudi starše. Ponudile so jim programsko opremo in starši so jo pričeli uporabljati doma. Ugotovljeno je bilo, da največ šol uporablja Linux – Mandrake, tako na strežniku kot na delovnih postajah. Poleg tega ima večina računalnikov nameščen program Star Office ali Open Office, ki je nekakšna zamenjava za plačljivi Microsoft Office. Uporabljajo pa tudi ostalo odprtokodno didaktično opremo, ki je je na voljo vedno več. Na splošno je bilo ugotovljeno, da so na vseh šolah zadovoljni s takšno rešitvijo in je ne nameravajo zamenjati za kaj drugega.

Primer vsesplošne uporabe odprtokodne programske opreme smo našli tudi na šolah v Indiji. Gre za projekt, ki ga je podprlo tamkajšnje Ministrstvo za šolstvo. Projekt vključuje uporabo in uvajanje odprtokodne programske opreme. Za učitelje so pripravili izobraževanja, s katerimi so jih seznanili z novo programsko opremo. V bistvu ne gre za projekt, ki bi bil namenjen povečanju informacijske varnosti, ampak je v prvi vrsti namenjen znižanju stroškov. Ampak glede na to, da je Linux poznan kot zelo varen, je to zagotovo zelo dobra rešitev.

Uporaba operacijskega sistema Linux je zelo razširjena tudi na šolah po Nemčiji in Avstriji. Zasledili smo kar nekaj sistemov, ki so prilagojeni za delovanje v šolskem okolju.

Pri iskanju rešitev, ki jih uporabljajo na šolah po svetu, smo se osredotočili na odprtokodne rešitve, se pravi takšne, ki temeljijo na operacijskem sistemu Linux. Omenjene rešitve so za šolo zelo dobrodošle, saj so dostopne po nizki ceni, odlikuje jih zanesljivost, varnost in prilagodljivost, hkrati pa nudijo dobro pomoč in podporo uporabnikom. Uporabniki imajo ob primernem znanju tudi možnost razvijanja lastnih rešitev. Poleg tega pa je odprta koda vsaj na osnovnih šolah pri nas premalo poznana.

V nadaljevanju smo raziskali in opisali nekaj rešitev, ki jih uporabljajo na šolah po svetu.

3.4.1 Open School Server

Open School Server v nadaljevanju OSS razvija podjetje EXTIS GmbH iz Uttenreutha v Nemčiji. Široka programska rešitev, ki ponuja več kot samo strežnik, temelji na operacijskem sistemu Suse Linux, ki je poznan kot zelo zanesljiv in varen operacijski sistem. OSS je prilagojen šolskim ustanovam in zasnovan z idejo karseda centraliziranega upravljanja uporabnikov in omrežja. Uporabniku prijazno okolje daje vedeti, da se njegovi razvijalci dobro zavedajo, da je med ciljnimi uporabniki veliko takšnih, ki z Linuxom, na katerem temelji, nimajo veliko izkušenj. Prva verzija je bila razvita leta 2003 in je temeljila na sistemu Suse Linux Enterprise Server 9. Razvoj odprtokodnega šolskega strežniškega sistema, kot bi ga lahko po slovensko poimenovali, pa ne miruje. Trenutno zadnja dostopna verzija je OSS 3.1.1, ki temelji na sistemu Suse Linux Enterprise Server 11.

Poglejmo si nekaj osnovnih značilnosti OSS:
OSS omogoča naslednje bistvene storitve, ki omogočajo zagotavljanje višje varnosti:

- domenski strežnik za overjanje uporabnikov,
- podatkovni strežnik,
- namestniški strežnik, z orodjem za filtriranje spletnih strani,
- požarno pregrado.

Upravljanje sistema je enostavno izvedljivo preko spletnega vmesnika, kjer lahko poleg upravljanja z uporabniki, nadziramo tudi celotni sistem.

Podatki o uporabnikih so shranjeni na enotni lokaciji v LDAP imeniku, katerega uporabljajo tudi ostali programi oz. storitve.

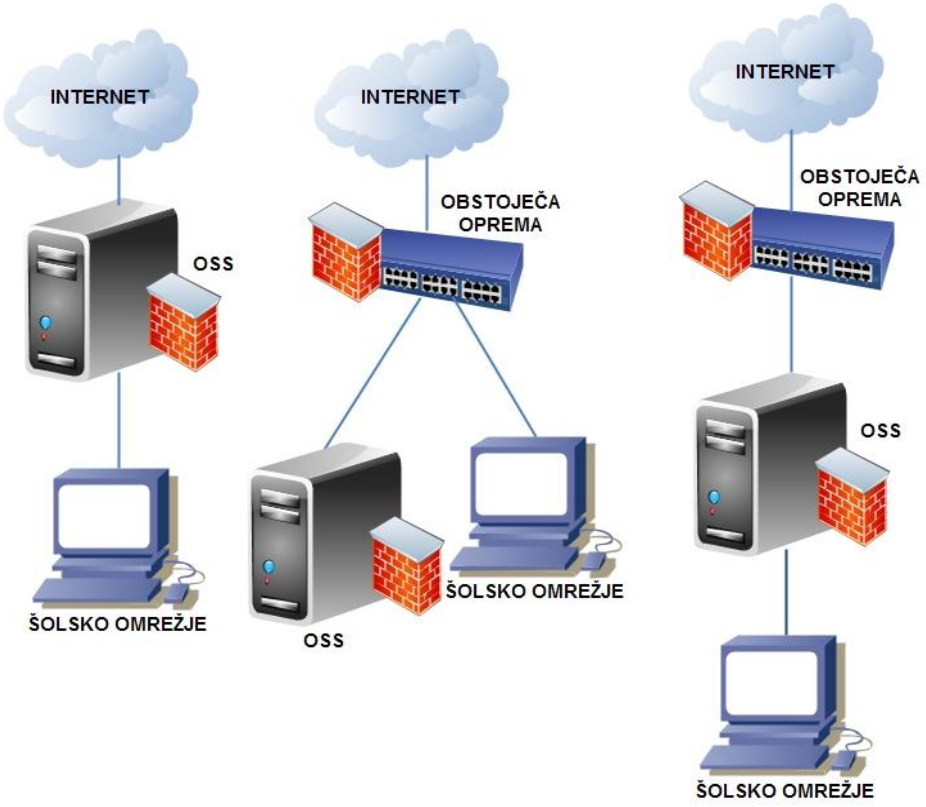
OSS lahko v omrežje postavimo na tri različne načine, ki jih prikazuje slika 6. Ti načini pomembno vplivajo na varnost šolskega omrežja ter na varnost sistema samega. Značilnosti omenjenih postavitev so naslednje:

- Prvi način je povezava z uporabo obstoječega usmerjevalnika, kjer delovne postaje in OSS za dostop do interneta neposredno uporabljajo obstoječ usmerjevalnik v omrežju. Varnost omrežja je v tem primeru v največji meri

odvisna od varnosti usmerjevalnika. S takšnim načinom povezave nimamo možnosti omejevanja dostopa interneta preko samega strežnika, posledično je lahko tudi varnost omrežja na nižji ravni.

- Drugi način povezave je takšen, kjer nam OSS Server zagotavlja povezavo do interneta. Omenjeni način povezave lahko uporabimo, če v omrežju še nimamo usmerjevalnika. Vlogo usmerjevalnika v tem primeru opravlja OSS. Z omenjenim načinom povezave lahko dosežemo višjo stopnjo varnosti, saj nam OSS zagotavlja tudi funkcijo požarne pregrade.

- Pri tretjem načinu uporabimo obstoječi usmerjevalnik, ki ima obenem še funkcijo požarne pregrade, na katerega priključimo OSS. Delovne postaje iz šolskega omrežja lahko do interneta dostopajo samo preko OSS in niso neposredno v povezavi z usmerjevalnikom. Na takšen način lažje spremljamo dogajanje v omrežju na lokalni ravni ter določimo promet iz lokalnega omrežja na usmerjevalnik in obratno. S tem dosežemo še višjo stopnjo varnosti omrežja.



Slika 6: Različni načini postavitve OSS v omrežje

3.4.2 Skolelinux

Skolelinux je distribucija informacijskega sistema, ki je prilagojen za delo v šolskih ustanovah in je izdelan na Debian različici operacijskega sistema Linux. Skolelinux je bil izdelan po projektu Debian Edu na Norveškem, kjer so ga sprva

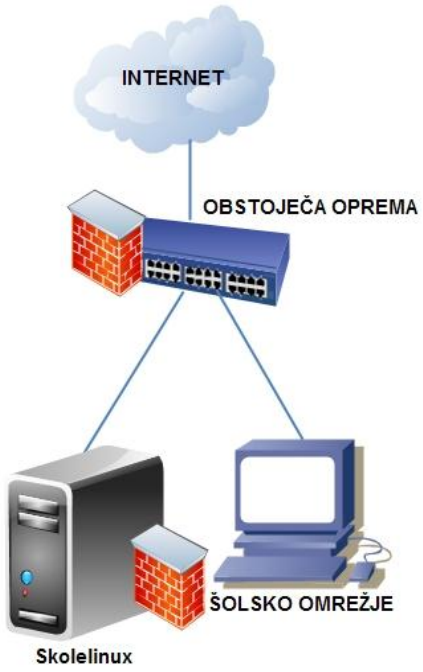
tudi največ uporabljali. Danes ga poleg Norveške veliko uporabljajo v Španiji, Nemčiji in Franciji.
Skolelinux lahko v omrežje postavimo na način, kjer za povezavo do interneta uporabljamo obstoječ usmerjevalnik in opremo, na katero so priključene delovne postaje in sistem Skolelinux. Način postavitve omrežja prikazuje slika 7.

Skolelinux ponuja številne storitve. Izmed tistih, ki služijo zagotavljanju višje varnosti, naj omenimo:

- overjanje uporabnikov na podlagi prijave v domeno,
- podatkovni strežnik s sistemom shranjevanja in arhiviranja podatkov,
- posredniški strežnik.

Sama zasnova sistema je podobna kot pri sistemu OSS. Sistem uporablja LDAP imenik kot centralno bazo podatkov o uporabnikih.

Upravljanje uporabnikov je mogoče izvajati preko spletnega vmesnika, za samo nadziranje sistema pa moramo uporabiti druga orodja.



Slika 7: Postavitev sistema Skolelinux v omrežje

3.4.3 Arktur – Schulserver

Arktur Schulserver je še ena različica informacijskega sistema, ki je prilagojena za rabo v šolskem okolju. Omenjeni sistem razvijajo učitelji in učenci iz mesta Braunschweig v Nemčiji. Informacijski sistem ponuja podobne storitve kot predhodno omenjena sistema. Poleg overjanja uporabnikov s prijavljanjem v domeno nam omogoča še postavitev posredniškega strežnika - Squid in podatkovnega strežnika - Samba.

Filozofija razdelitve lokalnega omrežja je podobna kot pri OSS sistemu. Lokalno omrežje nam razdeli na različne omrežne skupine, kar zagotavlja višjo varnost omrežja ter lažje aktivnosti v omrežju.

Sistem je mogoče upravljati preko oddaljene prijave s pomočjo SSH protokola ali preko same lokalne prijave v sistem.

3.4.4 Desktop in Server4education

Še ena zanimiva rešitev, ki smo jo odkrili z brskanjem po internetu, je operacijski sistem za delovne postaje imenovan Desktop4education in strežniška različica Server4education. Sistem je pričel nastajati pod okriljem učitelja matematike in dijakov na srednji šoli Weiz v Avstriji. Zasnovan je na operacijskem sistemu Linux, in sicer na distribuciji OpenSuse.

Z vidika varnosti nam je še posebno zanimiva rešitev za strežnik. Po videzu ter storitvah še najbolj spominja na sistem OSS. Server4education lahko uporabimo kot domenski strežnik, podatkovni strežnik, posredniški strežnik in kot požarno pregrado. Za centralno hranjenje podatkov se uporablja LDAP imenik. Pri postavitvi v omrežje lahko izbiramo med enakimi možnostmi, kot nam jih ponuja OSS.

Omeniti moramo tudi Desktop4education, ki se uporablja za delovne postaje. Gre za zelo varen operacijski sistem, ki poleg ostalega vsebuje tudi številne didaktične programe. Tako lahko v kombinaciji s sistemom Server4education postavimo zelo varen informacijski sistem, ki je obenem še brezplačen.

Uporabo omenjene rešitve in odprtokodne programske opreme nasploh močno spodbuja tudi tamkajšnje Ministrstvo za šolstvo, umetnost in kulturo. Na šole po Avstriji so poslali okoli 2000 brezplačnih CD in DVD medijev. Mediji so poleg omenjenih rešitev vključevali tudi obsežno gradivo za delo z odprtokodnimi programi. Kot zanimivost naj omenimo tudi to, da ministrstvo še dodatno spodbuja uporabo odprte kode, saj so šolam, ki Microsoft Office zamenjajo s programom Open namenili 10 EUR. Ta znesek dobi šola za vsako delovno postajo (Bierhals, 2009).

3.4.5 Linux Advanced

Linux Advanced je operacijski sistem, ki temelji na osnovi Debian Linux. Kot že nekaj prejšnjih za izobraževalne ustanove prilagojenih sistemov tudi ta izhaja iz sosednje Avstrije. Linux Advanced razvijajo učenci in učitelji na srednji šoli. Projekt zajema rešitve za delovne postaje in strežnike. Za delovne postaje ponujajo tako imenovane Live distribucije, kar pomeni da jih lahko poženemo in uporabljamo neposredno iz CD, DVD oz. USB medijev.

Operacijski sistem za strežnik se imenuje Linux Advanced Server. Ta ima poleg osnovnih funkcionalnosti tudi številne varnostne mehanizme. Strežnik lahko uporabljajo odjemalci z Linux ali Windows delovnimi postajami. Podatki o uporabnikih so shranjeni v centralnem LDAP imeniku. Na strežniku lahko omogočimo DNS in DHCP storitev, kar pomeni lažje upravljanje z odjemalci v omrežju ter preverjanje istovetnosti uporabnikov s prijavo v domeno.

Za centralno hranjenje in zasebnost uporabnikovih podatkov skrbi strežnik Samba.

Za izboljšanje omrežne varnosti je na strežnik nameščen tudi program za filtriranje spletne vsebine.

3.4.6 Uporaba lahkih odjemalcev

V šolstvu po svetu se zelo veliko uporablja tudi tehnologija lahkih odjemalcev (angl. thin client computing). Za delo v tem okolju je potreben tako imenovani terminalski strežnik, na katerega se povezujejo lahki odjemalci. Povezava na terminalski strežnik je hitra, ker se preko mreže prenašajo samo podatki za prikaz na namizju. Edini podatki, ki se morajo prenašati nazaj na strežnik, so ukazi, ki jih vnesemo preko tipkovnice oz. miške. Protokoli, ki se uporabljajo za komunikacijo med strežnikom in uporabnikom, so: Remote desktop protocol, Citrix ICA in NX tehnologija. Ker se shranjevanje in procesiranje podatkov vrši na strežniku, so zahteve za uporabnika minimalne. Za uporabnika lahko uporabimo vse, od mrežnega računalnika do popolnoma nameščenega osebnega računalnika. Moč in hitrost uporabnikovega računalnika je praktično nepomembna, ker je zelo malo udeležen v celotnem procesu.

Bistvo omenjene tehnologije je torej izraba manj zmogljivih računalnikov in hitrejše administriranje, saj se vse potrebno naredi na strežniku. Raziskave pa kažejo, da je omenjena tehnologija tudi varnejša (Neoware, 2006).

Bistvene varnostne prednosti v primerjavi z običajnimi delovnimi postajami so naslednje:

- prenos virusa med delovno postajo in strežnikom je redek pojav,
- varnost podatkov je v celoti odvisna od varnosti na strežniku,
- protivirusna zaščita, požarna pregrada in varnostne nastavitve se v celoti urejajo na strežniku, kar pomeni lažje upravljanje,
- varnostne posodobitve odjemalcev so minimalne v primerjavi z običajnimi delovnimi postajami.

Uporabo lahkih odjemalcev smo zasledili na šolah, ki so omejene s sredstvi ter tam, kjer želijo kar najbolje izrabiti manj zmogljive računalnike in opremo. Nekatere šole bi takšno opremo že zdavnaj odpisale.

Bistvena programska oprema pri delu z lahkimi odjemalci je operacijski sistem na strežniku. Uporabimo lahko Windows Terminal Server ali pa brezplačno Linux različico.

Verjetno je najbolj popularen terminalski strežnik, ki teče na Linuxu, LTSP (Linux Terminal Server Project). LTSP je vključen v številne Linux distribucije, med drugimi tudi v K12LTSP, ki jo šole po svetu veliko uporabljajo. K12LTSP temelji na Fedora jedru. Gre za neodvisen projekt, ki je začel nastajati leta 2000 v mestu Portland. Zasledili smo, da je večina tamkajšnjih šol že pričelo uporabljati omenjeno rešitev. (http://k12linux.mesd.k12.or.us/)

4 ANALIZA STANJA INFORMACIJSKE VARNOSTI V SLOVENSKIH OSNOVNIH ŠOLAH

Informacijska varnost v slovenskih osnovnih šolah je dokaj neraziskano področje. Vemo, da so skrbniki IKT običajno računalničarji oz. organizatorji informacijskih dejavnosti, ki v veliki meri skrbijo tudi za informacijsko varnost. Zaradi nenehnega tehnološkega razvoja in čedalje več opreme postaja to delo vedno težje obvladljivo, skrb za informacijsko varnost pa je pogosto postavljena v ozadje.

Omeniti moramo tudi dejstvo, da na delo skrbnika IKT in posledično tudi na informacijsko varnost v osnovnih šolah močno vpliva količina njegove zaposlitve. Delovno mesto skrbnika IKT je namreč vezano na število oddelkov na šoli, zato tudi ni redek pojav, da to delo opravlja učitelj, ki tega področja ne pozna in ga ne obvladuje. Vse to so dejavniki, ki še kako vplivajo na stanje informacijske varnosti v slovenskih osnovnih šolah.

Na nivoju države delujejo institucije, ki smo jih predhodno že opisali. Največ pomoči pri zagotavljanju informacijske varnosti nedvomno nudi Arnes. Infrastruktura, ki jo ponuja, zagotavlja visoko stopnjo varnosti šolskega omrežja, ob predpostavki, da sami zagotovimo ustrezno varnost na lokalni ravni.

V empiričnem delu smo najprej ugotovili, kakšna je informacijska varnost v slovenskih osnovnih šolah. Raziskavo smo opravili v obliki ankete, v kateri so sodelovali skrbniki IKT iz različnih šol po Sloveniji.

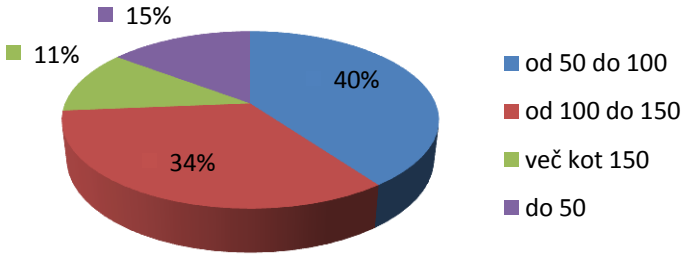
Nato smo raziskali, kakšno znanje in kakšen pogled na informacijsko varnost imajo šolski uporabniki. V tej raziskavi so sodelovali učitelji iz različnih šol po Sloveniji in učenci Osnovne šole Neznanih talcev Dravograd.

Anketni vprašalniki so priloženi k nalogi kot PRILOGA 1.

4.1 Analiza stanja z vidika skrbnikov IKT

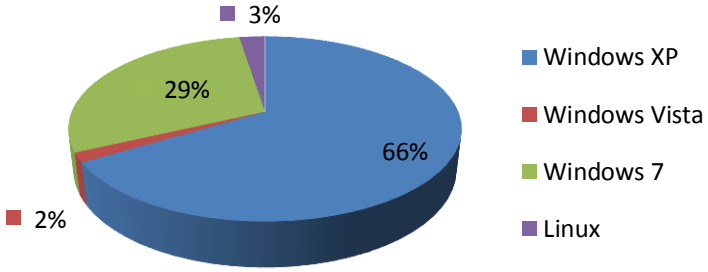
V raziskavi je sodelovalo 95 osnovnih šol iz celotne Slovenije. Sodelovale so različno velike šole, kar dokazujejo rezultati prvega vprašanja, ki so prikazani na sliki 8. Število računalnikov je namreč sorazmerno z velikostjo šole. Večje šole imajo običajno več zaposlenih, več učencev in s tem tudi večjo potrebo po računalnikih.

V raziskavi je sodelovalo največ šol, ki imajo med 50 in 150 računalnikov. Po izkušnjah sodeč so šole, ki imajo več kot 100 računalnikov, že dokaj velike. Glede na razpršenost podatkov pa lahko vidimo, da so v raziskavi sodelovale šole vseh velikosti.



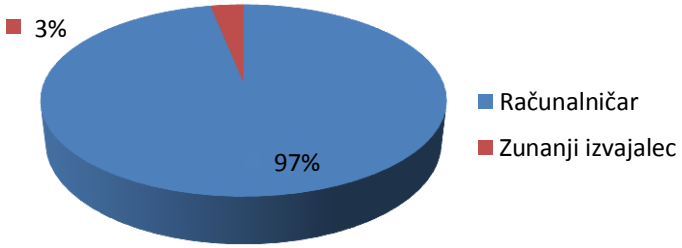
Slika 8: Število računalnikov v šoli

V nadaljevanju nas je zanimalo, kateri operacijski sistem šole največ uporabljajo, saj ima operacijski sistem zelo pomembno vlogo pri zagotavljanju informacijske varnosti. Ugotovili smo (glej sliko 9), da prevladuje operacijski sistem Windows XP, sledi pa mu Windows 7.



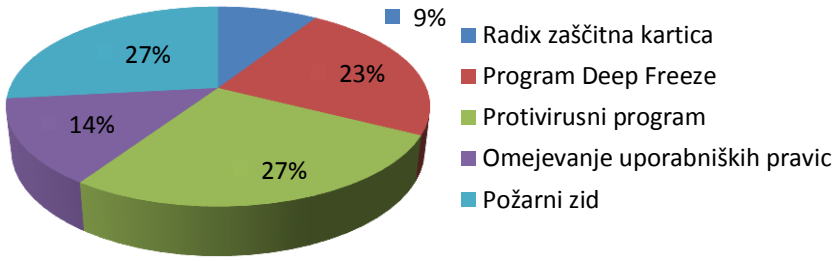
Slika 9: Najpogosteje uporabljen operacijski sistem

Že na začetku raziskave smo omenili, da so računalničarji tisti, ki skrbijo za IKT v osnovni šoli, z raziskavo pa smo to le še potrdili. Rezultati, prikazani na sliki 10 kažejo, da to nalogo v 97 % opravljajo računalničarji.



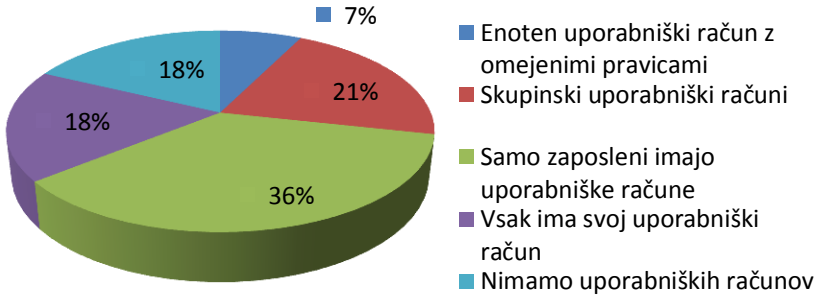
Slika 10: Skrbnik informacijsko-komunikacijske tehnologije

V nadaljevanju nas je zanimalo, katerih varnostnih mehanizmov se skrbniki IKT poslužujejo za izboljšanje sistemske varnosti. Na vprašanje je bilo možnih več odgovorov. Ugotovili smo, da sta najbolj uporabljena protivirusni program in požarni zid. Veliko pa je v uporabi tudi program DeepFreeze. V nekoliko manjšem obsegu zasledimo še uporabo Radix zaščitne kartice in izboljšanje varnosti z omejevanjem uporabniških pravic. Rezultati odgovorov na to vprašanje so prikazani na sliki 11.



Slika 11: Najpogosteje uporabljeni varnostni mehanizmi

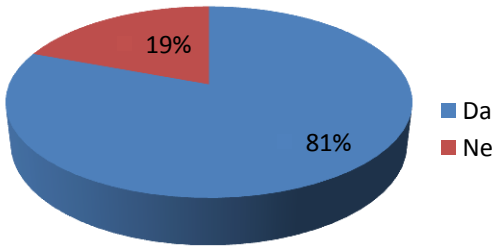
Nato smo raziskali, kako imajo na osnovnih šolah organizirane uporabniške račune. Ugotovili smo, da 18 % za prijavo v sistem ne uporablja uporabniških računov. Delež šol, kjer imajo samo zaposleni svoje uporabniške račune, znaša 36 %, sledijo šole s skupinskimi uporabniškimi računi, enak delež šol uporablja račune za vse uporabnike. Zasledili smo še odgovor, kjer imajo šole enoten uporabniški račun. Način organiziranja uporabniških računov prikazuje slika 12.



Slika 12: Organiziranje uporabniških računov

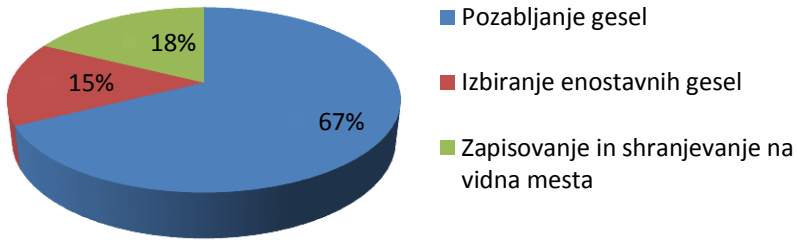
Pri izdelavi in uporabi uporabniškega računa ima zelo pomembno vlogo njegovo geslo. Geslo mora biti varno, kar pomeni, da ne sme biti beseda iz slovarja in seveda sestavljeno iz čim več znakov.

Skrbnike IKT smo vprašali, če pri izbiri gesla pomagajo in svetujejo uporabnikom. Ugotovili smo (glej sliko 13), da večina od njih uporabnikom pri tem pomaga.



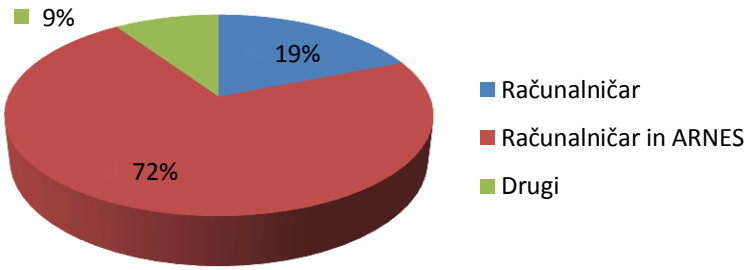
Slika 13: Pomoč in svetovanje pri izbiri gesla

Kje in zakaj imajo uporabniki z geslom največ težav? Kot prikazuje slika 14, smo ugotovili, da je največja težava pozabljanje gesla, izbira enostavnega gesla in nepravilno ravnanje z njim.



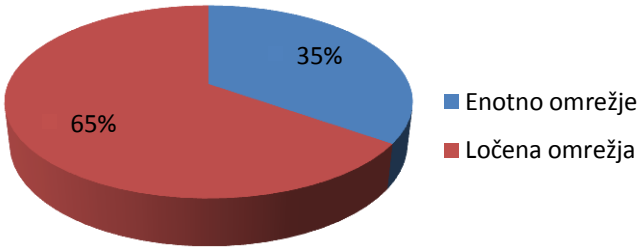
Slika 14: Težave, ki se pojavljajo pri izbiri gesla

Skrb za varnost omrežja, vsaj na logičnem nivoju, na osnovnih šolah prevzema Arnes. Arnes skrbi za zaščito lokalnega omrežja pred nevarnostmi z interneta, skrbi za ločitev administrativnega in pedagoškega dela omrežja, skrbi za zaščito strežnikov in podobno. Med šolami, ki so sodelovale v raziskavi, je bilo res največ takšnih, ki sodelujejo z Arnesom pri zaščiti in varovanju omrežja. Nekaj, verjetno manjših šol, pa za varnost omrežja skrbi samih. Rezultate odgovorov na ta vprašanja prikazuje slika 15.



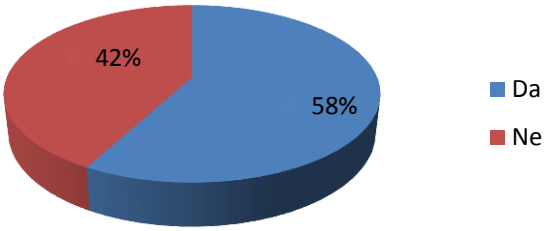
Slika 15: Osebe, ki skrbijo za varnost omrežja

Pomembno vlogo pri varnosti omrežja igra tudi sama organizacija omrežja. Ugotovili smo (glej sliko 16), da 65 % šol uporablja ločena omrežja, preostalih 35 % pa ima postavljeno enotno omrežje.



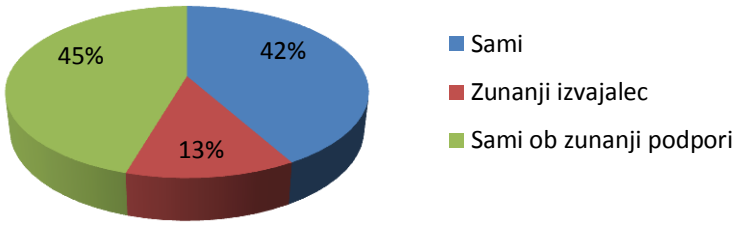
Slika 16: Organizacija omrežja

S strežnikom lahko na šoli veliko pridobimo. Lažje je administriranje uporabnikov, izboljša se sistemska varnost in varnost podatkov. Seveda pa nakup in postavitev strežnika predstavlja tudi določen strošek, zato je bilo za pričakovati, da ga vse šole ne uporabljajo. Ugotovili smo (glej sliko 17), da strežnik uporablja 58% šol, medtem ko ostalih 42% šol strežnika nima.



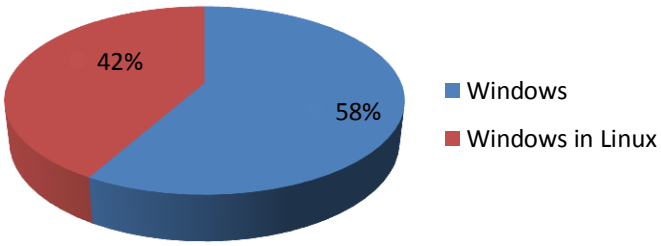
Slika 17: Delež uporabe in neuporabe strežnika

Postavitev in vzdrževanje strežnika zahteva tudi določeno znanje, kar je pogosto vzrok, da ga na osnovnih šolah ne uporabljajo. Ugotovili smo (glej sliko 18), da je skrbnik IKT sam ali ob zunanji podpori največkrat tisti, ki vzdržuje strežnik.



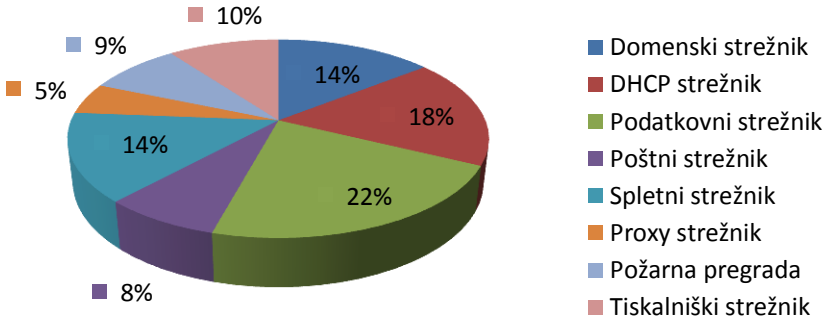
Slika 18: Oseba ali organizacija, ki vzdržuje šolski strežnik

Na strežniku nekoliko prevladuje operacijski sistem Windows, kot to prikazuje slika 19. Verjetno je to posledica boljše združljivosti in lažjega upravljanja.



Slika 19: Operacijski sistem na strežniku

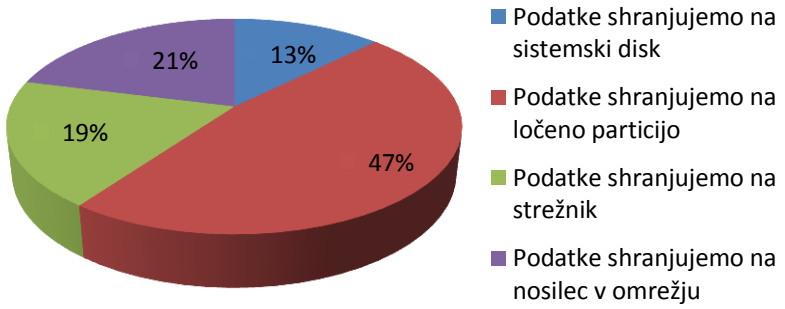
Za kakšne namene šole uporabljajo strežnike, smo ugotovili v nadaljevanju. Na sliki 20 lahko vidimo, da največ, in sicer 22% šol uporablja strežnik za shranjevanje podatkov. Sledijo ostale storitve, kot so: DHCP, domenski strežnik, spletni strežnik… Z vidika zagotavljanja varnosti velja omeniti namestniški oz. proxy strežnik ter požarno pregrado.



Slika 20: Najpogostejše storitve, ki jih nudi strežnik

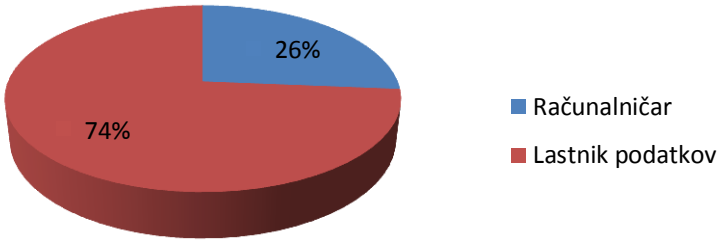
Nadaljevanje raziskave smo namenili varnosti podatkov. Vemo namreč, da predstavljajo podatki največjo vrednost informacijskega sistema. Kljub pomembnosti podatkov je za njihovo varnost ponekod še vedno slabo poskrbljeno.

Najprej nas je zanimalo, kako imajo v osnovnih šolah urejeno shranjevanje podatkov. Raziskava je pokazala (glej sliko 21), da je sistem shranjevanja podatkov v 47% šol naravnan na shranjevanje podatkov na lokalni disk in ločeno particijo. Sledi shranjevanje podatkov na nosilec v omrežju, ki ga uporablja 21% anketiranih šol. Na strežnik shranjuje podatke 19% šol, preostalih 13% pa shranjuje podatke kar na sistemski disk.



Slika 21: Sistem shranjevanja podatkov

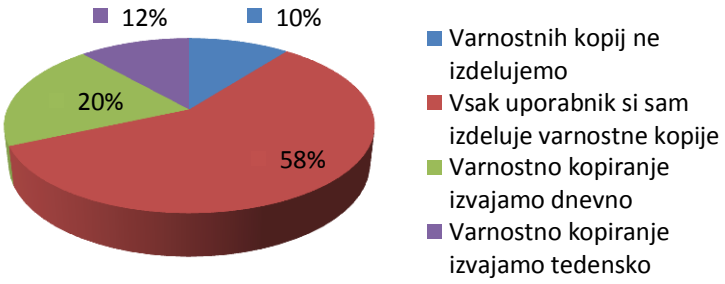
Za svoje podatke mora najprej skrbeti uporabnik sam, seveda ob predpostavki, da ima o tem dovolj znanja in mu je tehnološko to omogočeno. Raziskava je pokazala (glej sliko 22), da 74% šol oz. njihovih uporabnikov za podatke skrbi samih. Na preostalih osnovnih šolah pa za varnost uporabniških podatkov skrbi računalničar oz. skrbnik IKT.



Slika 22: Oseba, ki v šoli skrbi za varnost podatkov

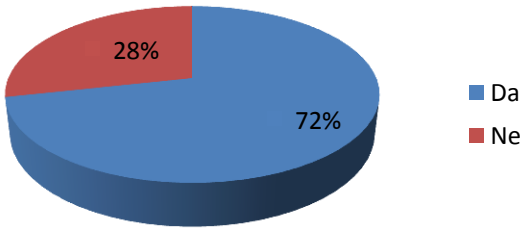
Za zagotavljanje ustrezne podatkovne varnosti moramo imeti poskrbljeno tudi varnostno kopiranje podatkov. Rezultate odgovora na vprašanje, kako na osnovnih šolah izvajajo varnostno kopiranje podatkov, prikazuje slika 23, rezultati odgovorov pa so naslednji:

- 10% udeleženih v raziskavi varnostnega kopiranja ne izvaja,
- na 58% šol si uporabniki sami izdelujejo varnostne kopije,
- 20% šol ima izdelano dnevno arhiviranje podatkov,
- preostalih12% izvaja tedensko varnostno kopiranje podatkov.



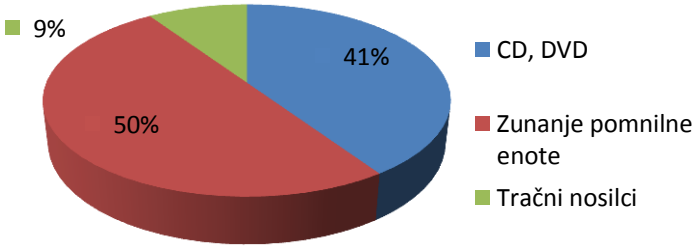
Slika 23: Način varnostnega kopiranja podatkov

Poleg varnostnega kopiranja je pomembno tudi arhiviranje podatkov. Arhiviranje je varno hranjenje podatkov, s katerimi ne delamo več redno, a jih potrebujemo zaradi potreb v prihodnosti, zakonskih potreb ali česa podobnega. Ugotovili smo (glej sliko 24), da za arhiviranje podatkov skrbi 72% šol.



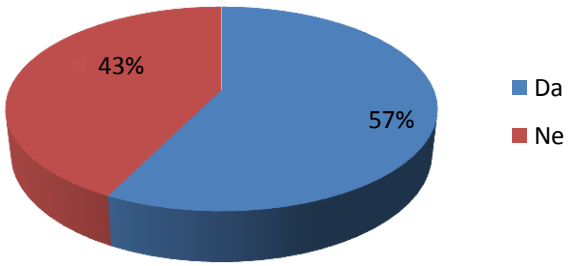
Slika 24: Skrb za arhiviranje podatkov

Raziskali smo tudi, na katere nosilce šole arhivirajo podatke. Ugotovili smo (glej sliko 25), da se največ uporabljajo zunanji prenosni mediji (trdi disk, mediji z vgrajenim flash pomnilnikom in podobno). Zelo pogosta in priljubljena medija za arhiviranje podatkov še vedno ostajata CD in DVD. Poleg omenjenega na nekaterih osnovnih šolah za arhiviranje podatkov uporabljajo tudi tračne nosilce.



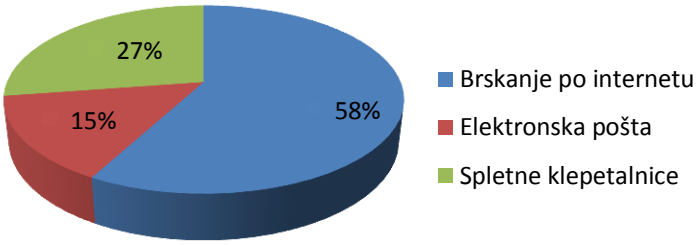
Slika 25 : Mediji, uporabljeni za arhiviranje podatkov

Kljub temu, da skrbimo za ustrezno varnostno kopiranje in arhiviranje podatkov, se lahko zgodi, da podatkov kasneje več ne moremo obnoviti. Vzrok je lahko slab medij ali pa recimo napake, ki se pojavijo pri zapisovanju podatkov na medij. Napake se lahko pojavijo tudi zaradi neustrezno shranjenih medijev (sonce, vlaga, magnetno sevanje …). Upoštevati moramo dejstvo, da je z leti tudi berljivost medijev slabša. Zaradi omenjenih dejstev nas je zanimalo, če na osnovnih šolah kdaj preverjajo berljivost zapisanih podatkov. Slika 26 prikazuje, da 57% šol medije preverja, preostalih 43% pa temu ne posveča posebne pozornosti.



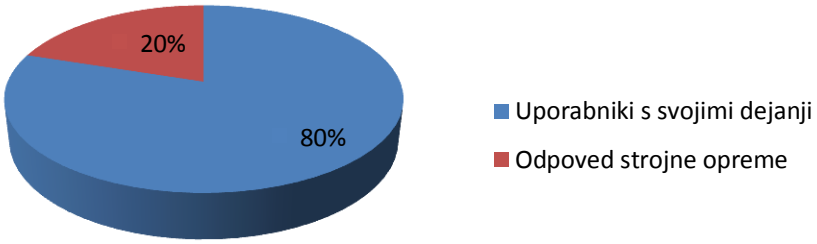
Slika 26: Preverjanje berljivosti medijev v osnovnih šolah

Uporaba internetnih storitev je v osnovnih šolah močno razširjena, zato nas je zanimalo katere storitve so tiste, ki po mnenju skrbnikov IKT najbolj ogrožajo informacijsko varnost. Ti menijo (glej sliko 27), da največjo nevarnost predstavlja že samo brskanje po internetu, sledi uporaba elektronske pošte in spletnih klepetalnic.



Slika 27: Največje nevarnosti uporabe internetnih storitev

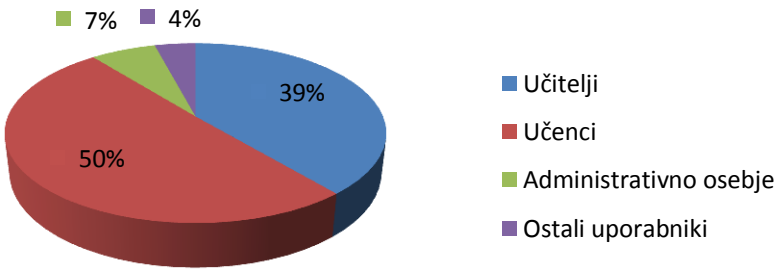
V nadaljevanju nas je zanimalo, kateri so najpogostejši izvori groženj informacijske varnosti v osnovnih šolah. Največ skrbnikov IKT, in sicer kar 80%, meni, da te grožnje izvirajo iz človeških dejanj, 20% pa jih meni, da grožnje izvirajo iz odpovedi strojne opreme. Najpogostejše izvore groženj prikazuje slika 28.



Slika 28: Najpogostejši izvori groženj informacijske varnosti

Administratorji računalnikov in računalniških omrežij so neprestano pred novimi izzivi, novimi težavami, pogosto se srečujejo s težavami uporabnikov, tehničnimi težavami in tudi težavami zaradi pomanjkanja časa, znanja, izkušenj in še bi lahko naštevali. Zaradi tega smo skrbnike IKT povprašali, kdo izmed šolskih uporabnikov najbolj ogroža informacijsko varnost.

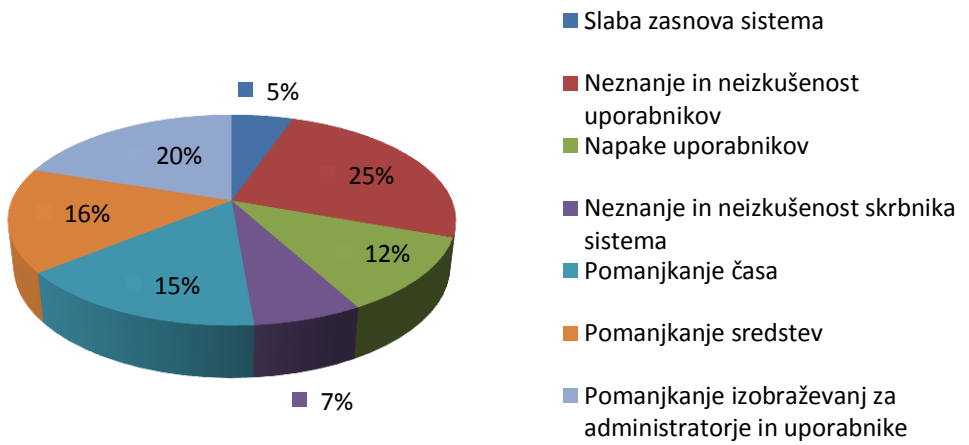
Raziskava je pokazala (glej sliko 29), da informacijsko varnost najbolj ogrožajo učitelji ter učenci.



Slika 29: Šolski uporabniki, ki najbolj ogrožajo informacijsko varnost

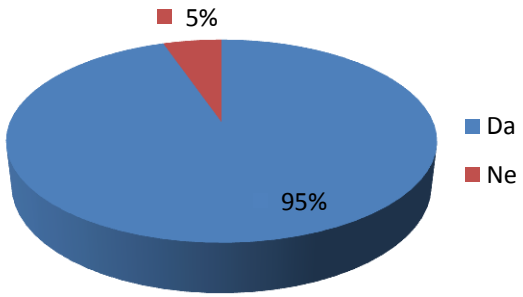
Že predhodno smo ugotovili, da prav uporabniki najbolj ogrožajo varnost informacijskega sistema. Kaj je vzrok, da uporabniki povzročajo informacijske grožnje, pa smo raziskali v nadaljevanju.

Ugotovili smo (glej sliko 30), da je največja težava neznanje in neizkušenost uporabnikov, pomanjkanje izobraževanj za administratorje in uporabnike, pomanjkanje sredstev ter pomanjkanje časa za izboljšavo. Nekaj skrbnikov IKT pa meni, da informacijski sistem ogroža tudi neznanje in neizkušenost skrbnika sistema in slaba zasnova sistema samega.



Slika 30: Najpogostejši vzroki groženj

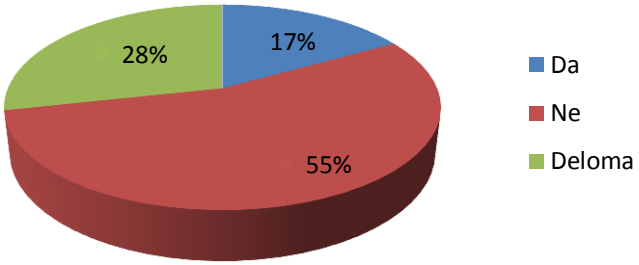
Skrbnik IKT je v večini primerov tisti, ki najpogosteje skrbi za varnost informacijskega sistema na osnovnih šolah. Zanimalo nas je, ali skrbnik IKT opravlja tudi nalogo tistega, ki uporabnike ozavešča o informacijski varnosti. Ugotovili smo (glej sliko 31), da praktično vsi skrbniki IKT skrbijo tudi za ozaveščanje uporabnikov o informacijski varnosti.



Slika 31: Ozaveščanje o informacijski varnosti

Nato nas je zanimalo, če imajo šole izdelano varnostno politiko informacijskega sistema.

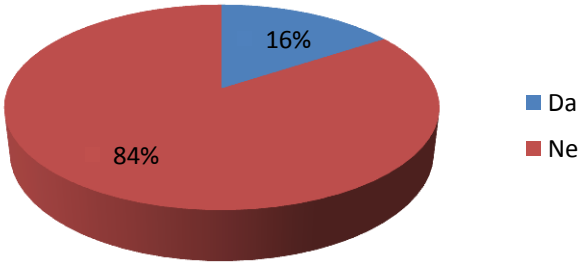
Ugotovili smo (glej sliko 32), da 55% šol varnostne politike nima izdelane, 17% šol ima politiko izdelano, medtem ko ima 28% šol delno izdelano varnostno politiko.



Slika 32: Prisotnost varnostne politike v osnovnih šolah

Ugotovili smo, da v Sloveniji deluje kar nekaj državnih iniciativ, ki predvsem ozaveščajo učitelje, učence in starše o informacijski varnosti, posebnih tehnološko izdelanih rešitev pa ni zaznati.

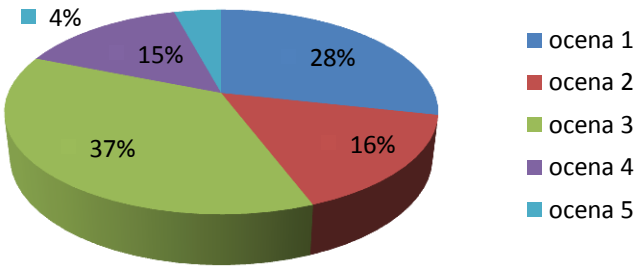
Zanimalo nas je, kaj o podpori na področju informacijske varnosti menijo skrbniki IKT. Kar 84% skrbnikov IKT meni, da na tem področju nimajo zadostne pomoči in podpore (glej sliko 33).



Slika 33: Mnenje o podpori na področju informacijske varnosti

Za konec smo skrbnike IKT vprašali, kako bi ocenili trenutno stanje informacijske varnosti na svoji osnovni šoli. Rezultate odgovorov prikazuje slika 34 in so naslednji:

- največ skrbnikov IKT je informacijsko varnost ocenilo z oceno 3,
- 28% jih meni, da je stanje na področju informacijske varnosti v njegovi šoli zelo slabo (ocena 1),
- 16% je informacijsko varnost v šoli ocenilo z oceno 2,
- 15% je informacijsko varnost ocenilo z oceno 4,
- preostali 4% pa varnost ocenjujejo z oceno 5.



Slika 34: Ocena stanja na področju informacijske varnosti v osnovnih šolah

Povzetek raziskave

Raziskava je pokazala, da je informacijska varnost problem, ki se ga zavedajo vsi skrbniki IKT, ki skušajo kljub pomanjkanju časa, sredstev in znanja zagotoviti ustrezno informacijsko varnost v svojih osnovnih šolah. Ugotovili smo, da informacijsko varnost v osnovnih šolah najbolj ogrožajo človeški dejavniki, in sicer učitelji ter učenci, ki so tudi večinski uporabniki. Najpogostejši vzroki težav so: neznanje in neizkušenost uporabnikov, pomanjkanje izobraževanj, pomanjkanje sredstev ter slaba zasnovna sistema. Ugotovili smo, da med najnevarnejšimi storitvami izstopa uporaba internetnih storitev, kot so brskanje po internetu, spletne klepetalnice in elektronska pošta.

Med operacijskimi sistemi na delovnih postajah prevladuje Microsoft Windows XP, na strežnikih pa sta v uporabi tako Windows kot operacijski sistem Linux.

Pri zagotavljanju sistemske varnosti se največ uporabljajo naslednji mehanizmi: protivirusni programi, program Deep Freeze ter požarna pregrada operacijskega sistema.

Glede omrežne varnosti in infrastrukture smo ugotovili, da veliko šol uporablja Arnes-ovo infrastrukturo ločenih omrežij.

Naslednje, kar smo ugotavljali, je skrb za varnost podatkov. Ugotovili smo, da se na večini šol trudijo skrbeti za njihovo varnost. Podatke shranjujejo na varnejše mesto, največkrat na ločeno particijo, na nosilec v omrežju ali pa na strežnik. Varnostno kopiranje izvajajo uporabniki sami, medtem ko za arhiviranje podatkov skrbijo skrbniki IKT.

Ugotovili smo, da 55% šol nima izdelane varnostne politike informacijskega sistema, kar 84% skrbnikov IKT pa meni, da podpora na tem področju ni ustrezna.

Zanimiva je tudi ocena, s katero so ovrednotili informacijsko varnost na svoji šoli. Ocene so zelo razpršene; 28% informacijsko varnost ocenjuje z najslabšo oceno, 16% je varnost ocenilo z zadostno oceno, 37% z dobro, 15% s prav dobro in 4% z odlično.

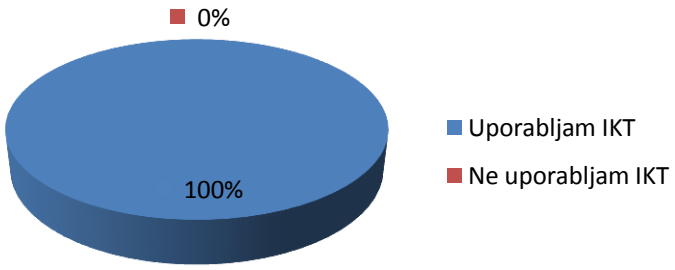
Na koncu smo skrbnike IKT še povprašali, kje vidijo rešitve za izboljšanje informacijske varnosti. Večina jih meni, da je potrebno sprejeti neko enotno rešitev na državnem nivoju, nujno potrebna pa so tudi izobraževanja.

4.2 Analiza stanja z vidika uporabnikov - učiteljev

Zelo pomembno vlogo pri zagotavljanju informacijske varnosti imajo zaposleni na šoli. Med zaposlenimi so zelo pomembni učitelji, saj jih je največ, poleg tega pa lahko svoje znanje koristno prenašajo tudi na učence.

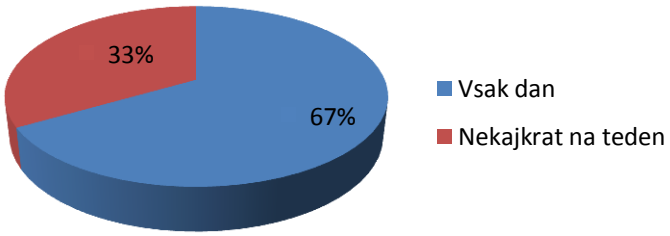
Za učitelje smo pripravili splošna vprašanja o uporabi IKT in z njimi povezanimi nevarnostmi. V tej raziskavi je sodelovalo 90 učiteljev iz šol po celotni Sloveniji.

Na začetku smo pridobili vpogled v odstotek tistih, ki uporabljajo računalnik in ostalo IKT. Ugotovili smo, da so vsi zaposleni tudi uporabniki IKT, kar potrjujejo rezultati na sliki 35.



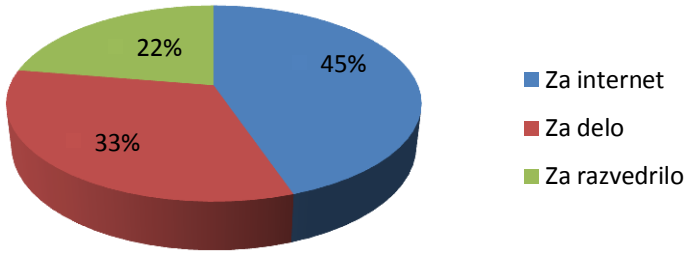
Slika 35: Delež uporabe IKT

Zanimalo nas je, kako pogosto zaposleni uporabljajo računalnik, saj bi bilo logično sklepati, da imajo tisti, ki računalnik uporabljajo pogosteje, tudi nekaj več izkušenj in znanja na tem področju. V naši raziskavi je sodelovalo 67 % takšnih, ki računalnik uporabljajo vsak dan, preostala tretjina pa ga uporablja vsaj nekajkrat tedensko. Pogostost uporabe računalnika prikazuje slika 36.



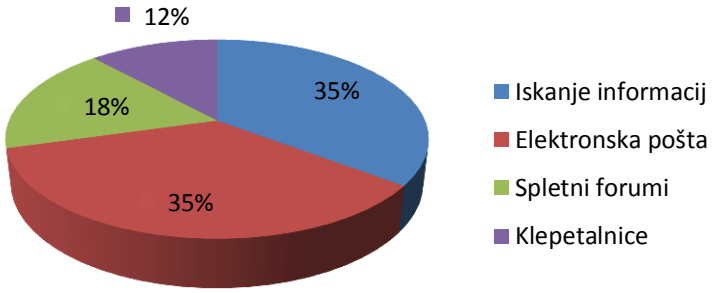
Slika 36: Pogostost uporabe računalnika

Nato smo zaposlene povprašali, v katere namene uporabljajo računalnik. Ugotovili smo (glej sliko 37), da le-ti računalnik največ uporabljajo za brskanje po internetu, za delo in razvedrilo.



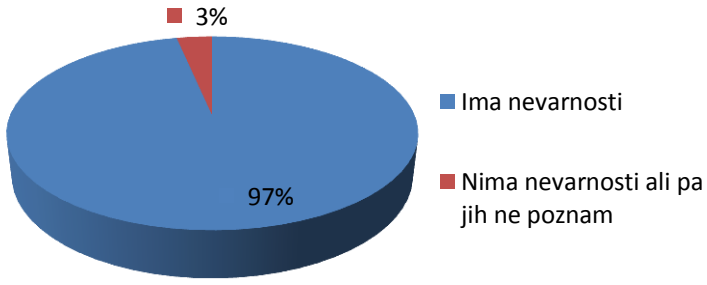
Slika 37: Namen uporabe računalnika

Predvidevali smo, da bo uporaba interneta prisotna v veliki večini, zato smo raziskali, katere internetne storitve pri uporabi izstopajo. Ugotovili smo (glej sliko 38), da zaposleni uporabljajo internet največ za iskanje najrazličnejših informacij in za elektronsko pošto.



Slika 38: Namen uporabe interneta

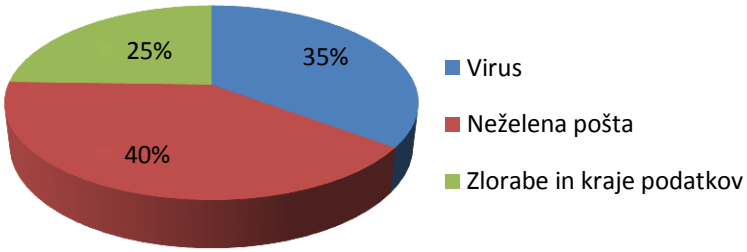
Uporaba interneta je tesno povezana s številnimi nevarnostmi. Kaj menijo zaposleni o internetnih nevarnostih, smo ugotovili v naslednjem delu raziskave. Kar se tiče same uporabe interneta, jih 97% meni, da ima lahko uporaba interneta tudi številne nevarnosti, preostali 3% pa nevarnosti ne pozna. Rezultate odgovorov na to vprašanje prikazuje slika 39.



Slika 39: Mnenje učiteljev o nevarnostih interneta

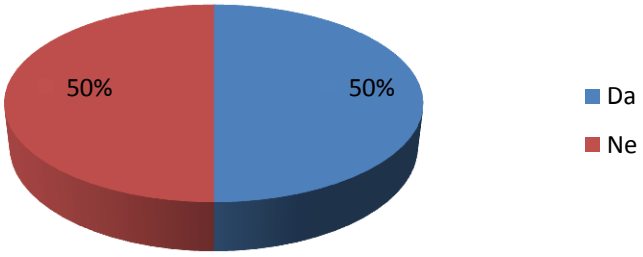
Učitelje smo nato vprašali, katere nevarnosti interneta poznajo. Ugotovili smo (glej sliko 40), da poznajo naslednje nevarnosti:

- neželena pošta,
- računalniški virus ter
- zlorabe in kraje podatkov.



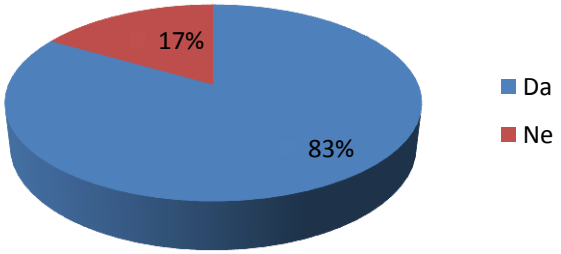
Slika 40: Internetne nevarnosti, ki jih poznajo učitelji

V zadnjem delu raziskave smo ugotovili, koliko so zaposleni »tehnično« podkovani na tem področju ter ali imajo že kaj dejanskih izkušenj z informacijskimi nevarnostmi. Ugotovili smo (glej sliko 41), da je ravno polovica takšnih, ki so že imeli kdaj virus na svojem računalniku.



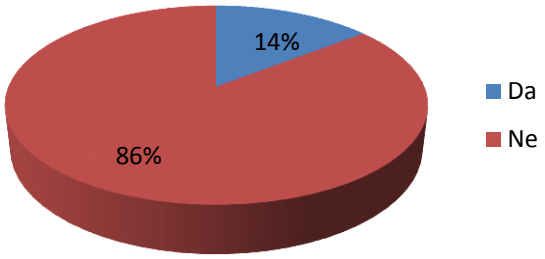
Slika 41: Prisotnost virusa na računalniku

Nato nas je zanimalo, če poznajo razliko med virusom, črvom in trojanskim konjem. Rezultate tega vprašanja prikazuje slika 42, kjer je kar 83% zaposlenih odgovorilo, da pozna razliko med virusom in trojanskim konjem.



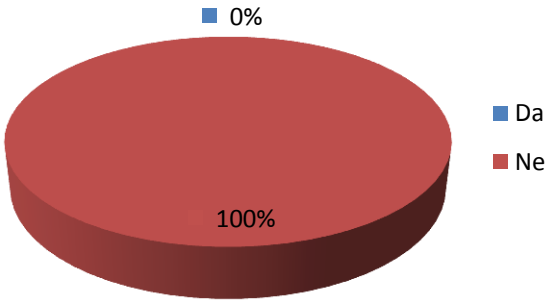
Slika 42: Poznavanje razlik med virusom in trojanskim konjem

V negativni smeri pa nas je presenetil odgovor o poznavanju spletnih strani glede virusov in nevarnosti, saj smo ugotovili (glej sliko 43), da kar 86% ne pozna nobene spletne strani o računalniških virusih in drugih nevarnostih.



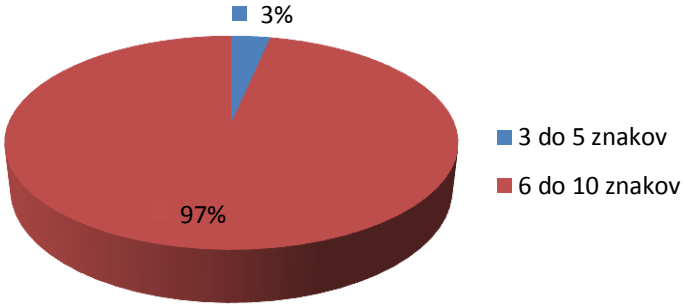
Slika 43: Poznavanje spletnih strani o virusih in drugih nevarnostih

Geslo je pomemben element zagotavljanja informacijske varnosti. Vemo pa tudi, da imajo zaposleni veliko opraviti z različnimi gesli. Ugotovili smo (glej sliko 44), da ti geslo varujejo in ga ne zaupajo ostalim, čeprav glede na izkušnje in glede na rezultate predhodne raziskave, temu ni vedno tako.



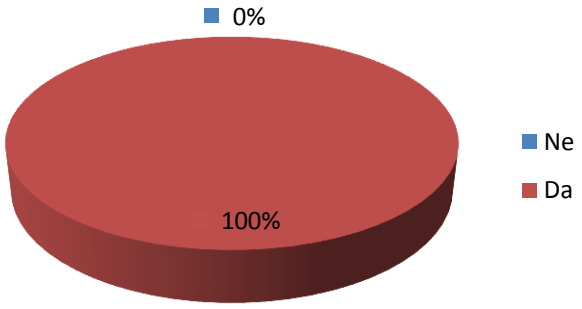
Slika 44: Varovanje gesla v smislu zaupanja le-tega ostalim

Pomembna varnostna lastnost gesla je njegova dolžina. Informativno nas je zanimalo, kako dolga gesla si zaposleni izbirajo. Ugotovili smo (glej sliko 45), da si 97% zaposlenih izbira gesla, ki so dolga od 6 do 10 znakov.



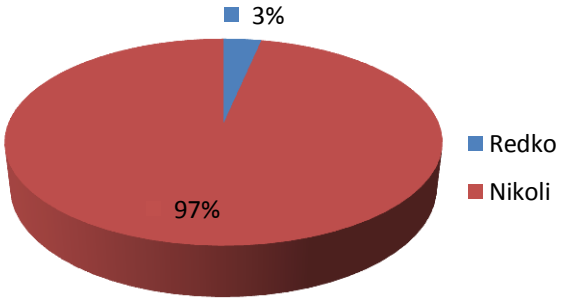
Slika 45: Dolžina gesla, ki si ga običajno izbirajo učitelji

Vsi učitelji se strinjajo s predlogom (glej sliko 46), da bi se na šoli uvedel tečaj o varni rabi računalnika in interneta.



Slika 46: Mnenje učiteljev o uvedbi tečaja o varni rabi računalnika in interneta

Za konec smo učitelje povprašali, če so o podobnih nevarnostih že sami kaj razmišljali. 3 % jih je pošteno priznalo, da na te stvari pomislijo, čeprav zelo poredko, preostalih 97 % pa o tem niti ne razmišlja. Rezultate tega vprašanja prikazuje slika 47.



Slika 47: Na splošno razmišljanje o internetnih nevarnostih

Povzetek raziskave

Raziskava, ki smo jo opravili med učitelji, je pokazala, da vsi učitelji uporabljajo IKT praktično vsakodnevno. Računalnik uporabljajo pretežno za internet in kot delovni pripomoček. Internet uporabljajo največ za elektronsko pošto ter za iskanje informacij.

Kar se tiče ozaveščanja o internetnih nevarnostih, smo ugotovili, da se večina učiteljev teh nevarnosti zaveda. Izmed nevarnosti pa poznajo najbolj pogoste, kot so: virus, neželena pošta ter kraje in zlorabe podatkov.

Ugotovili smo, da 86% učiteljev ne pozna spletnih strani o virusih in drugih nevarnostih. Sklepamo pa, da je slabo poznavanje spletnih strani predvsem posledica nezanimanja, saj je kar 97% učiteljev potrdilo, da o tovrstnih stvareh niti ne razmišljajo.

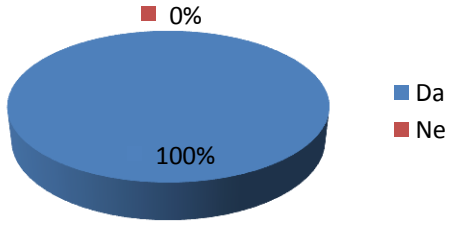
Kot rešitev v tej smeri predlagamo izobraževanje in ozaveščanje o informacijski varnosti, ki bi se ga po rezultatih raziskave, učitelji z veseljem udeležili.

4.3 Analiza stanja z vidika uporabnikov - učencev

V podobni raziskavi, kot učitelji, so sodelovali tudi učenci Osnovne šole Neznanih talcev Dravograd. Sodelovalo je 85 učencev od 4. do 9. razreda.

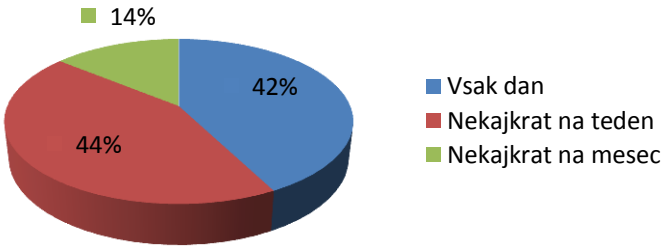
Raziskali smo, kako pogosto uporabljajo računalnik, kaj je tisto, kar na njem najraje počno ter koliko so seznanjeni z najrazličnejšimi nevarnostmi glede uporabe računalnika.

Rezultati na sliki 48 kažejo, da je računalnik med učenci sila priljubljen, uporabljajo ga namreč vsi učenci naše šole, ki so sodelovali v raziskavi.



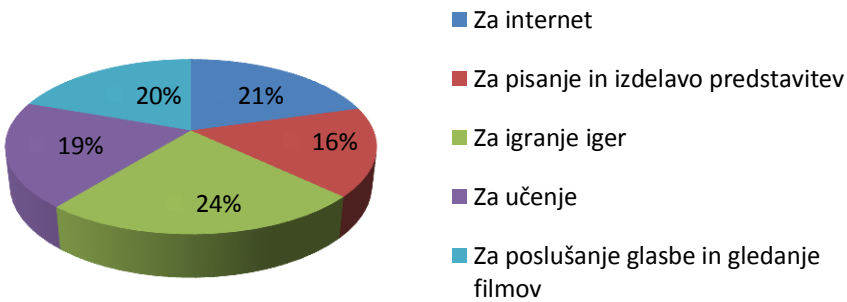
Slika 48: Uporaba računalnika med učenci

Nato smo ugotovili (glej sliko 49), da 42% učencev uporablja računalnik vsak dan, 44% uporablja računalnik nekajkrat na teden, preostalih 14% pa ga uporablja nekajkrat na mesec.



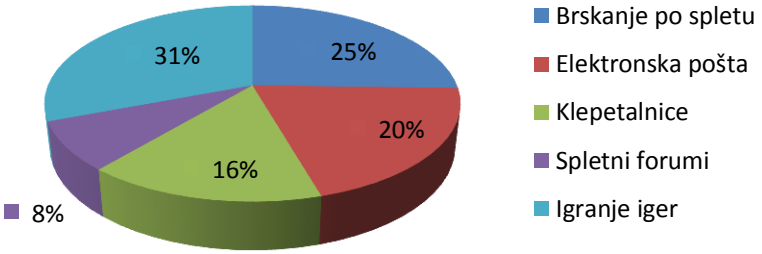
Slika 49: Pogostost uporabe računalnika med učenci

Učenci računalnik najpogosteje uporabljajo za igranje iger, internet, poslušanje glasbe in gledanje video vsebin ter kot pripomoček za učenje. Rezultate odgovoraov na to vprašanje prikazuje slika 50.



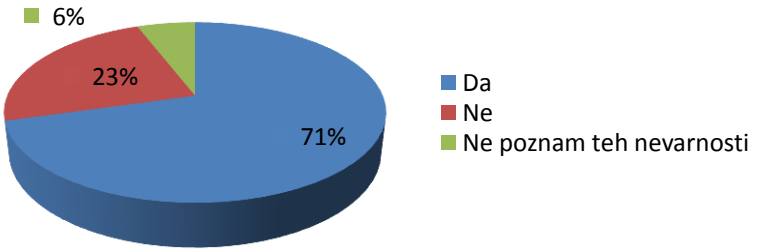
Slika 50: Namen uporabe računalnika

Rezultati raziskave so potrdili, da je internet med učenci zelo priljubljen, zato nas je zanimalo, za katere namene učenci internet uporabljajo. Ugotovili smo (glej sliko 51), da je na prvem mestu igranje iger, sledi brskanje po spletu, uporaba elektronske pošte, klepetalnic in spletnih forumov.



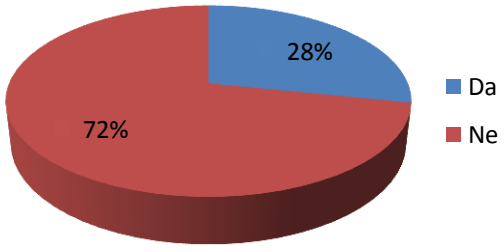
Slika 51: Namen uporabe interneta

Mediji veliko govorijo o internetnih nevarnostih, zato tudi rezultati naslednje raziskave niso presenetljivi. Ugotovili smo (glej sliko 52), da je 71% učencev že slišalo za internetne nevarnosti, preostalih 29% pa tega ne ve oz. ne pozna.



Slika 52: Poznavanje internetnih nevarnosti

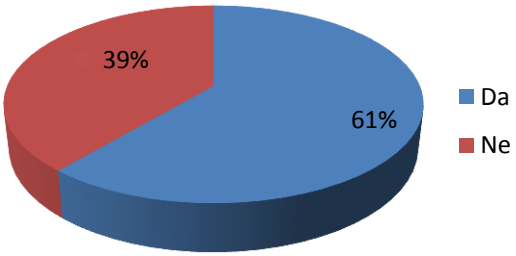
Ena izmed nevarnosti je povezana tudi z izgubo podatkov zaradi takšnih ali drugačnih razlogov. Na šoli pogosto slišimo, da je nekdo nekomu podatke izbrisal ali kako drugače poškodoval. Med učenci, ki so sodelovali v raziskavi, je 28% takšnih, ki so že kdaj izgubili podatke, shranjene na računalniku. Rezultate odgovorov na to vprašanje prikazuje slika 53.



Slika 53: Delež učencev, ki so že kdaj izgubili podatke, shranjene na računalniku

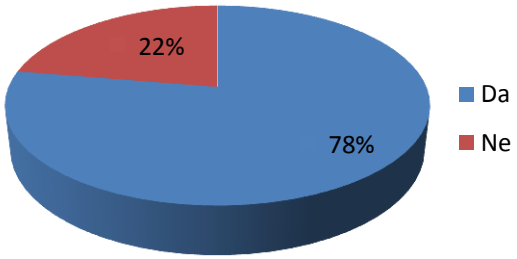
Med učenci pogosto slišimo besedo računalniški virus, zato nas je zanimalo, če leti vedo, kaj je to. Ugotovili smo (glej sliko 54), da je 61% učencev takšnih, ki

pozna oz. ve nekaj o računalniškem virusu. Večina pozna virus kot nekaj nevarnega, kot nekaj, kar jim lahko računalnik pokvari.



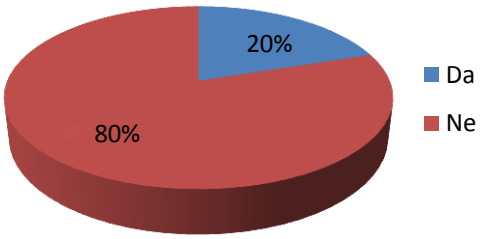
Slika 54: Poznavanje pojma računalniški virus

Slika 55 prikazuje, da je 78% učencev, ki so sodelovali v raziskavi, že imelo virus na računalniku.



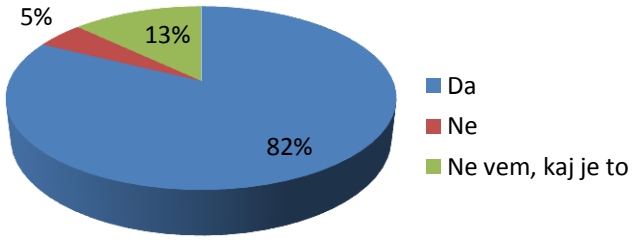
Slika 55: Prisotnost virusa na računalnikih učencev

Odstranitev virusa je večkrat zahtevno opravilo. Način odstranitve je tesno povezan z naravo virusa in orodjem, ki ga uporabljamo. Predhodno smo ugotovili, da je 78% učencev že imelo virus na računalniku, zato nas je zanimalo, koliko izmed njih bi virus znalo ali vsaj skušalo odstraniti. Ugotovili smo (glej sliko 56), da bi 20% učencev znalo oz. skušalo odstraniti računalniški virus.



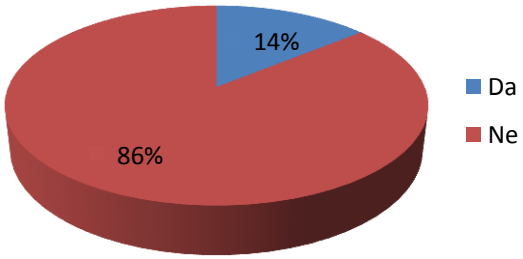
Slika 56: Delež učencev, ki bi znali ali pa bi bili pripravljeni odstraniti virus

Ugotovili smo (glej sliko 57), da 82% učencev tudi doma uporablja protivirusno programsko opremo.



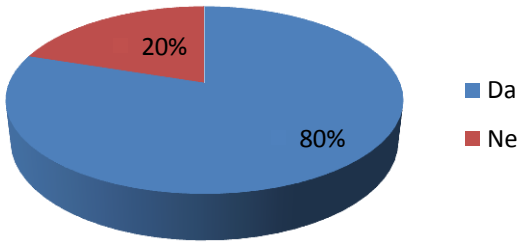
Slika 57: Uporaba protivirusne zaščite na domačih računalnikih

Veliko spletnih strani govori o nevarnostih uporabe računalnika in interneta. Slika 58 prikazuje, da kar 86% učencev teh strani ne pozna, še bolj verjetno pa je, da jih to ne zanima.



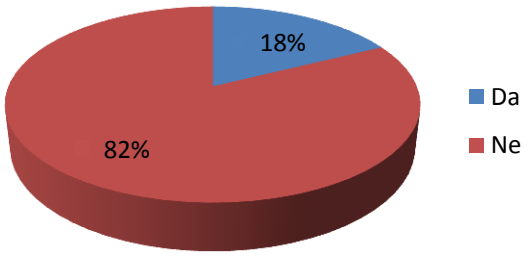
Slika 58: Poznavanje spletnih strani o internetnih nevarnostih

Zelo priljubljena med učenci je elektronska pošta, takoj za tem pa so to spletne klepetalnice. Pa se učenci zavedajo internetnih nevarnosti? Ugotovili smo (glej sliko 59), da se 80% učencev teh nevarnosti zaveda.



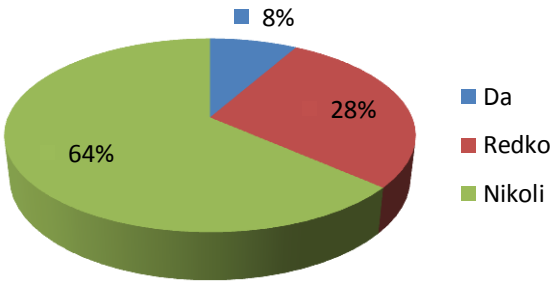
Slika 59: Zavedanje učencev o internetnih nevarnostih

Objava osebnih podatkov na internetu je dokaj pogosto početje, vemo pa tudi, da je takšno početje nevarno. In kaj o tem menijo učenci? 82% učencev meni (glej sliko 60), da svojih osebnih podatkov ne smejo javno objavljati.



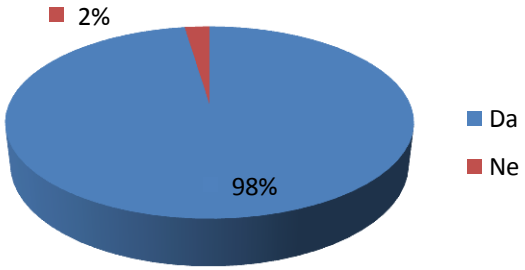
Slika 60: Mnenje učencev o objavi svojih osebnih podatkov

Kakšen je delež učencev, ki so že kdaj objavljali svoje podatke na internetu, pa si lahko ogledamo na sliki 61.



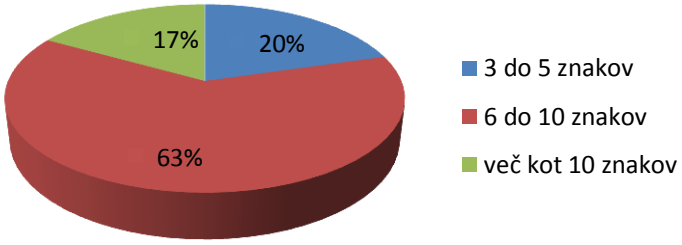
Slika 61: Delež učencev, ki so na internetu že kdaj objavili svoje osebne podatke

Nato smo učence vprašali, če vedo, kaj je to geslo. Ugotovili smo (glej sliko 62), da 98% učencev ve, kaj je to geslo, kar verjetno pomeni, da geslo tudi uporabljajo.



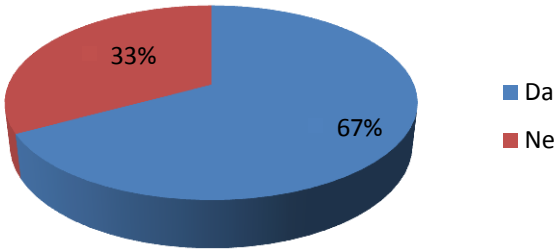
Slika 62: Poznavanje besede geslo

Ker je pri uporabi gesla pomembna njegova dolžina, nas je zanimalo, kako dolga gesla si učenci običajno izberejo. Ugotovili smo (glej sliko 63), da 63% učencev uporablja geslo, sestavljeno iz 6 do 10 znakov, 20% učencev uporablja gesla krajša od 6 znakov, preostalih 17% pa uporablja gesla, ki so daljša od 10 znakov.



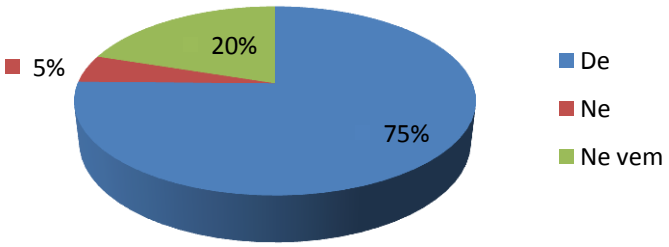
Slika 63: Dolžina gesel, ki jih uporabljajo učenci

Pomembno lahko na ozaveščanje o informacijski varnosti vplivajo tudi učitelji. Slika 64 prikazuje, da je bilo 67% učencev obveščenih o informacijski varnosti tudi s strani učiteljev.



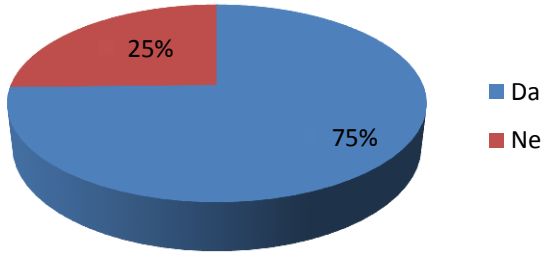
Slika 64: Ozaveščanje o informacijski varnosti s strani učiteljev

Zanimalo nas je, kaj menijo učenci o tečaju varne uporabe računalnika in interneta. Ugotovili smo (glej sliko 65), da se 75% s tečajem strinja, 20% je takšnih, ki ne vedo, ali tečaj potrebujejo ali ne, preostalih 5% pa meni, da tečaja ne potrebujejo.



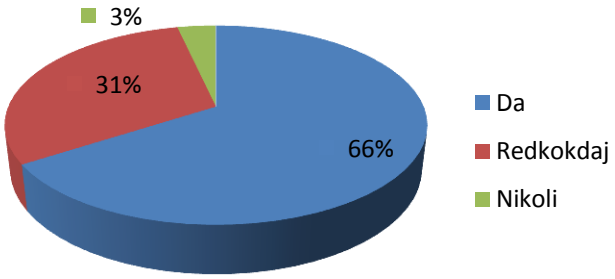
Slika 65: Mnenje učencev o tečaju varne rabe računalnika in interneta

Tudi pogovor s starši lahko veliko pripomore k izboljšanju informacijske varnosti. Ugotovili smo (glej sliko 66), da se je 68% učencev s starši že kdaj pogovarjalo o tej tematiki.



Slika 66: Ozaveščanje učencev s strani staršev

Na koncu smo učence vprašali, če so sami že kdaj pomislili na nevarnosti uporabe računalnika ter interneta. 65% jih je odgovorilo da so, 31% pravi, da redko pomislijo na to, preostali 4% pa še nikoli niso razmišljali o tem. Rezultate odgovora na to vprašanje prikazuje slika 67.



Slika 67: Razmišljanje učencev o nevarnostih uporabe računalnika ter interneta

Povzetek raziskave

Raziskava je pokazala, da učenci uporabljajo računalnik praktično vsakodnevno. Uporabljajo ga predvsem za igranje iger, gledanje video vsebin, kot pripomoček za učenje in seveda za internet.

Internet uporabljajo v največji meri za igranje iger, elektronsko pošto, iskanje informacij, udeležujejo pa se tudi forumov in klepetalnic.

Glede ozaveščenosti o internetnih nevarnostih smo ugotovili, da se učenci nevarnosti dokaj dobro zavedajo. Najverjetneje je to tudi posledica dobre informiranosti s strani elektronskih medijev in staršev.

Zanimivo je tudi to, da učenci pogosteje kot učitelji razmišljajo o informacijskih nevarnostih in posledično poznajo tudi več tovrstnih spletnih strani.

Podobno kot za učitelje bi bilo potrebno tudi za učence organizirati tečaj o informacijski varnosti. Za boljši učinek pa bi bilo potrebno vključiti še njihove starše.

4.4 Smernice za celovito zagotavljanje informacijske varnosti v osnovni šoli

Zagotavljanje informacijske varnosti mora biti sistematično in postopno. Pri izboljšanju informacijske varnosti moramo zajeti ali pa vsaj predvidevati večino morebitnih slabosti in nevarnosti. Upoštevati moramo trenutno stanje, zato je priporočljivo, da so nove rešitve združljive z obstoječo infrastrukturo.

Pri zagotavljanju informacijske varnosti smo upoštevali splošne smernice in tiste, ki smo jih ugotovili v opravljeni raziskavi.

Splošne smernice za izboljšanje informacijske varnosti:
- izboljšanje sistemske varnosti,
- izboljšanje podatkovne varnosti,
- izboljšanje omrežne varnosti in
- izboljšanje fizične varnosti.

Na podlagi obstoječih pomanjkljivosti, ki smo jih ugotovili v raziskavi med skrbniki IKT v slovenskih osnovnih šolah, predlagamo naslednje:
- obvladovanje informacijske varnosti mora biti kar se da enostavno,
- sistem mora biti enostaven za namestitev, upravljanje in vzdrževanje,
- rešitev mora biti zanesljiva in preizkušena,
- rešitev mora biti ali tehnično podprta ali pa vsaj dobro dokumentirana,
- izboljšati se mora varnost za vse uporabnike (pedagoški delavci, učenci…),
- zagotoviti je potrebno višjo varnost pri uporabi internetnih storitev,
- izboljšati je potrebno organizacijsko varnost.

4.4.1 Vidik skrbnika IKT

Sklepne ugotovitve raziskave, ki smo jo opravili med skrbniki IKT, so pokazale številne varnostne pomanjkljivosti, ki jih moramo izboljšati.

Sistemsko varnost najbolj ogrožajo uporabniki, predvsem zaradi neustreznih pravic, pomanjkljivega znanja ali pa tudi namernih dejanj. Zato priporočamo, da uporabniške račune z omejenimi pravicam kreiramo za vse uporabnike. Tako organizirani uporabniški računi nam bodo pomagali tudi pri spremljanju uporabniških aktivnosti, da bomo lahko ob nepravilnostih ustrezno ukrepali.

Skrb za varnost podatkov je zelo pomembna, saj ima lahko vsaka izguba le-teh nepopravljive posledice. Zato moramo vsakemu uporabniku omogočiti varnost in zasebnost njegovih podatkov.

Rezultati raziskave kažejo, da predstavlja največjo grožnjo uporaba interneta. Te grožnje zagotovo ne bomo popolnoma odpravili, lahko pa jo z nekaterimi varnostnimi mehanizmi kot sta npr. požarna pregrada ali pa namestniški strežnik v povezavi z orodjem za filtriranje spletnih strani ali ključnih besed vsaj delno omilimo.

Napake uporabnikov so pogosto posledica neznanja. Zato je potrebno vse uporabnike primerno izobraziti o ustrezni rabi šolskega informacijskega sistema, predvsem pa o nevarnostih njegove uporabe. V šoli je potrebno oblikovati varnostno politiko informacijskega sistema, ki se je morajo uporabniki strogo držati. Prav tako pa morajo biti seznanjeni tudi z ukrepi v primeru kršitev.

4.4.2 Vidik učiteljev

Ugotovili smo, da učitelji IKT uporabljajo vsakodnevno, zavedajo se nekaterih nevarnosti, ampak jim ne posvečajo dovolj pozornosti. Menimo, da je zato potrebno v šoli organizirati program ozaveščanja o informacijski varnosti. Učitelji se morajo programa udeležiti na začetku šolskega leta, o vseh morebitnih spremembah pa jih nato obveščamo sproti. Program lahko na šoli izvede skrbnik IKT ali pa se učitelji udeležijo zunanjih srečanj.

Zavedamo se, da je potrebno poleg ozaveščanja o informacijski varnosti marsikaj storiti tudi na tehničnem področju.

Učitelji veliko uporabljajo internetne storitve, kot so: elektronska pošta, svetovni splet, zato je potrebno z ustreznimi varnostnimi mehanizmi poskrbeti za varnost le-teh.

Nič manj ni pomembna varnost na lokalni ravni. Učitelji imajo namreč večino dokumentacije shranjene v elektronski obliki. Gre za dokumente (npr. gradiva, priprave, kontrolne naloge…), ki so nujno potrebni za učni proces, njihova izguba ali zloraba pa ima lahko tudi nepopravljive posledice. Zato je potrebno poskrbeti za primerno varnost in zasebnost teh podatkov.

4.4.3 Vidik učencev

Vidik zagotavljanja varnosti za učence je dokaj podoben tistemu za učitelje. Učenci uporabljajo računalnike za internetne storitve, šolska opravila ter za razvedrilo. Informacijsko varnost v šoli najbolj ogrožajo internetne storitve, predvsem brskanje po internetu, uporaba socialnih omrežij, klepetalnic in elektronske pošte.

Učenci, podobno kot učitelji, poznajo kar nekaj teh nevarnosti, ampak se jih pogosto ne zavedajo. Zato je potrebno za njih pripraviti podoben program ozaveščanja o informacijski varnosti kot za učitelje. Seveda pa ozaveščanje učencev ni le naloga skrbnika IKT in učiteljev ampak tudi njihovih staršev.

Za vzpostavitev primerne informacijske varnosti potrebujemo tudi nekatere tehnične ukrepe. Za razliko od učiteljev so učenci tisti, ki marsikatero dejanje izvedejo namenoma, kljub temu da se tega zavedajo. V tem primeru pa je potrebno nekatere storitve onemogočiti. Tipičen primer je recimo obisk neprimerne spletne strani.

Tudi učenci vedno več uporabljajo računalnik pri pouku. Izdelki, narejeni z računalnikom, so za učence zelo dragoceni, saj dobijo učenci na podlagi teh tudi oceno. Vse skupaj pa nato vpliva na splošni učni uspeh in nadaljnje šolanje. Zato moramo tudi učencem omogočiti varnost in zasebnost njihovih podatkov.

4.4.4 Tehnični vidik

Da lahko zagotovimo ustrezno informacijsko varnost, moramo imeti tudi ustrezno IKT opremo. Šole računalnike kupujejo preko razpisov, nekaj omrežne opreme priskrbi ministrstvo.

Raziskava je pokazala, da so šole dobro opremljene z računalniki, saj ima kar 74 % šol od 50 do 150 računalnikov. Število računalnikov in njihova zmogljivost pa vpliva tudi na informacijsko varnost. Več kot je računalnikov, več je tudi možnih groženj za informacijski sistem.

Pri uporabi strojne opreme šole kaj dosti ne morejo izbirati, saj je večina računalniške opreme kupljene na razpisih. Za vsakdanjo uporabo je ta oprema povsem dovolj. Lahko pa se zgodi, da starejši računalniki ne bodo več dovolj zmogljivi za poganjanje novejšega operacijskega sistema in protivirusnih programov. Takšne računalnike moramo nadgraditi, zamenjati oz. jih kako drugače usposobiti za ustrezno delovanje.

Pri zagotavljanju omrežne varnosti igra pomembno vlogo infrastruktura omrežja, ki jo uporabljamo.

Nekatera omrežna oprema nima vgrajenih ustreznih varovalnih mehanizmov ali pa enostavno ni dovolj zmogljiva. Poleg ustrezne omrežne opreme je pomembna tudi organizacija omrežja. Tako lahko npr. s segmentacijo omrežja medsebojno zavarujemo posamezne segmente omrežja, hkrati pa tudi izboljšamo zmogljivost delovanja.

Pri vzpostavitvi internetne povezave ter pri urejanju omrežne infrastrukture šolam svetujemo, da se obrnejo na Arnes. Če je tehnično izvedljivo, naj bo Arnes tisti, ki vam zagotavlja varnost internetne povezave ter poskrbi za segmentacijo omrežja.

Nadaljnja infrastruktura omrežja je bolj ali manj odvisna od šol samih. Glede na to, kar smo ugotovili, bi šolam priporočali vsaj še naslednje ukrepe, za izboljšanje informacijske varnosti:

- postavitev domenskega strežnika za overjanje uporabnikov,
- postavitev podatkovnega strežnika za centralno shranjevanje podatkov,
- postavitev namestniškega strežnika z možnostjo filtriranja spletnih strani.

Z uporabo strežnika izboljšamo varnost podatkov, sistemsko varnost in varnost omrežja, poleg tega pa veliko pridobimo na samem času, saj je upravljanje takšnega sistema bistveno hitrejše.

Priporočljivo je, da uporabimo domenski strežnik, saj lahko s tem lažje upravljamo s pravicami uporabnikov, poleg tega pa so podatki o uporabnikih shranjeni na enem mestu, kar še dodatno pripomore k višji varnosti.

Ustrezno organizirani uporabniški računi znatno izboljšajo sistemsko varnost. V raziskavi smo ugotovili, da ima največ šol uporabniške račune izdelane le za zaposlene, z vidika varnosti pa to zagotovo ni rešitev. Največjo nevarnost predstavljajo ravno učenci, zato je potrebno uporabniške račune dodeliti tudi njim. S pomočjo ustreznega strežnika lahko vodimo uporabniške račune za vse

uporabnike, z ustreznimi pravicami pa lahko izboljšamo tako sistemsko kot tudi podatkovno varnost. Po potrebi lahko uporabniške aktivnosti nadziramo ter uporabnike ob morebitnih nepravilnostih na to opozorimo.

Uporaba podatkovnega strežnika je naslednja stvar, ki se je praktično ne moremo izogniti. Nemogoče je namreč skrbeti za varnost podatkov, ki so razpršeni na različnih lokacijah. Centralno shranjevanje podatkov je pogoj za uspešno varnostno kopiranje in arhiviranje le-teh.

Z namestniškim strežnikom lahko veliko pripomoremo k boljši omrežni varnosti, saj predstavlja brskanje po internetu eno izmed hujših groženj za šolski informacijski sistem.

Zagotoviti moramo tudi fizično varnost dobrin informacijskega sistema. Običajno objekt varujemo z alarmnimi napravami oz. osebjem za varovanje, na varovanje ostalih stvari pa velikokrat pozabimo. Dobrine informacijskega sistema morajo biti fizično zaščitene pred nepooblaščenim osebjem, pa tudi pred naravnimi nesrečami, kot sta npr. požar in poplava.

Predvidevamo, da bo šolam na začetku največjo finančno oviro predstavljal nakup strežnika. Ampak glede na to, da imajo šole dovolj osebnih računalnikov, svetujemo, da sprva v ta namen uporabijo kar nekoliko zmogljivejši osebni računalnik.

Z vidika zagotavljanja varnosti na strežniku je zelo pomemben trdi disk. Priporočljivo je, da uporabimo RAID podatkovno polje z dvema ali več diski. RAID lahko uporabimo samo za podatke, če pa imamo diske primernih kapacitet, je smiselno RAID uporabiti kar za celoten sistem.
Dolgoročno priporočamo uporabo namenskega strežniškega računalnika. Takšen strežnik ima vgrajene hitrejše in zmogljivejše komponente, izboljšano ima hlajenje ter napajanje in je tako v bistvu prilagojen za neprestano delovanje vseh 24 ur na dan in 365 dni v letu.

Strežniškemu računalniku moramo nujno zagotoviti ustrezno brezprekinitveno napajanje, da ga lahko v primeru izpada električne energije vsaj varno izklopimo. Naprave za zagotavljanje brezprekinitvenega napajanja (UPS) lahko hkrati tudi ščitijo pred prenapetostnimi sunki in udari strele. Te naprave so redkeje objavljene na razpisih, zato jih morajo šole kupiti same. Pred nakupom takšne naprave moramo predvsem preveriti, če njena zmogljivost ustreza našim zahtevam.

Strežnik mora biti nameščen v posebnem varovanem prostoru, do katerega ima dostop le pooblaščena oseba. Prostor mora biti zaščiten pred požarom, poplavami in drugimi naravnimi nevarnostmi. Priporočljivo je, da je prostor klimatiziran, saj lahko drugače, sploh v poletnem času, pride do pregrevanja komponent in okvare strežnika.

Namenski strežniki imajo vgrajena tudi posebna fizična varovala, ki onemogočajo nepooblaščeno ugašanje in ponovni zagon strežnika.

Zelo pomembne so tudi nastavitve v samem BIOS-u. Onemogočiti moramo nalaganje sistema z optičnih medijev ter zunanjih izmenljivih nosilcev, poleg tega moramo dostop do BIOS-a zaščititi z geslom. Svetujemo, da takšne nastavitve za BIOS uporabimo tudi na ostalih računalnikih ali pa vsaj na tistih, ki jih za delo uporabljajo učenci.

Na varnost pomembno vpliva tudi uporabljena programska oprema. Operacijski sistem je tisti, na katerem sloni praktično celotna sistemska varnost. Ugotovili smo, da sta na osnovnih šolah največ v uporabi Windows XP in Windows 7. Rezultat je razumljiv, saj ministrstvo zagotavlja brezplačno licenco za njuno uporabo in tudi za program Microsoft Office. Windows 7 vsebuje številne varnostne izboljšave v primerjavi s predhodnimi verzijami, zato priporočamo prehod z Windows XP na Windows 7, kjer je to mogoče. To pa ne pomeni, da uporaba najbolj priljubljenega sistema Windows XP za šole ni primerna, le pri zagotavljanju sistemske varnosti smo nekoliko omejeni.

Šolam svetujemo, da na delovnih postajah preizkusijo tudi operacijski sistem Linux. Linux je brezplačen, poleg tega ga odlikuje varnost in zanesljivost delovanja. Nekatere distribucije pa lahko učinkovito uporabimo na manj zmogljivih računalnikih. Menimo, da popoln prehod na Linux trenutno ni mogoč, saj vse več didaktičnih programov zahteva Windows okolje.

Priporočamo, da pričnejo šole najprej uporabljati Linux na manj zmogljivih računalnikih, kjer uporaba operacijskega sistema Windows XP oz. Windows 7 ni mogoča. Prav tako priporočamo uporabo Linux okolja v javnih prostorih šole (npr. na hodnikih, v avli, v knjižnicah, v e-učilnicah…). Ti računalniki in njihovi uporabniki predstavljajo za šolski sistem zelo veliko nevarnost, saj nad njimi običajno nimamo nadzora. Ker se ti računalniki uporabljajo pretežno za internet, morajo biti varni, zagotavljati pa morajo tudi zanesljivost ter hitrost delovanja in Linux je ravno idealen za takšne pogoje.

Kljub vsem varnostnim mehanizmom ne smemo pozabiti na uporabo protivirusnih programov. Šole imajo trenutno licenco za uporabo protivirusnega programa F-Secure. Program deluje dokaj dobro, a ima tudi svoje slabosti. Verjetno je največja slabost zelo velika poraba sistemskih virov. Nekateri manj zmogljivi računalniki postanejo na takšen način praktično neuporabni. Priporočamo, da šole na takšne računalnike namestijo katerega od brezplačnih protivirusnih programov.

Nekakšna alternativa ali mogoče celo dopolnitev je uporaba programa Deep Freeze, do katerega imajo šole prav tako pravico uporabe. Program po ponovnem zagonu računalnika vrne računalnik na prvotno sistemsko stanje. Ugotovili smo, da kar nekaj šol uporablja tudi to rešitev. Verjetno je največja slabost omenjenega programa zamudno nameščanje programske opreme, h kateri spadajo tudi varnostne posodobitve sistema. Ker je takšen operacijski sistem zelo zamudno posodabljati z najnovejšimi varnostnimi popravki, se lahko kaj hitro zgodi, da so zadnje posodobitve že zastarele. Računalniki lahko s takšnimi sistemi predstavljajo resno grožnjo za informacijski sistem. Če se odločimo za uporabo programa Deep Freeze, moramo računalnike predhodno temeljito pregledati s protivirusnim programom, namestiti najnovejše posodobitve operacijskega sistema ter upoštevati potrebne varnostne nastavitve.

Še boljša rešitev je uporaba strežniških uporabniških profilov. Ti profili sicer ne ščitijo samega sistema, za kar lahko poskrbimo z ustreznimi uporabniškimi pravicami. Lahko pa te profile uporabimo za povrnitev uporabnikovega okolja (predvsem namizja). Z njimi si lahko znatno poenostavimo tudi administriranje računalnikov. Pogoj za delovanje in uporabo računalniških profilov je centralni strežnik z ustrezno programsko opremo.

Ne glede na vrsto uporabljenega operacijskega sistema priporočamo še naslednje varnostne nastavitve:

- operacijski sistem redno posodabljajmo,
- vsi uporabniški računi morajo imeti dodeljena gesla,
- račun za goste je potrebno onemogočiti (pomanjkljivost v Windows XP),
- administratorski račun je smiselno preimenovati ali pa ga onemogočiti in izdelati drugega z najvišjimi pooblastili,
- vsi uporabniki naj imajo dodeljene nižje pravice od administratorskih.

4.4.5 Organizacijski vidik

Organizacijski vidik zagotavljanja informacijske varnosti je običajno še zahtevnejši kot pa sama tehnična izvedba. Tehnične rešitve so običajno v domeni skrbnika IKT ali zunanjih izvajalcev. Pogosto gre za uporabo že preizkušenih rešitev, ki jih samo nekoliko prilagodimo našim razmeram. Organizacijski vidik pa zahteva podporo in pomoč celotne organizacije. Prav tako ne moremo uporabiti že izdelanih rešitev, saj se vsaka organizacija razlikuje od druge.

Najverjetneje bo v šoli skrbnik IKT tisti, ki bo dal pobudo za izvajanje organizacijske varnosti. Skrbnik IKT mora pri tem pridobiti podporo vodstva ter ostalih zaposlenih, saj lahko le medsebojno sodelovanje privede do učinkovitih rezultatov.

Za zagotavljanje organizacijske varnosti v šoli predlagamo naslednje ukrepe:

- V šoli naj se ustanovi odbor za zagotavljanje organizacijske varnosti. Sestavo odbora naj predlaga skrbnik IKT, ki se pri tem posvetuje z vodstvom šole. Odbor naj sestavljajo učitelji iz različni predmetnih področij in predstavniki tehničnega ter administrativnega osebja.

- Analizirati je potrebno šolski informacijski sistem ter ovrednotiti njegove vire. Priporočljivo je, da za vsak vir prepoznamo relevantno grožnjo ter ocenimo verjetnost uresničitve in stopnjo ranljivosti.

- Izdelati je potrebno varnostno politiko informacijskega sistema.

- Izdelati je potrebno navodila in priporočila za varno uporabo informacijskega sistema.

- Organizirati oz. oblikovati je potrebno program ozaveščanja o informacijski varnosti.

Vsa dokumentacija mora biti objavljena na vidnem mestu, njena vsebina pa mora biti napisana jasno in razumljivo.

Z vsebino dokumentacije morajo biti seznanjeni vsi šolski uporabniki, ki so svojim podpisom potrdijo, da se z navedenim strinjajo.

5 PRENOVA INFORMACIJSKEGA SISTEMA V OŠ NEZNANIH TALCEV DRAVOGRAD

Prenovo informacijskega sistema v OŠ Neznanih talcev Dravograd smo izvedli v skladu s predlaganimi smernicami in z dobrimi praksami, ki se uporabljajo v tujini. Upoštevali smo naslednje smernice za izboljšanje informacijske varnosti:

- V šoli moramo vzpostaviti primerno organizacijsko varnost.
- Izboljšati moramo podatkovno, omrežno ter fizično varnost informacijskega sistema.
- Poleg splošnih smernic se bomo trudili odpraviti tudi večino slabosti, ki smo jih ugotovili v raziskavi za skrbnike, učitelje ter učence.
- Pri prenovi bomo upoštevali obstoječe stanje. Večino sprememb bomo skušali realizirati z najmanjšimi možnimi stroški, z uporabo lastnih virov.

5.1 Predstavitev organizacije

Na OŠ Neznanih talcev Dravograd je okoli 80 redno zaposlenih učiteljev. Šolo letno obiskuje okoli 500 učencev. K matični šoli spadajo še 4 podružnice šole, ki se nahajajo v bližnji okolici.

Tehnološko prelomnico je šola pa tudi podružnice doživela leta 2006. Tega leta smo morali zaradi uvedbe devetletke in njenih novosti kar dodobra prestrukturirati celotno šolo. Med večje pridobitve štejemo izgradnjo nove multimedijske knjižnice in računalniške učilnice. Spremenila pa se je tudi celotna fizična in logična infrastruktura šolskega omrežja. Vse prostore na šoli smo opremili s komunikacijskimi priključki.

Proces informacijskega razvoja smo peljali naprej v letu 2009. V tem letu smo vse učilnice opremili s projektorji in ostalo multimedijsko opremo. V omrežje smo vključili dodatno vozlišče za potrebe nove računalniške učilnice v prvi triadi, ki jo imamo namen postaviti oz. prenoviti v bodoče.

Glede na opravljeno raziskavo v zvezi s številom računalnikov na šoli lahko trdimo, da spadamo med bolje opremljene šole v Sloveniji. S pomočjo rednih razpisov MŠŠ in nabave v lastni režiji smo na šoli od leta 2006 do danes pridobili približno 90 osebnih računalnikov, nekaj prenosnikov in ostalo opremo. Na šoli je tako trenutno okoli 150 računalnikov. Vsi računalniki so povezani v lokalno omrežje in imajo hkrati tudi širokopasovni dostop do interneta. Dobro so opremljene tudi naše podružnične šole. Vse imajo širokopasovni dostop do interneta ter dobro računalniško opremo.

5.2 Trenutno stanje

Dostop do interneta in osnovne nastavitve na usmerjevalnik nam ureja Arnes. Na usmerjevalniku, ki obenem služi kot požarna pregrada, so omogočeni filtri »IP

access list«. Na določenem vmesniku je definiran en filter za vhodni (angl. inbound access list) in en filter za izhodni promet (angl. outgoing access list).

Na logičnem nivoju imamo omrežje razdeljeno na dva dela. Prvi del omrežja je namenjen administrativnim delavcem, drugi del pa učiteljem in učencem. Ločitev omrežja je izvedena na glavnem stikalu. Vsebina podatkov, s katerimi razpolagajo člani prve – t.i. administrativne skupine, je s stališča varnosti bolj občutljiva in zahteva višjo stopnjo varovanja, zato je računalnikom v pedagoškem delu omrežja preprečeno "prisluškovanje" (angl. sniffing) prometa, ki poteka na administrativnem delu omrežja.

V šoli pretežno uporabljamo operacijski sistem Windows XP, ponekod pa tudi Windows 7. Varnost zagotavljamo z dokaj rednimi posodobitvami in omejenimi uporabniškimi pravicami. Povsod uporabljamo tudi protivirusne programe, ki se samodejno redno posodabljajo. V računalniški učilnici in knjižnici sistem dodatno varujemo še s programom DeepFreeze.

Za prijavo v sistem uporabljamo naslednjo politiko uporabniških računov:

- V računalniški učilnici in knjižnici uporabljamo za vse uporabnike enotne uporabniške račune.
- V kabinetih in pisarnah uporabljajo uporabniki svoje osebne uporabniške račune.

Za varnost podatkov skrbijo uporabniki sami. V prostorih knjižnice in računalniške učilnice, kjer je sistem varovan še s programom DeepFreeze, uporabniki shranjujejo podatke na particijo D. Na sistemsko particijo C zaradi zaščite namreč ni mogoče trajno shranjevati podatkov. Uporabniki po ostalih prostorih podatke običajno shranjujejo v privzeto mapo »Moji dokumenti«. Uporabnikom pogosto svetujemo, da si naj podatke shranijo tudi na kakšen zunanji medij (npr. USB pomnilnik). Občasno pa uporabnikom podatke shranimo tudi na optične medije.

Med storitvami, ki jih šolski uporabniki največ uporabljajo, prevladuje uporaba interneta. Učenci uporabljajo internet pri pouku, kjer z brskanjem po spletnih straneh, pridobivajo koristne informacije in se učijo novih znanj. V zadnjem času pa je vedno več v uporabi tudi šolska spletna učilnica. Seveda ne moremo mimo uporabe interneta v prostem času. V šoli lahko učenci uporabljajo računalnike tudi v nekaterih dneh po pouku. Takrat ti uporabljajo internet za vse mogoče stvari. V raziskavi, ki smo jo izvedli v šoli, smo ugotovili, da največ učencev igra spletne igre ter uporablja elektronsko pošto.

Tudi med učitelji je uporaba interneta dokaj pogosta. Raziskava, ki smo jo izvedli v šoli, je pokazala, da učitelji računalnik največ uporabljajo ravno za internet. Med internetnimi storitvami pa je v ospredju iskanje informacij po spletu ter elektronska pošta. Vedno več učiteljev uporablja tudi spletne učilnice, tako za potrebe izobraževanja kot tudi za izvedbo pouka.

Izmed splošnih programov v šoli največ uporabljamo Microsoft Word, Microsoft Excel in Microsoft Power Point. Poleg tega pa učenci uporabljajo tudi nekaj programov, ki so vezani izključno na pouk. Tako recimo pri tehnični vzgoji uporabljajo program za tehnično risanje ciciCAD. Pri likovni vzgoji uporabljajo

več različnih programov, kot so: Slikar, ArtRage, TuxPaint, Gimp. Pri fiziki pa uporabljajo program Edison, ki je namenjen risanju in simulaciji elektronskih vezij.

V šoli uporabljamo tudi program Lo.Polis. Gre za program, ki je zasnovan kot »šolsko mesto« in je sestavljen iz različnih modulov. Program uporabljamo za vpisovanje ocen, izpis spričeval in obvestil, vpis učencev, izdelavo urnikov in podobne stvari, ki se nanašajo na učence in njihove ocene. Gre za mrežno aplikacijo, kjer mi kot uporabniki dostopamo do baze podatkov, ki so shranjeni na oddaljeni lokaciji podjetja Logos. V šoli uporabljajo ta program vsi učitelji, saj ga potrebujejo za vpis in pregledovanje ocen. Poleg učiteljev uporablja program še ravnatelj, psihologinja, socialna delavka in tajnica. Administrator programa je skrbnik IKT, ki je zadolžen za dodeljevanje uporabniških imen, gesel in dostopnih pravic.

Knjižničarka uporablja program WinKnj, ki je namenjen računalniškemu evidentiranju fizičnega ter elektronskega gradiva. Baza podatkov se nahaja na samem lokalnem računalniku.

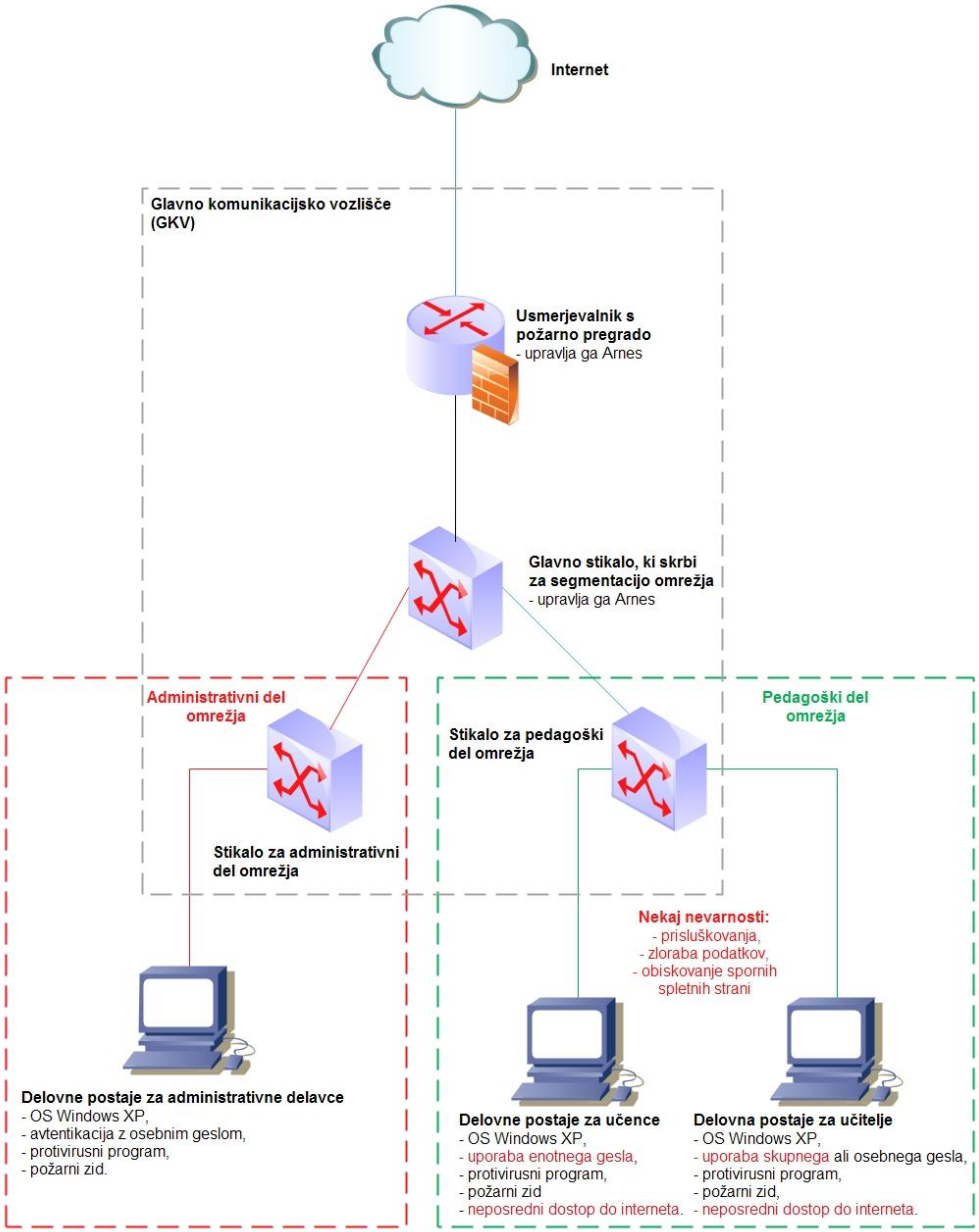
Administrativno osebje poleg že omenjenih internetnih storitev vsakodnevno uporablja še program SAOP, ki je namenjen računovodsko knjigovodskim storitvam. Program uporablja enotno bazo podatkov, do katere imajo dostop le pooblaščeni uporabniki. Uporabniki se v program prijavijo s svojim uporabniškim imenom in geslom, ki jim ga je dodelil administrator programa SAOP. V našem primeru program SAOP administrira kar podjetje, ki program razvija. Program trenutno uporablja pet uporabnikov.

Posebno pozornost in visoko stopnjo varnosti zahtevata tudi spletni storitvi, ki jih uporablja administrativno osebje v šoli.

Prva storitev je namenjena vodenju in organiziranju delovnih mest, zaposlenih na šoli. Storitev je dostopna na portalu Ministrstva za izobraževanje, znanost, kulturo in šport. Dostop do portala imajo pooblaščene osebe s svojim osebnim certifikatom, ki ga je predhodno overila certifikatna agencija.

Naslednja storitev je uporaba portala ujp.net. Gre za portal Uprave Republike Slovenije za javna plačila. Preko tega portala spremljamo plačilni promet, ki poteka med šolo in ostalimi subjekti. Dostop do portala imajo prav tako le pooblaščene osebe s svojim osebnim certifikatom, ki je bil predhodno overjen od certifikatne agencije.

Na sliki 68 je prikazana infrastruktura šolskega omrežja pred prenovo.



Slika 68: Šolska infrastruktura pred prenovo

Raziskava, ki smo jo naredili med skrbniki IKT v slovenskih osnovnih šolah, je pokazala, da informacijsko varnost najbolj ogrožajo uporabniki s svojimi dejanji.

Na šoli zaznavamo, da največ groženj izvira od znotraj. Nekaj groženj je posledica slabo varovanega informacijskega sistema, nekaj pa jih s svojimi dejanji povzročajo uporabniki.

Grožnje, ki se pojavljajo zaradi pomanjkljive varnosti omrežja in neustrezne infrastrukture, so naslednje:

- trenutna požarna pregrada ne omogoča storitev filtriranja spletnih strani, zato učenci prosto obiskujejo spletne strani, ki ogrožajo informacijsko varnost;
- spremljanje prometa v omrežju ni mogoče, zato veliko groženj niti ne zaznamo;
- dostop do podatkov v omrežju zagotavljamo s funkcijo skupne rabe, kar lahko privede do nepooblaščenega dostopa do podatkov. Poleg tega pa lahko skupna raba podatkov sproži širjenje škodljive programske opreme v omrežju.

Grožnje, ki jih zaznavamo zaradi neustrezne sistemske varnosti, so naslednje:

- na več računalnikih uporabljamo program Deep Freeze, ki vrne sistem na prvotno stanje, ko ponovno zaženemo računalnik. Zaradi tega se pogosto dogaja, da so posodobitve sistema pa tudi ostale programske opreme (npr. spletni brskalniki) zastarele in z vidika varnosti neprimerne;
- lokalno vodeni uporabniški računi nam ne omogočajo skupinske politike urejanja uporabniških pravic, zato ni redek primer, ko ima nek uporabnik na sistemu neprimerne pravice ali nastavitve.

Zaradi neprimerne varnosti podatkov se pojavljajo naslednje grožnje:

- uporabniki shranjujejo podatke na enotno lokacijo, zato jih lahko hote ali nehote izbrišejo ali odtujijo ostali uporabniki;
- podatki uporabnikov se shranjujejo na lokalne diske osebnih računalnikov. V primeru okvare kakšnega izmed diskov, lahko pride do trajne izgube podatkov;
- baza podatkov in varnostna kopija programov WinKnj in SAOP sta shranjeni na lokalnem disku računalnika. V primeru okvare diska obstaja velika verjetnost izgube baze podatkov;
- varnostne kopije podatkov si pretežno izdelujejo uporabniki sami. Za varnostne kopije se trudi skrbeti tudi skrbnik IKT, vendar je to zaradi velike razpršenosti zelo težko izvedljivo;
- za arhiviranje podatkov skrbi skrbnik IKT, vendar je zaradi velike razpršenosti podatkov tudi to zelo oteženo;
- podatki so shranjeni le na lokaciji šole, zato lahko v primeru naravne katastrofe to pomeni trajno izgubo podatkov.

Grožnje, ki jih zaznavamo zaradi neprimerne organizacijske varnosti, so naslednje:

- neprimerna uporaba računalnika in opreme,
- neprimerna uporaba programov,
- neustrezno ravnanje z gesli,

- neustrezno ravnanje s podatki,
- neustrezno ravnanje z izmenljivimi mediji,
- neustrezno ravnanje z dokumenti,
- neprimerna uporaba svetovnega spleta in elektronske pošte.

Grožnje, ki jih zaznavamo zaradi neprimerne fizične varnosti, so naslednje:

- oprema ni varovana pred izpadi električne energije,
- pogosto je omogočen prost fizični dostop do računalnikov in opreme,
- računalniki z bazami podatkov nimajo zagotovljene redundance niti niso zaščiteni pred morebitnimi naravnimi katastrofami,
- računalniki z bazami podatkov se ne nahajajo v prostorih z ustreznimi klimatskimi pogoji, kar lahko sploh v poletnem času privede do odpovedi opreme.

5.3 Zahteve in izhodišče

Da bi zadostili smernicam za zagotavljanje informacijske varnosti, smo se v šoli odločili za temeljito prenovo informacijskega sistema. Vsem uporabnikom želimo zagotoviti primerno informacijsko varnost ter karseda omiliti grožnje, ki smo jih sedaj prepoznali.

Za izboljšanje informacijske varnosti moramo izboljšati:

- omrežno varnost – na tem področju moramo uporabnikom omogočiti varnost pri uporabi internetnih storitev, skrbniku omrežja pa možnost nadzora in evidentiranja dogodkov v omrežju;
- sistemsko varnost – na tem področju moramo skrbniku omogočiti centralno upravljanje uporabniških računov, ter možnost poenostavljenega upravljanja računalnikov;
- podatkovno varnost – tukaj moramo omogočiti varnost in zasebnost uporabniških podatkov ter podatkovnih baz;
- fizično varnost - za izboljšanje fizične varnosti moramo najprej izboljšati fizično varnost ključnih virov informacijskega sistema, kot so: baze podatkov, komunikacijska oprema, računalniki z občutljivimi podatki;
- organizacijsko varnost – na tem področju moramo pripraviti ustrezno dokumentacijo šolskega informacijskega sistema, kot je npr. varnostna politika, pravila, priporočila, navodila… Uporabnikom moramo zagotoviti primerna usposabljanja in izobraževanja na področju informacijske varnosti.

Upoštevali bomo omejenost s sredstvi, zato bomo v čim večji možni meri planirali izrabo lastnih sredstev. Zavedamo pa se, da bo za nekatere izboljšave potrebna tudi določena finančna podpora.

5.4 Zagotavljanje informacijske varnosti za pedagoške delavce in učence

Verjetno je najbolj pereč problem v osnovnih šolah ta, kako zagotoviti ustrezno varnost šolskega informacijskega sistema za učence. Nato pa se pojavlja tudi vprašanje, kako naj zagotovimo informacijsko varnost za učitelje, če enak sistem uporabljajo hkrati tudi učenci.

Po analizi in preizkušanju najrazličnejših rešitev, smo se odločili, da v šoli uporabimo Open School Server (OSS). Razlogi, zaradi katerih smo omenjeno odločitev sprejeli, so naslednji:

- operacijski sistem Suse Linux Enterprise Server (SLES), na katerem temelji omenjena rešitev, je znan kot izredno zanesljiv in varen,
- zelo dobra tehnična podpora,
- zelo dobra navodila za uporabo in namestitev sistema,
- enostavna namestitev in postavitev sistema v okolje,
- enostavno upravljanje s pomočjo uporabniku prijaznega spletnega vmesnika,
- združljivost z obstoječo programsko in strojno opremo ter okoljem,
- številne varnostne funkcije, ki se skladajo z našimi zahtevami.

5.4.1 Zagotavljanje sistemske varnosti

Ker zahteve za namestitev niso pretirano visoke, smo se odločili, da bomo sistem najprej namestili in preizkusili na zmogljivejšem osebnem računalniku. V računalnik smo najprej vgradili dodaten pomnilnik, disk ter mrežno kartico. Nadaljnja namestitev je enostavna in je potekala brez posebnih zapletov.

Prvi korak namestitve je namenjen razdeljevanju diska. Zaradi varnosti smo se odločili za zrcaljenje podatkov, uporabili smo »Software RAID«. Glede na to, da smo razpolagali z dvema dovolj velikima diskoma (500GB), smo se odločili, da zrcaljenje podatkov izvedemo za celoten sistem.

Med samo namestitvijo smo določili še močno geslo za uporabnika z vsemi pravicami, v sistemu Linux je to uporabnik root. Pred zaključkom namestitve smo vpisali še nekaj parametrov, povezanih z našo šolo, kot npr. koliko razredov in koliko oddelkov imamo ter koliko je na šoli učilnic. Sistem glede na te vrednosti pripravi uporabniške skupine.

Nato smo izbrali storitve, ki jih bomo na strežniku potrebovali. Izbrali smo samo tiste najbolj nujne, saj več kot je delujočih storitev, več nevarnosti za sistem obstaja. Za optimalno delovanje in upravljanje smo omogočili naslednje storitve:

- LDAP imenik,
- datotečni strežnik - Samba,
- DNS in DHCP strežnik,
- namestniški strežnik s podporo filtriranja spletnih strani,
- SSH za oddaljeno upravljanje sistema,
- spletni strežnik za dostop do spletnega vmesnika, ki omogoča upravljanje sistema.

Vse storitve, razen SSH, so na voljo le odjemalcem znotraj omrežja, zato le-te ne predstavljajo dodatnih nevarnosti za sistem ter omrežje.

Številni podatki (uporabniški podatki, nastavitve omrežja, nastavitve sistema …) so shranjeni v LDAP imeniku. Dostop do tega imenika ima le administrator, ki smo ga določili ob namestitvi sistema. Čeprav so gesla shranjena v obliki prstnega odtisa (NT metoda), je pomembno, da administratorsko geslo za dostop do LDAP imenika

skrbno zavarujemo. Ker imajo do LDAP imenika dostop tudi ostale storitve na strežniku, je zelo pomembna tudi varnost medsebojne povezave. V primeru, da se strežnik z LDAP imenikom nahaja na ločenem strežniku ali celo lokaciji, je nevarnost še toliko večja. Kljub temu, da se pri nas vse odvija na enem strežniku, smo med LDAP imenikom in ostalimi storitvami omogočili šifrirano povezavo (TLS protokol).

Med pomembne varnostne storitve na strežniku uvrščamo strežnik Samba. Samba deluje kot domenski kontroler in podatkovni strežnik, se pravi da skrbi za overjanje uporabnikov in hkrati omogoča dostop do datotek in map, ki se nahajajo na Linux sistemu. Podatke o uporabniških računih dobi iz LDAP imenika, za overjanje pa potrebuje ime računalnika ter uporabniški račun.

Samba deluje podobno kot Windows Active Directory, s tem da nekaterih funkcionalnosti ne omogoča. Tako recimo ne podpira urejanja skupinske politike (angl. Group policy), ki bi jo lahko drugače uporabili pri nastavitvah, uporabniških pa tudi ostalih pravic. Omenjeno pomanjkljivost smo odpravili z vnaprej pripravljenimi uporabniškimi profili, ki smo jih podrobneje opisali v nadaljevanju. Poleg profilov si lahko pri upravljanju pomagamo tudi z ukazom, ki se izvede ob prijavi uporabnika v sistem. Izvedemo lahko tudi več ukazov hkrati, če jih združimo v tako imenovano prijavno skripto. Takšno skripto lahko uporabimo recimo za časovno sinhronizacijo med strežnikom in odjemalcem ali pa za preslikovanje uporabniške mape v omrežni pogon.

Veliko smo na varnosti pridobili z uporabo ločenih uporabniških računov. Vsakemu šolskemu uporabniku smo izdelali lasten uporabniški račun. Učitelje smo dodelili v uporabniško skupino učitelji, učence pa v uporabniško skupino učenci. Uporabniški skupini se samodejno izdelata že ob namestitvi sistema. V uporabniški skupini učenci so tudi že oddelki, ki smo jih ob namestitvi določili. Poleg oddelkov imamo v sistemu tudi uporabnike, ki nam lahko služijo kot predloga za kreiranje uporabniških profilov.

Spletni vmesnik omogoča ročni vnos uporabnikov ali pa masovni uvoz iz vnaprej pripravljene datoteke. Odločili smo se za uvoz podatkov, saj bi bilo ročno vnašanje zelo zamudno. V Excelu smo pripravili ustrezno datoteko z uporabniki. Potrebovali smo uporabniško ime, ime, priimek, rojstni datum in geslo, za učence pa tudi oddelek. Uporabniške podatke smo pridobili iz programa LoPolis. Uporabniško ime učenca smo sestavili iz prve črke imena in njegovega priimka, zaradi morebitnih težav s šumniki pa smo le te odstranili. Pri določevanju gesel smo imeli na voljo dve možnosti:

- uporabnikom lahko dodelimo enotno geslo, ki ga morajo ob prvi prijavi spremeniti,
- ali pa jim tudi sami določimo geslo.

Pri učiteljih smo se odločili za prvo možnost, saj smo mnenja, da si znajo učitelji sami izbrati varno geslo.

Za učence smo uporabili drugo možnost. Naredili smo enostavni program, ki v Excelu generira gesla. Upoštevali smo pravila za generiranje dobrih gesel ter geslo sestavili iz 8 znakov, ki vsebujejo velike in male črke ter številke.

Zaščita uporabniškega profila

Uporaba ločenih uporabniških računov nam omogoča spreminjanje in prilagajanje uporabniških in sistemskih nastavitev (meni start, namizne ikone, nastavitve zaslona, barve ozadja…) na samem strežniku.

S profili omogočimo uporabnikom lastno delovno okolje, z ustrezno nastavitvijo profila pa lahko izboljšamo tudi sistemsko varnost. Glede na to, da sploh učenci zelo radi spreminjajo uporabniške profile, smo se odločili za uporabo predpisanega (angl. mandatory) profila.

Predpisani profil je posebna vrsta profila, shranjenega na strežniku, ki ima onemogočeno možnost spreminjanja. Predpisani profil je shranjen na strežniku, ki se pri prijavi naloži na delovno postajo. Uporabnik lahko začasno spremeni nastavitve, vendar se pri odjavi spremembe ne shranijo.

Za pripravo strežniškega uporabniškega profila smo najprej izdelali in uredili lokalni uporabniški profil, to je profil, ki se samodejno kreira ob prvi prijavi na delovno postajo. Pripravili smo start meni, izdelali bližnjice na namizju in ustrezne sistemske nastavitve. Spremenili smo še privzete poti za shranjevanje dokumentov, ki sedaj kažejo v uporabniško mapo, ki se nahaja na strežniku. Profil smo shranili na strežnik, in sicer v imenik, ki služi kot predloga za izdelavo profilov. Za učitelje je to imenik /tteachers za učence pa /tstudents. Ob uvozu uporabnikov v sistem se ta profil samodejno prekopira v profil uporabnikov.

V Windows 7 smo si pri prenašanju profila pomagali s programom Windows Enabler, saj drugače uporabniškega profila nismo mogli shraniti. Za vključitev profila, ki ga ni mogoče spreminjati (mandatory), smo morali datoteko ntuser.dat, ki se nahaja v imeniku uporabniškega profila, spremeniti v ntuser.man.

Zaščita pred virusi

Linux je znan kot dokaj varen pred virusi, zato uporaba protivirusnih programov na Linux sistemih ni tako zelo pogosta kot npr. v Windows okolju. Seveda pa tudi Linux ni imun na škodljivo programsko opremo, kar dokazuje čedalje več protivirusnih programov, namenjenih odprtokodnim sistemom. Glede na to, da na našem sistemu gostimo datoteke Windows odjemalcev, je nevarnost prisotnosti škodljive programske opreme še toliko večja. OSS ima vgrajen odprtokodni protivirusni program ClamAV. ClamAV pozna več kot 1 mio virusov, trojanskih konjev, makro virusov, črvov in ostale škodljive programske opreme. Pregledovati je zmožen številne vrste datotek, med njimi tudi na našem sistemu najbolj pogoste (dokumente, slike in arhivske datoteke).

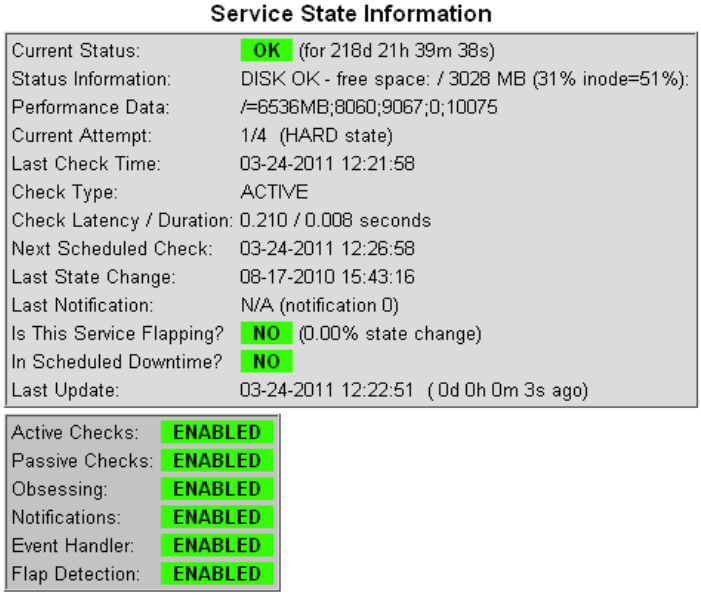
Nastavitve programa so shranjene v datoteki /etc/clamav.conf. ClamAV lahko ročno poženemo z ukazom clamscan ali pa s pomočjo OSS vmesnika. Za avtomatsko pregledovanje lahko ukaz vpišemo tudi v crontab datoteko. Delovanje programa smo omogočili v zavihku »security«, kjer smo določili čas avtomatskega pregledovanja. S to nastavitvijo se med opravila prenese ukaz clamscan, ki pregleda in odstrani viruse na /home particiji. Slika 69 prikazuje aktiviranje protivirusnega programa, ki bo s pregledom pričel ob 2. uri zjutraj.

Slika 69: Aktiviranje protivirusnega programa

Nadzor in vzdrževanje sistema

Tipična praksa Linux administratorjev je ta, da po postavitvi sistema dobesedno pozabijo nanj. Linux je namreč znan kot izredno zanesljiv, zato se zdi, da dodatno vzdrževanje ni potrebno. Kljub vsemu pa moramo imeti sistem pod kontrolo in vsake toliko časa preveriti, kaj se s sistemom dogaja. Preveriti moramo stvari, kot so npr.: stanje storitev, zasedenost kapacitet, log datoteke, morebitne posodobitve in ne nazadnje tudi stanje strojne opreme, ki sistem poganja.

OSS ima nameščeno aplikacijo Nagios, ki nam omogoča spremljanje tekočih sistemskih procesov, pregledovanje stanja sistema, poleg tega pa nas obvešča o morebitnih težavah s procesi ter omogoča izdelavo poročil o procesih za določeno časovno obdobje. Slika 70 prikuje status particije »root« s programom Nagios.



Slika 70: Pregled root particije s programom Nagios

Spletni vmesnik OSS nam omogoča tudi spremljanje stanja storitev. Osnovne storitve so že vpisane, mi pa lahko ostale sami dodamo ter njihovo stanje poljubno spreminjamo.

Med vzdrževanje sistema spadajo tudi njegove posodobitve. Sistem lahko posodabljamo neposredno s spletnega vmesnika ali pa s pomočjo nadzornega središča YaST (angl. YaST Control Center). Yast je dosegljiv v grafičnem načinu, lahko pa ga poženemo tudi iz ukazne vrstice z ukazom yast.

Kljub številnim možnostim, ki nam jih vmesnik na OSS ponuja, bomo morali kdaj pa kdaj poseči po kakšnem ukazu in ukazni vrstici. Med slednje zagotovo sodi pregledovanje log datotek. Večina sistemskih dogodkov se namreč beleži in shranjuje v te datoteke. Log datoteke se zapisujejo v imenik /var/log. Datoteke so shranjene v besedilni obliki in jih lahko pregledujemo z urejevalniki ali ukazi, kot so recimo: tail, less in more.

Med pomembnejšimi log datotekami, ki se nahajajo v /var/log imeniku in jih moramo spremljati na našem sistemu, so naslednje:

- boot.msg - vanj se shranjujejo dogodki procesov, ki se izvedejo ob zagonu sistema in tudi morebitne težave s strojno opremo,
- failog - v datoteko se zapisujejo vse neuspele prijave v sistem;
- lastlog - datoteka, ki omogoča pregled zadnjih prijav v sistem – datoteka ni v besedilni obliki, ampak je pogled možen z ukazom lastlog;
- messages - ta datoteka omogoča celoten pogled nad dogajanjem, vanjo se namreč zapisujejo napake, opozorila, stanje in seveda dogodki ostalih storitev na sistemu;
- warning - v to datoteko se zapisujejo opozorila, npr. požarne pregrade;
- samba/log.nmbd – logi, povezani z NetBIOS strežnikom, ki je potreben Windows odjemalcem;
- samba/log.smbd - v tej datoteki so zapisani dogodki, povezani z datotečnim strežnikom in domenskim kontrolerjem;
- squid/access.log - v to datoteko se shranjujejo dogodki, povezani z uporabo namestniškega strežnika. V datoteki lahko točno vidimo, kateri uporabnik je iz katerega IP naslova obiskal določeno spletno stran;
- squid/store.log - v to datoteko se zapisujejo že obiskane spletne strani, ki hkrati omogočajo hitrejše brskanje;
- squidGuard/squidGuard.log - v to datoteko se zapisujejo dogodki, povezani s programom squidGuard, ki ga uporabljamo za filtriranje spletnih strani. V tem imeniku se nahajajo tudi log datoteke filtriranih kategorij spletnih strani.

Naslednje, kar moramo paziti pri log datotekah, je njihova velikost. Velikost postaja vedno večja, zato moramo kdaj pa kdaj te datoteke tudi počistiti. Linux ima vgrajen program (logrotate), ki omogoča shranjevanje in arhiviranje log

datotek. Običajno se ta postopek izvaja povsem samodejno, ker je vpisan med cron opravila.

Na našem sistemu se shranjevanje in arhiviranje vseh najpomembnejših log datotek izvaja dnevno.

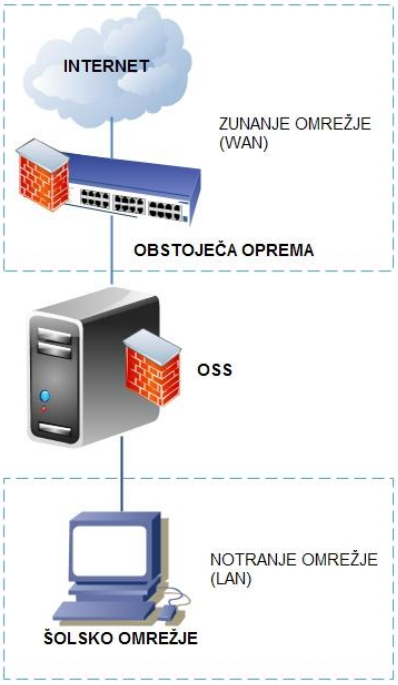
5.4.2 Zagotavljanje omrežne varnosti

Komunikacijskim napravam smo dodelili močna gesla, za dostop do njih pa omogočili le varne komunikacijske kanale. Arnes pa je s filtri na usmerjevalniku omogočil dostop do njih le iz točno določenih IP naslovov.

Lokalno omrežje smo dodatno zaščitili še z mehanizmi, ki jih ponuja OSS. OSS omogoča različne načine postavitev v omrežje, s tem pa tudi različno stopnjo omrežne varnosti. Izbrali smo postavitev, ki zagotavlja najvišjo stopnjo omrežne varnosti, prikazana pa je na sliki 71.

Na obstoječi usmerjevalnik, ki še vedno služi kot požarna pregrada, smo povezali zunanji del omrežja OSS. Šolsko pedagoško omrežje smo povezali na lokalni del omrežja OSS. OSS nam s tako postavitvijo omrežje razdeli na notranji in zunanji del ter obenem služi tudi kot požarna pregrada. Delovne postaje nimajo več neposrednega dostopa do interneta, ampak le preko OSS posrednika. Politiko dostopa do interneta in spletnih strani lahko upravljamo na sistemu samem.

S takšno organizacijo smo bistveno izboljšali omrežno varnost pedagoškega dela omrežja. Promet poteka preko dveh požarnih pregrad, ki zagotavljata varnost na različnih omrežnih nivojih.



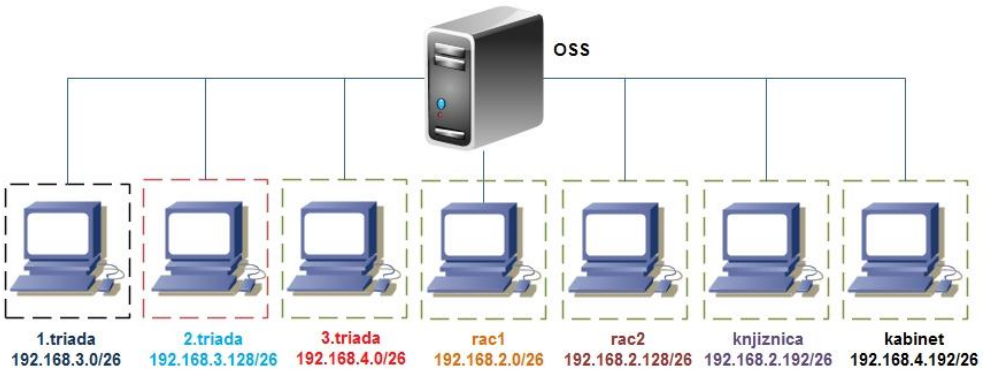
Slika 71: Postavitev OSS v omrežje

Segmentacija in upravljanje pedagoškega dela omrežja

OSS omogoča nadaljnjo segmentacijo pedagoškega dela omrežja. Odločili smo se, da pedagoško omrežje razdelimo glede na prostore uporabe. Naredili smo omrežje za:

- 1. triado
- 2. triado
- 3. triado
- rac1 (računalniška učilnica 1)
- rac2 (računalniška učilnica 2)
- knjižnico
- kabinet

Na sliki 72 je prikazana segmentacija pedagoškega dela omrežja.



Slika 72: Segmentacija pedagoškega dela omrežja

Segmentacija omogoča spreminjanje varnostne politike za vsako omrežno skupino posebej, kot to prikazuje slika 73. Omogočimo ali onemogočimo lahko:

- dostop do interneta,
- namestniški strežnik,
- dostop do domene in s tem prijavo v računalnik,
- dostop do elektronske pošte, če OSS uporabljamo tudi kot poštni strežnik.

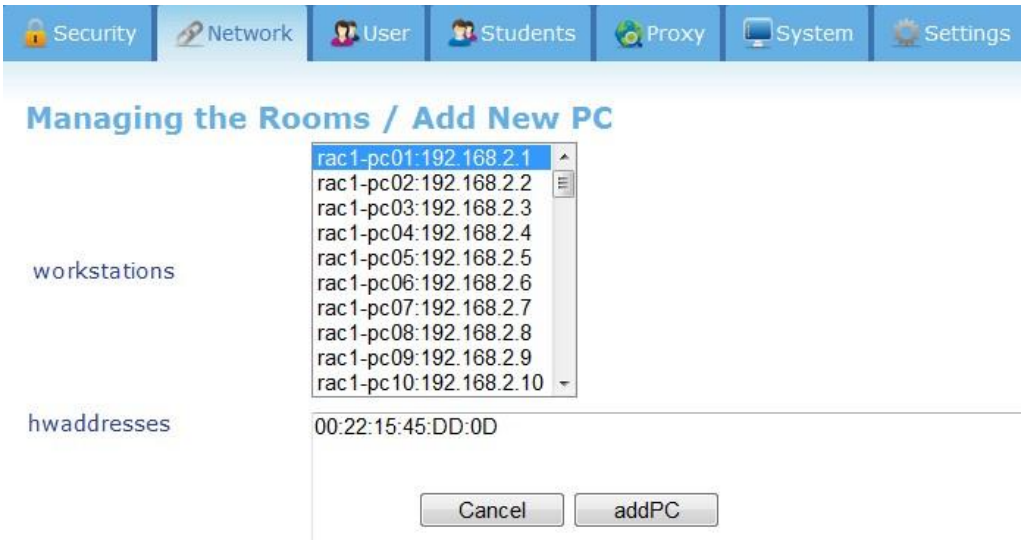
Poleg tega pa lahko omogočimo samodejno spreminjanje statusa storitev v določenih časovnih intervalih. S posamezno omrežno skupino lahko upravlja administrator sistema ali pa kateri izmed uporabnikov, če mu v sistemu dodelimo ustrezne pravice.

Slika 73: Spreminjanje varnostne politike po posameznih omrežnih skupinah

V sistemu smo omogočili tudi DHCP strežnik, ki omogoča samodejno dodeljevanje omrežnih nastavitev delovnim postajam v omrežju. Omenjena funkcionalnost ima tudi nekatere slabosti, ki lahko ogrozijo informacijsko varnost. Ena izmed njih je ta, da lahko nekdo v omrežje na skrivaj doda računalnik. Da bi se izognili tej nevarnosti, moramo v OSS najprej vpisati MAC naslove delovnih postaj, ki se skupaj z omrežnim imenom delovne postaje (angl. NetBIOS name) shranita v LDAP.

Pred prvo prijavo delovnih postaj v domeno se ustreznost teh podatkov preveri. Prvo prijavo delovne postaje v domeno pa lahko nato izvede le administrator OSS.

Način dodajanja delovnih postaj v omrežje prikazuje slika 74.



Slika 74: Dodajanje delovnih postaj v omrežje

Filtriranje spletnih strani z uporabo namestniškega strežnika

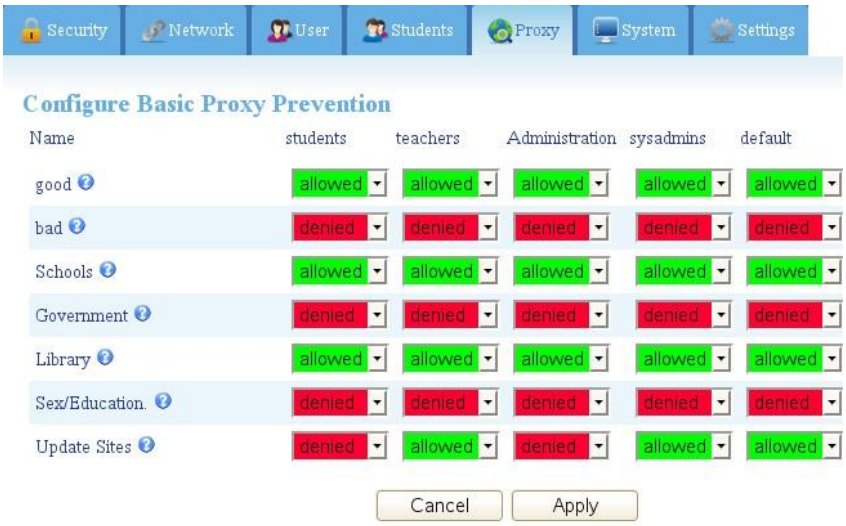
Naslednja velika varnostna pridobitev za naš sistem je namestniški strežnik, ki ima dodano zmožnost filtriranja spletnih strani. Namestniški strežnik je prvotno namenjen hitrejšemu brskanju po omrežju, saj lokalno hrani vsebino že obiskanih spletnih strani, omogoča tudi varnejše brskanje, saj lahko ves promet preusmerimo vanj. Brskanje je bolj transparentno, v dnevniških datotekah se namreč zbere ogromno podatkov o spletnih navadah uporabnikov. Če namestniški strežnik uporabimo še v navezi s kakšnim programom, nam lahko služi tudi za fitriranje spletnih strani.

Na OSS je nameščen namestniški strežnik Squid, ki je tudi najpogosteje uporabljen namestniški strežnik na Linux sistemih. Squid sam po sebi ni zmožen izvajati filtriranja, zato to nalogo opravlja SquidGuard. SquidGuard nam omogoča časovno razdelitev prometa, omejevanje posameznih uporabnikov, preusmerjanje prometa na alternativne lokacije in uporabo črnih seznamov. Prav slednji so zaslužni za filtriranje, tako URL-naslovov kot tudi njihove vsebine. Squid in SquidGuard lahko upravljamo preko ukazne vrstice, podobno kot tudi vse ostale storitve, vendar nam tudi spletni vmesnik omogoča praktično vse potrebno. Ker lahko namestniški strežnik nastavljamo ločeno po omrežnih skupinah, smo se odločili za naslednje nastavitve:

- računalniki, ki jih pretežno uporabljajo učenci (računalniška učilnica in knjižnica), bodo do interneta dostopali izključno preko namestniškega strežnika;
- računalnikom v učilnicah (1., 2. in 3. triada), ki jih uporabljajo učitelji, politiko dostopa določajo sami;
- računalniki v kabinetih imajo do interneta neposreden dostop.

Nato smo nastavili filtriranje spletnih strani. OSS ima naslove spletnih strani razporejene v različne kategorije. Kategorije lahko nato nastavljamo za vsako uporabniško skupino posebej, kot to prikazuje slika 75. Poleg kategorij pa sistem vsebuje tudi obsežno črno listo, v kateri so prepovedani naslovi spletnih strani. Na

enostaven način lahko tudi sami oblikujemo listo prepovedanih in dovoljenih strani.



Slika 75: Filtriranje spletnih strani

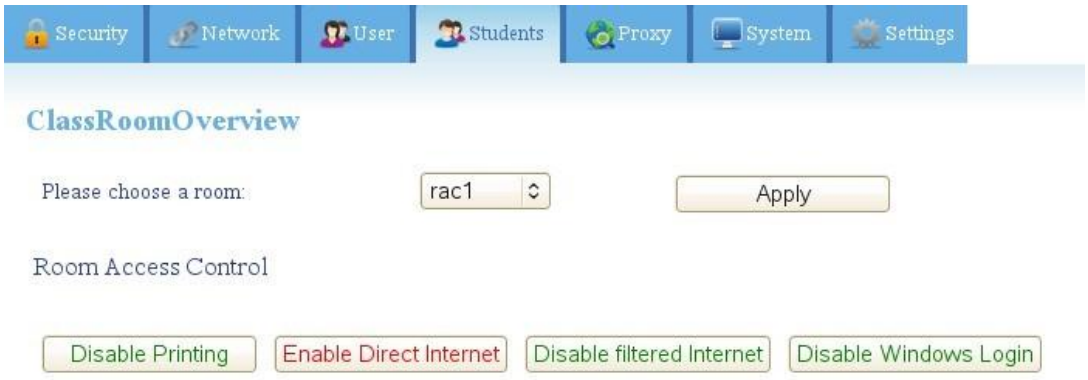
Na šoli smo določili naslednjo politiko filtriranja spletnih naslovov: uporabniška skupina z učenci ima omogočene samo kategorije šola, knjižnica, posodobitve in kategorijo spletni iskalniki. Kot že sama imena kategorij povedo, gre za spletne strani, povezane s šolo, posodobitvami sistema in seveda spletne iskalnike. Čez čas smo ugotovili, da nekatere onemogočene strani potrebujemo, zato smo jih dodali na seznam dovoljenih. Primer vnosa dovoljene spletne strani prikazuje slika 76.

Slika 76: Vnos dovoljene spletne strani

Opazili smo, da je kljub veliki bazi prepovedanih naslovov še vedno dostopnih veliko neprimernih strani, zato smo jih ročno vnesli med prepovedane. Primer vnosa nedovoljene spletne strani prikazuje slika 77.

Slika 77: Vnos prepovedane spletne strani

Za učitelje je nastavitev filtriranja spletnih strani podobna, s to razliko, da lahko oni za svojo učilnico oz. omrežno skupino to spreminjajo tudi sami. Slika 78 prikazuje različne možnosti spreminjanja pravic znotraj učilnice, med katerimi je tudi spletno filtriranje.



Slika 78: Spletno filtriranje po učilnicah oz. omrežnih skupinah

5.4.3 Zagotavljanje podatkovne varnosti

Zagotavljanje podatkovne varnosti nam omogoča strežnik Samba. Samba deluje kot podatkovni strežnik in omogoča Windows odjemalcem shranjevanje podatkov na Linux sistem.

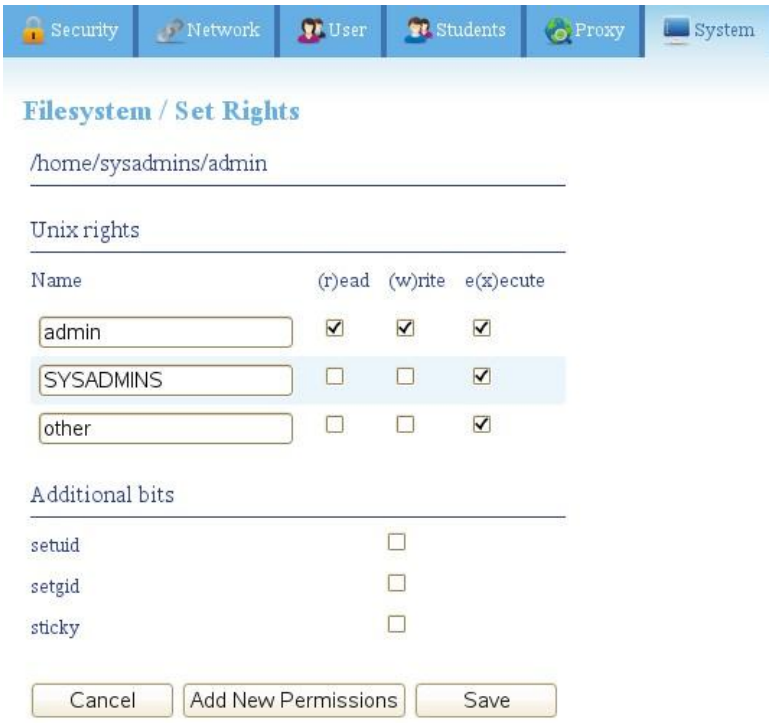
Ob prijavi v domeno se uporabniška mapa preslika v omrežni pogon, na katerega uporabnik shranjuje svoje podatke. Na strežniku so ti podatki shranjeni na enotni particiji »/home«, ki je tipična značilnost Linux sistemov.

Dostop do uporabniške mape ima le uporabnik sam ter seveda najvišji uporabnik na sistemu Linux, to je uporabnik »root«.

Seveda pa lahko dovoljenja na mapah in datotekah poljubno spreminjamo. To lahko storimo iz ukazne vrstice, za tiste manj vešče pa je več kot dobrodošla uporaba OSS vmesnika.

Za spremembo dovoljenja najprej izberemo mapo, nato vnesemo uporabnika in uporabniško skupino in nato potrdimo ustrezne pravice. Spremenimo lahko osnovne varnostne pravice, kot je branje, pisanje in izvajanje (rwx), lahko pa vključimo tudi nastavitvene bite »setuid«, »setgid« ali »stickybit«. Tako lahko npr. vsem uporabnikom dodelimo nek imenik ter s »stickybitom« onemogočimo brisanje datotek v njem.

Postopek spreminjana dovoljenj je prikazan na sliki 79.



Slika 79: Spreminjanje dovoljenj na izbranem imeniku

Za varnost baze podatkov WinKnj smo poskrbeli na naslednji način:
Program WinKnj uporablja relacijsko podatkovno bazo Firebird, ki jo lahko arhiviramo iz ukazne vrstice s pomočjo ukaza gbak.exe. Zato smo napisali enostavno skripto, ki dnevno arhivira in shranjuje bazo podatkov v mapo na OSS, ki je nato vključena v varnostno kopiranje in arhiviranje podatkov. Skripta se izvaja s pomočjo Urejevalnika opravil, ki je del operacijskega sistema Windows.

Varnostno kopiranje in arhiviranje podatkov

Podatki, shranjeni na enotni lokaciji, nam sedaj omogočajo izdelavo varnostnih kopij. Varnostne kopije v Linux sistemih običajno izdelujemo kar s pomočjo

ukazov, ki se izvajajo ob vnaprej določenih časovnih terminih. Podobno je za varnostno kopiranje poskrbljeno tudi v OSS, ki ga lahko omogočimo kar neposredno iz OSS vmesnika.

Odločili smo se, da bomo varnostne kopije shranjevali na zunanji disk. Zunanji disk smo dodelili v privzet imenik »/mnt/backup« z ukazom »mount«. Nato smo izbrali, katere podatke bomo vključili v izdelavo varnostnih kopij. Izbrali smo najpomembnejše, in sicer: uporabniške podatke na particiji »/home« in LDAP imenik. Časovni interval varnostnega kopiranja smo nastavili enkrat dnevno. Program, ki omogoča časovno nastavljanje opravil, se imenuje cron. Opravilo lahko vpišemo v »crontab« datoteko ali pa skripto enostavno dodamo v imenik »/etc/cron.daily«. OSS ima skripte za izdelavo varnostnih kopij že shranjene v omenjenem imeniku, zato dodatne nastavitve niso bile potrebne.

Varnostne kopije podatkov zapisujemo skupaj s podatki iz administrativnega dela tudi na tračne medije. Uporabljamo metodo dnevnega popolnega kopiranja podatkov, kjer za vsak dan v tednu uporabimo svoj medij. Metodo omenjenega varnostnega kopiranja bomo podrobneje opisali v naslednjih poglavjih.

Arhiviranje podatkov izvajamo tedensko skupaj s podatki iz administrativnega dela. Mesečno pa vse podatke shranimo na DVD medij ter ga ustrezno označenega odložimo na varno mesto.

Nastavitev parametrov varnostnega kopiranja je prikazan na sliki 80.

Slika 80: Nastavitev varnostnega kopiranja v OSS

5.4.4 Dodatne varnostne nastavitve

Za dodatno varnost našega sistema smo opravili še nekaj varnostnih nastavitev.

Zagonski nalagalnik GRUB smo zaščitili z geslom. S tem smo preprečili nepooblaščeno zaganjanje sistema.

Oddaljeno upravljanje sistema je mogoče le preko varne lupine SSH, ki privzeto deluje na vratih 22. Ta vrata so pogosto tarča napadalcev, zato smo privzeto vrednost vrat spremenili. Poleg tega smo najvišjemu uporabniku root onemogočili varno prijavo. Namesto tega se v sistem prijavljamo z nižjimi pravicami, po prijavi pa uporabimo root pravice, ko jih seveda potrebujemo.

Za upravljanje požarne pregrade imamo na voljo orodje Suse firewall 2, ki deluje v grafičnem načinu in je dosegljivo iz nadzornega središča YaST. Na požarni pregradi smo omogočili samo storitve, ki jih potrebujemo.

5.5 Zagotavljanje informacijske varnosti za administrativno in tehnično osebje

Največ pozornosti pri zagotavljanju informacijske varnosti smo namenili pedagoškim delavcem in učencem. Ti dve uporabniški skupini namreč sestavlja večina šolskih uporabnikov, pa tudi z vidika varnosti sta najbolj problematični. Seveda pa so na šoli še ostali uporabniki, ki jim moramo prav tako zagotoviti informacijsko varnost.

Predhodno smo omenili, da administrativno osebje lokalno največ uporablja poslovno informacijski sistem SAOP in pisarniške programe, kot sta Microsoft Word ter Excel. Izmed internetnih storitev pa uporabljajo predvsem elektronsko pošto, portal MSS in ujp.net ter svetovni splet.

Dokaj visoke sistemske zahteve programa SAOP so bile povod za nakup strežnika. Odločili smo se, da kot osnovo namestimo operacijski sistem ESXi, ki omogoča hkratno uporabo več virtualnih operacijskih sistemov na enem samem fizičnem strežniku. Zaradi zahteve po uporabi operacijskega sistema Windows smo se odločili za operacijski sistem Windows Server 2003.

5.5.1 Zagotavljanje sistemske varnosti

V strežnik smo vgradili dva trda diska ter postavili RAID 1 podatkovno polje.

Windows Server 2003 smo namestili kot virtualni operacijski sistem v ESXi okolje. Ob namestitvi sistema smo dodeliti močno geslo administratorju sistema. Privzeto uporabniško ime administrator smo preimenovali, saj napadalci pogosto izvajajo napade ravno na ta uporabniški račun.

Pred nadaljnjo pripravo in uporabo smo poskrbeli za osnovne varnostne nastavitve sistema. Namestili smo najnovejše varnostne posodobitve. Samodejno posodabljanje smo nastavili na točno določeno uro, ko sistem predvidoma ne bo v uporabi. Nato smo omogočili požarno pregrado operacijskega sistema ter izbrali možnost ne dovoli izjem. Namestili smo protivirusni program F-Secure, ki se prav tako samodejno posodablja.

V Windows 2003 strežniškem omrežju predstavljajo domene osnovno prijavno in zaščitno okolje. To pomeni, da se lahko vsi uporabniki, ki imajo veljaven uporabniški račun na domenskem strežniku, prijavijo iz poljubnega računalnika v domeno. Za postavitev domene smo morali najprej postaviti imeniški servis, ki omogoča hranjenje, nadzor, upravljanje ter varovanje objektov, ki se nahajajo v omrežju. Za postavitev domene smo morali omogočiti in nastaviti še DNS strežnik, ki omogoča hierarhično poimenovanje domene.

DNS strežnik je pogosto tarča napadalcev, zato je pomembno, da zagotovimo tako fizično kot logično varnost strežnika. DNS strežnik je najbolj izpostavljen napadom »IP spoofing«, »cache poisoning« in »DoS«, zato smo Arnes zaprosili za varnostne nastavitve na usmerjevalniku in omrežnih stikalih.

Sistemska varnost je močno odvisna od delujočih storitev na sistemu. Več kot imamo delujočih storitev, več možnih groženj obstaja. V Windows Server 2003 lahko storitve nastavljamo preko čarovnika, kjer lahko strežnik konfiguriramo za posamezno storitev. Poleg DNS strežnika smo omogočili še podatkovni strežnik, ki go bomo potrebovali za hranjenje uporabniških podatkov.

DHCP strežnik, ki delovnim postajam samodejno dodeljuje omrežne nastavitve, smo onemogočili, da bi zmanjšali možnost nepooblaščene rabe omrežnih virov ter nadaljnjih groženj. To je sicer povzročilo nekaj več administrativnega dela, saj smo morali omrežne nastavitve na delovne postaje ročno vpisati.

Pred prijavo uporabnikov v domeno smo morali izdelati uporabniške in računalniške račune. Pogoj za prijavo uporabnikov v domeno je skladnost obeh računov. Račune smo izdelali s programom Active Directory Users and Computers. Uporabnike smo dodali v uporabniško skupino »Users«, ki so jim onemogočena višje nivojska opravila. Vključili smo zahtevek za spremembo gesla ob prvi prijavi v domeno. Uporabniki si morajo sami izbrati geslo, ki pa se mora v ujemati s pravili nastavljenimi na strežniku.

Za nastavitev varnostne politike odjemalcev smo uporabili varnostno predlogo. Predloga poskrbi za spremembo varnostnih nastavitev. Med drugim zahteva od odjemalcev NTLMv2 obliko overjanja, ki je bolj varna od recimo NTLM, ki se privzeto uporablja. S predlogo se spremenijo tudi številne varnostne nastavitve za uporabniške račune. Tako si morajo recimo uporabniki določiti 24 novih gesel, preden lahko spet uporabijo prejšnjega, dolžina zahtevanega gesla pa se spremeni na minimalno 8 znakov.

Nadaljnje varnostne nastavitve smo določili s pomočjo Group Policy. To je tehnologija, ki preko aktivnega imenika omogoča centralno administracijo uporabnikovega delovnega okolja, dostop do aplikacij in njihovo namestitev, nadzor nad dogodki in sredstvi v aktivnem imeniku in varnostnimi nastavitvami. Na strežniku lahko do najbolj uporabnih nastavitev Group Policy dostopamo preko dveh administracijskih orodij: Domain Security Policy in Domain Controller Security Policy. Prva določa nastavitve vseh računalnikov v domeni, druga pa samo domenskih strežnikov. Poleg teh imamo na vsakem računalniku možnost določevanja varnostnih nastavitev preko Local Security Policy.

S pomočjo Group Policy smo nekoliko prilagodili naslednje varnostne nastavitve za gesla:

- »Maximum Password Age« določa časovno veljavnost gesla. Določili smo, da morajo uporabniki spremeniti svoje geslo vsake 4 mesece.
- »Enforce password history« določa število gesel, ki si jih računalnik zapomni, preden lahko uporabnik zopet uporabi isto geslo. Vrednost smo nastavili na 5.
- »Minimum Password length« določa minimalno število znakov, ki so potrebni za geslo. Število znakov smo pustili na minimalno 8.
- »Password must meet complexity requirements« zahteva od uporabnika, da geslo vsebuje vsaj tri pravila od naštetih:
  - uporabiti mora velike črke angleške abecede,
  - uporabiti mora male črke angleške abecede,
  - uporabiti mora števila,

- uporabiti mora alfa numerične znake (! @ $%&…).

Omogočili smo zahteve za velike črke, male črke ter števila.

- »Account lockout treshold« določa, po kolikšnem številu napačnih poskusov se bo račun avtomatično zaklenil. Računa, ki je zaklenjen, ne moremo več uporabiti za ponovno prijavo, dokler ga administrator ne odklene. Nastavili smo, da se račun po 5 poskusih avtomatično zaklene.

V domenskem okolju je zelo pomembna časovna sinhronizacija med delovnimi postajami in strežnikom. Časovna sinhronizacija omogoča, da se vsi sistemski dogodki vršijo in shranjujejo ob enakem času. To je zelo pomembno kasneje, ko v primeru kakšnih težav analiziramo pretekle dogodke.

Za časovno sinhronizacijo smo na strežniku najprej omogočili storitev za časovno sinhronizacijo. Ob prijavi delovnih postaj v domeno smo kot časovni strežnik izbrali našega domenskega. Z ukazom »netstat« smo preverili morebitna odprta vrata in povezave. Omogočili smo samo tista vrata, ki jih v sistemu potrebujemo za izvajanje storitev, ostala pa smo blokirali.

Za analiziranje varnostnih nastavitev na sistemu smo na koncu zagnali še Microsoft Baseline Security Analyzer. To je orodje, ki preveri varnostne nastavitve ter predlaga morebitne izboljšave.

Za oddaljeno upravljanje in nadziranje sistema smo nastavili uporabo IPsec (Internet Protocol Security) protokola. IPsec omogoča tako overjanja kot tudi šifriranje podatkov.

5.5.2 Zagotavljanje podatkovne varnosti

Za boljšo fizično varnost podatkov od običajne smo poskrbeli že ob sami namestitvi sistema, kjer smo se odločili za zrcaljenje podatkov z uporabo RAID 1.

Za varno shranjevanje uporabniških podatkov smo na sistemu omogočili podatkovni strežnik. Windows Server 2003 podpira vse tri dobro znane datotečne sisteme (Fat16, Fat32, NTFS), z vidika varnosti pa je najbolj primeren NTFS. Za vsako datoteko lahko določimo, kdo ima do nje dostop ter kakšne narave je ta dostop. Lastnik datoteke ali administrator lahko določita vrsto dostopa. Enako velja tudi za mape. NTFS vsebuje torej varnost na nivoju datotek.

Na strežniku smo vsakemu uporabniku izdelali mapo z najvišjimi pravicami in do katere lahko dostopa le on sam. Mapa se ob prijavi delovne postaje v domeno samodejno preslika v mrežni pogon, ki služi za shranjevanje uporabniških podatkov.

Še ena pomembna lastnost NTFS datotečnega sistem je uporaba diskovnih kvot. Z uporabo kvot lahko preprečimo, da bi uporabniki prekoračili dovoljen prostor na disku. Velikost prostora se določa z lastništvom dokumentov na vsaki particiji posebej. To pomeni, da moramo na vsakem disku in particiji posebej nastaviti omejitev uporabe prostora. Pri omejevanju prostora imamo možnost nastaviti opozorilne omejitve, ki uporabnika opozori, da se približuje omejitvi, ko ne bo mogel več uporabljati diska. Za vse uporabnike, ki so člani skupine »administrators«, omejitve prostora na disku ne veljajo.

Na strežniku smo omogočili uporabo diskovnih kvot ter vsakemu uporabniku dodelili določen del prostora na disku. Sicer ne gre ravno za varnostno funkcijo, vendar pa lahko iz pregleda stanja porabe, predvidimo tudi morebitne pomanjkljivosti in nevarnosti.

V primeru, da pride do prekinitve povezave med delovno postajo in strežnikom, smo omogočili možnost datoteke brez povezave. Na delovni postaji se v tem primeru rezervira prostor, kjer se delajo kopije dokumentov, ki se uporabljajo preko omrežja. V primeru prekinitve omrežne povezave lahko uporabnik dela normalno naprej z dokumenti, ki so se hranili na njegovem lokalnem disku. Ob ponovni vzpostavitvi povezave se izvede sinhronizacija med lokalno shranjenimi dokumenti in tistimi na strežniku.

Varnostno kopiranje in arhiviranje podatkov

Varnostno kopiranje in arhiviranje podatkov izvajamo s programom Backup, ki je del operacijskega sistema Windows Server 2003. Program za arhiviranje podpira pet različnih metod arhiviranja. Pri arhiviranju je pomemben arhivski bit oziroma arhivska zastavica. Zastavica se vključi oziroma postavi glede na izbrano metodo:

- Normal - kopirajo se vsi izbrani dokumenti in mape, zastavica se postavi.
- Copy - kopirajo se vsi izbrani dokumenti in mape, zastavica se ne postavi.
- Incremental - kopirajo se vsi izbrani dokumenti in mape, ki so se spremenili glede na zadnji arhiv, zastavica se postavi.
- Differential - kopirajo se vsi izbrani dokumenti in mape, ki so se spremenili glede na zadnji arhiv, zastavica se ne postavi.
- Daily Copy - kopirajo se vsi izbrani dokumenti in mape, ki so se spremenili tekom dneva, zastavica se ne postavi.

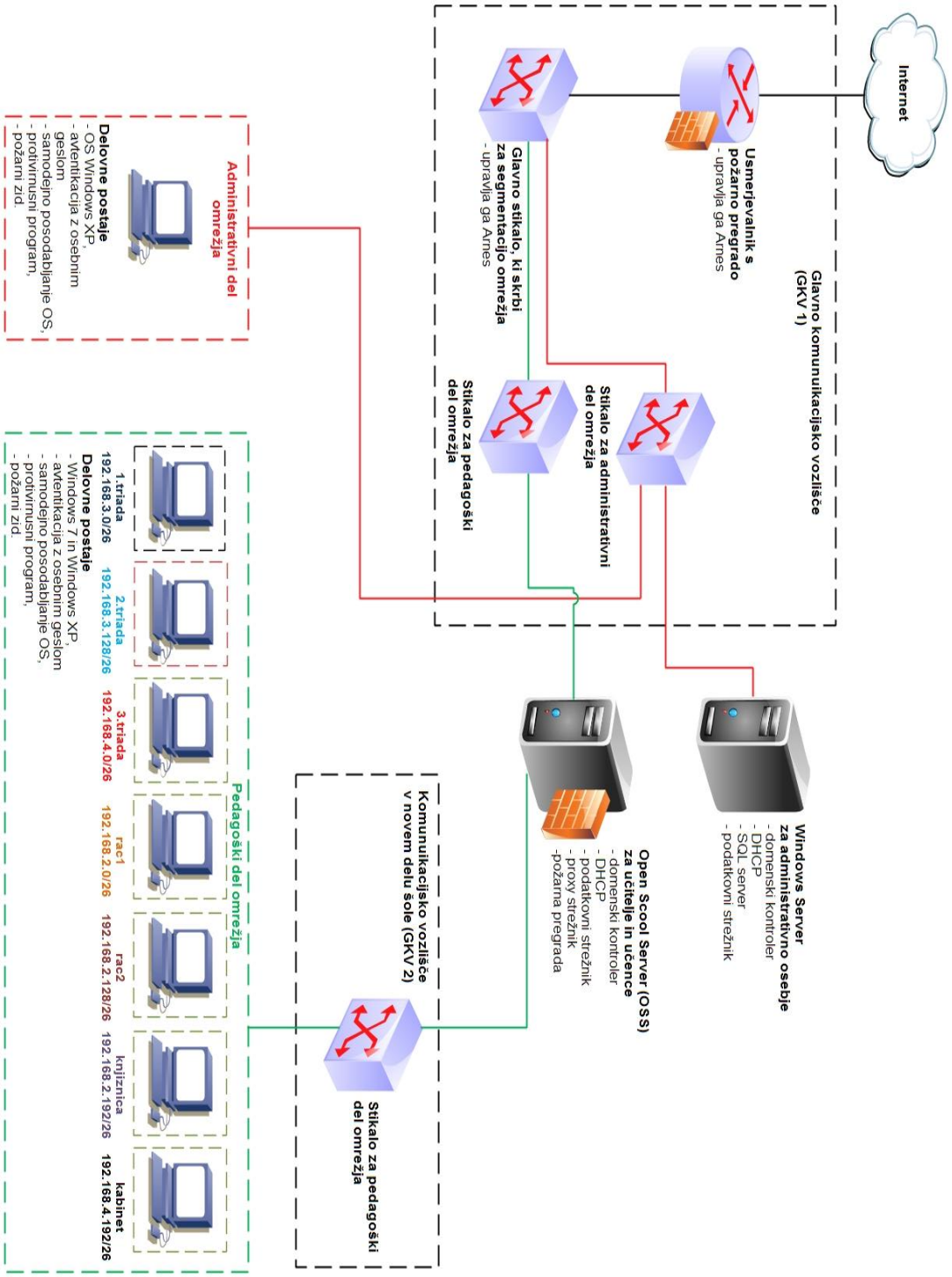
Izberemo lahko posamezno metodo ali pa kombinacijo različnih metod varnostnega kopiranja.

Odločili smo se za tedensko polno metodo (Normal) kopiranja podatkov, kjer se vsak dan v tednu izdela polna varnostna kopija podatkov. Omenjena metoda zahteva nekoliko več diskovnega prostora ali pa več podatkovnih nosilcev. Ampak glede na to, da ne razpolagamo z veliko količino podatkov, nam omenjena metoda ne predstavlja večjih težav.

Glede na to, da imamo v strežniku vgrajeno tračno enoto, smo se odločili za uporabo tračnih medijev. Uporabljamo 5 tračnih medijev ter vsak dan v tednu kopiramo podatke na svoj tračni medij. Ta metoda omogoča obnovitev podatkov za teden dni nazaj, kar sicer ni veliko, vendar trenutno zadošča našim zahtevam.

Arhiviranje podatkov izvajamo na koncu vsakega tedna na tračni medij, mesečno pa na DVD medije, ki jih ustrezno označene shranjujemo na varno mesto.

S prenovo šolskega informacijskega sistema smo precej spremenili tudi infrastrukturo omrežja. Infrastruktura omrežja po prenovi je prikazana na sliki 81.



Slika 821: Šolsko infrastruktura po prenovi

5.6 Varnost delovnih postaj

Zelo pomembno vlogo pri zagotavljanju varnosti imajo tudi delovne postaje oz. računalniki. Na varnost delovnih postaj pomembno vpliva uporabljen operacijski sistem in varnostne nastavitve.

Vsem računalnikom smo v BIOS nastavitvah onemogočili zaganjanje sistema iz zunanjih medijev. Dostop do spremembe BIOS nastavitev smo zaščitili z geslom.

Na vse računalnike smo namestili enako programsko opremo z enakimi nastavitvami. Na zmogljivejše računalnike smo namestili operacijski sistem Windows 7, medtem ko smo na ostale namestili Windows XP. Po osnovni namestitvi smo namestili še varnostne posodobitve operacijskega sistema in protivirusni program F-Secure, za katerega imamo tudi licenco za uporabo. Poleg omenjenega smo na sistem namestili še brezplačni orodji za pregledovanje računalnika, Malwarebytes in Hijackthis. V Windows 7 smo omogočili tudi program Windows Defender, medtem ko smo ga za Windows XP prenesli z interneta.

Glede na to, da uporabniki veliko uporabljajo internet, je zelo pomembna tudi varnost spletnega brskalnika. Odločili smo se, da bomo na vseh računalnikih privzeto uporabljali brskalnik Mozilla Firefox, ki je poznan kot zelo varen brskalnik. V brskalniku smo spremenili še nekaj nastavitev, ki nudijo uporabnikom boljšo varnost. Tako smo npr. onemogočili shranjevanje gesla, onemogočili smo tudi shranjevanje spletne zgodovine, omogočili pa smo blokiranje nevarnih strani in spletnih prevar. Za spletne brskalnike je značilno, da se pogosto posodabljajo, zato smo omogočili samodejno nameščanje posodobitev.

Med pomembnimi varnostnimi nastavitvami operacijskega sistema smo naredili še naslednje:

- onemogočili smo administratorski račun v Windows XP, ki je bil privzeto omogočen brez gesla,
- onemogočili smo račun za goste,
- onemogočili smo storitve, kot so: oddaljena prijava v sistem, skupna raba datotek in možnost urejanja ter spreminjanja registra,
- onemogočili smo samodejno zaganjanje programske opreme z izmenljivih nosilcev,
- vključili smo samodejne posodobitve operacijskega sistema,
- omogočili smo požarno pregrado operacijskega sistema,
- onemogočili smo lokalno hranjenje uporabniških gesel,
- vključili smo samodejno odjavljanje iz sistema v primeru neaktivnosti,
- v Windows XP smo omogočili samo NTLMv2 metodo overjanja.

5.7 Zagotavljanje fizične varnosti

Računalnik z nameščenim OSS, strežnik in ostale komunikacijske naprave smo namestili v varovano komunikacijsko omaro. Dostop do omare ima skrbnik IKT in ravnatelj šole. Prostor ni klimatiziran, zato ga v poletnem času ustrezno zračimo.

Na samem strežniku imamo zaklenjeno tudi področje za dostop do tipke za vklop in izklop sistema, fizično pa je onemogočen tudi dostop do DVD pogona, tračne enote in USB priključka.

Strežniku in komunikacijskim napravam smo zagotovili brezprekinitveno napajanje. Naprava za brezprekinitveno napajanje omogoča ob trenutni porabi nekje do pol ure samostojnega delovanja. To nam zadošča za varen izkop strežnika ter preprečuje morebitne izgube podatkov ali druge okvare na strežniku.

Prostor, v katerem se ta oprema nahaja, je v področju, kjer so tudi pisarne, zato je ta del še dodatno varovan z alarmnim sistemom.

Vsi prostori, v katerih se nahajajo delovne postaje, so v primeru odsotnosti uporabnikov zaklenjeni. Prostori, kot sta računalniški učilnici in knjižnica, ki se lahko uporabljajo tudi v času izven pouka, so dostopni samo z dovoljenjem in pod nadzorom učitelja, skrbnika IKT oz. tistega, ki aktivnost takrat izvaja.

Vse delovne postaje v šoli so nameščene nekoliko dvignjeno od tal, kar preprečuje morebitne poškodbe ob poplavi ali izlitju vode.

V prostorih in na hodnikih šole so nameščeni tudi gasilni aparati, ki v primeru požara omogočajo varno gašenje električnih naprav.

5.8 Zagotavljanje organizacijske varnosti

Za zagotavljanje organizacijske varnosti smo v šoli oblikovali odbor za zagotavljanje informacijske varnosti. Odbor sestavlja 6 učiteljev, ravnatelj šole ter skrbnik IKT, ki je tudi vodja odbora. Glavne naloge odbora so:

- ozaveščanje in usposabljanje uporabnikov,
- skrb za dokumentacijo o uporabi informacijskega sistema,
- oblikovanje in dopolnjevanje varnostne politike informacijskega sistema,
- evidentiranje in odprava varnostnih pomanjkljivosti,
- aktivno sodelovanje z zunanjimi izvajalci.

Na začetku smo oblikovali predlog varnostne politike informacijskega sistema (glej PRILOGO 2), ki trenutno zajema:.

- politiko fizičnega varovanja,
- politiko rabe informacijskega sistema,
- politiko rabe internetnih storitev,
- politiko varovanja podatkov,
- politiko storitev zunanjih izvajalcev,
- politiko upravljanja informacijskega sistema,
- politiko vzdrževanja informacijskega sistema,
- politiko varnostnih elementov, povezanih s človeškimi viri.

Pripravili smo tudi pravilnik o uporabi šolskega informacijskega sistema (glej PRILOGO 3), ki trenutno vsebuje:

- pravilnik o uporabi računalnikov,
- pravilnik o uporabi programske opreme,
- pravilnik o ravnanju s podatki,

- pravilnik o ravnanju z izmenljivimi nosilci podatkov,
- pravilnik o uporabi internetnih storitev.

Odbor neprestano skrbi za ozaveščanje uporabnikov. Učence ozaveščamo na več različnih načinov, kot npr.:

- s pomočjo ostalih učiteljev na oddelčnih urah, pa tudi pri pouku,
- preko spletne strani šole,
- preko gradiv in vaj, objavljenih v spletni učilnici,
- s pomočjo izobraževanj, ki jih izvajamo zaposleni na šoli,
- s pomočjo izobraževanj, ki jih izvajajo zunanjih izvajalci,
- preko številnih obvestil, ki so objavljena na vidnih mestih po šoli,
- s pomočjo njihovih staršev.

Učitelje in ostale uporabnike ozaveščamo:

- z rednimi izobraževanji, ki potekajo na šoli,
- preko spletne strani,
- preko spletne učilnice,
- s pomočjo zunanjih izvajalcev.

5.9 Ocena prenove in perspektive nadaljnjega dela

Z uvajanjem informacijske varnosti smo pričeli v začetku šolskega leta 2010, zato lahko že podamo prve odzive.

Uvajanje se je izkazalo za učinkovito že povsem na začetku, saj smo prve odzive opazili že pri in po sami raziskavi, ki smo jo izvedli v šoli. Zdi se nam, da so začeli uporabniki drugače razmišljati o informacijski varnosti. Opazili smo namreč nekoliko večjo previdnost pri uporabi internetnih storitev ter pri delu s podatki.

Največji vpliv na delo uporabnikov je imelo organiziranje ločenih uporabniških računov. Največjo težavo so učencem povzročala uporabniška gesla, ki so bila po njihovi oceni preveč »kompliciranа«. Naslednji problem je bila slaba skrb za uporabniške izkaznice, katere smo učencem izdelali za prijavo v računalnik. Veliko učencev je izkaznice pozabljalo v računalniški učilnici ali doma. Teh problemov sedaj praktično ni več, saj so si učenci svoje uporabniško ime in geslo zapomnili. Trenutna ocena takšnega organiziranja uporabniških računov je zelo pozitivna. Menimo, da so uporabniki, predvsem pa učenci, s tem dobili občutek zasebnosti, vrednosti in pomembnosti. Zavedati so se začeli dejstva, da lahko »vidimo«, kdo je računalnik uporabljal, zato so jih začeli tudi bolj preudarno uporabljati.

Zelo se je izboljšala tudi podatkovna varnost. Ob predpostavki, da uporabniki uporabljajo računalnike v skladu s pravili in priporočili, je za podatke zagotovljena primerna varnost in zasebnost.

Z uporabo filtriranja spletnih strani se je zelo izboljšala omrežna varnost, posledično pa tudi celotna varnost šolskega informacijskega sistema. Pred tem so lahko učenci obiskovali spletne strani brez omejitev. Kljub prisotnosti učiteljev je bilo nemogoče nadzirati te storitve. Z uporabo filtriranja spletnih strani smo dostop do veliko spletnih strani onemogočili. Seveda ni mogoče filtrirati vseh

spletnih strani, niti ni to naš namen, saj se zavedamo, da bi učenci hitro poiskali kakšno drugo pot za dostop do interneta.

Odločitev za uporabo šolskega informacijskega sistema - OSS je bila pravilna, OSS pa lahko ocenimo z odlično oceno. Sistem je enostaven za namestitev in upravljanje, zato ga lahko uporabljajo tudi tisti, ki niso strokovnjaki za Linux. Sistem deluje varno in zanesljivo od dneva njegove namestitve pa vse do danes. Edina slabost, če lahko temu tako rečemo, je cena uporabe sistema. OSS temelji na operacijskem sistemu Suse Linux Enterprise, katerega licenca je plačljiva. Cena za šole znaša 400 EUR. V ceno je vključena enoletna posodobitev in podpora preko elektronske pošte. Lahko pa podoben model naredimo tudi z minimalnimi stroški, če uporabimo katerega izmed nekomercialnih operacijskih sistemov Linux (npr. Open Suse ali CentOS).

Podobno oceno lahko podamo tudi za informacijski sistem, ki ga uporablja administrativno in tehnično osebje. Sama sprememba ni imela bistvenega vpliva na delo uporabnikov, zato tam težav nismo zaznali. Zelo smo izboljšali varnost podatkov, sistemsko varnost ter fizično varnost, kar je bil tudi naš namen.

Zavedamo se, da samo tehnični ukrepi niso in ne bodo dovolj za izboljšanje informacijske varnosti. V ta namen smo ustanovili odbor za zagotavljanje informacijske varnosti, ki bo skrbel za organizacijsko varnost. Čeprav je v šoli ozračje pogosto »naelektreno«, pa želimo zagotavljati informacijsko varnost v kar se da pozitivnem duhu.

Informacijsko varnost bomo izboljševali tudi v prihodnje. Najprej bi radi OSS preselili na ustrezen fizičen strežnik, ki bo zagotavljal še zanesljivejše in varnejše pogoje delovanja. Dokončali in uradno sprejeli bomo varnostno politiko ter jo vključiti v sistemizacijo šole.

S procesom zagotavljanja informacijske varnosti bomo nadaljevali na podružničnih osnovnih šolah. Najverjetneje bomo uporabili podoben pristop in rešitve kot sedaj.

Varnost podatkov še vedno ogroža dejstvo, da so ti shranjeni le na lokaciji šole. V nadaljevanju razmišljamo o shranjevanju podatkov na oddaljeno lokacijo. Ena izmed možnosti je ta, da izberemo zunanjega ponudnika, ki bo skrbel za to. Razmišljamo pa tudi o tem, da bi podatke shranjevali na katero izmed podružničnih šol, ko bomo tam vzpostavili primerno stanje.

Rešitev z uporabo OSS se nam zdi zelo primerna, zato smo se odločili, da jo v prihodnosti predstavimo tudi ostalim šolam po Sloveniji. Nadvse dobrodošla bi bila podpora ministrstva, saj bi s sofinanciranjem takšne ali podobne rešitve znatno pripomogli k izboljšanju informacijske varnosti v osnovnih šolah.

6 ZAKLJUČEK

Z vse večjim razvojem IKT dobiva področje zagotavljanja informacijske varnosti tudi v šolstvu vse večji pomen. Organizacije, kot so osnovne šole, se zdijo na prvi pogled zelo majhne in s tega stališča enostavne, vendar je zagotavljanje informacijske varnosti vse prej kot lahko opravilo. Posledic neustrezne informacijske varnosti se običajno začnemo zavedati šele takrat, ko je škoda že narejena.

V nalogi smo opisali stanje na področju zagotavljanja informacijske varnosti v slovenskem šolstvu in predstavili državne institucije, ki na tem področju delujejo.

Stanje na področju informacijske varnosti v slovenskih osnovnih šolah smo preverili s pomočjo ankete, v kateri je sodelovalo 95 osnovnih šol iz vse Slovenije. Rezultati ankete, ki smo jo izvedli med skrbniki IKT v slovenskih osnovnih šolah, kažejo, da se ti kljub slabi podpori s strani države in neustrezni sistemizaciji delovnega mesta, zelo trudijo skrbeti za zadovoljivo stanje na področju informacijske varnosti. Anketa med šolskimi uporabniki (učitelji in učenci) pa je pokazala, da je največji problem nezadostno zavedanje nevarnosti, ki informacijskemu sistemu pretijo.

Na podlagi študija dostopnih informacij smo ugotovili, da drugod po svetu šole zagotavljajo informacijsko varnost na bolj racionalen in učinkovit način. Veliko rešitev namreč temelji na odprti kodi, pa tudi računalniška oprema v šolah je manj zmogljiva kot pri nas. Za informacijsko varnost pa ponekod skrbijo tudi zunanji izvajalci, ki v večini primerov rešitev postavijo in upravljajo, šolski uporabniki pa jo le uporabljajo.

Na podlagi novo pridobljenega znanja in dobrih praks, ki se uporabljajo v tujini, smo oblikovali splošne smernice za zagotavljanje informacijske varnosti v osnovni šoli. V skladu s temi smernicami smo prenovili informacijski sistem v Osnovni šoli Neznanih talcev Dravograd.

Izboljšali smo informacijsko varnost na več področjih in za vse šolske uporabnike (skrbnik IKT, učitelji učenci).

Za uporabnike smo informacijsko varnost izboljšali z organizacijskimi in tehničnimi spremembami. Vzpostavili smo odbor za zagotavljanje informacijske varnosti, ki uporabnike neprestano ozavešča in izobražuje. Odbor za informacijsko varnost je oblikoval tudi predlog varnostne politike informacijskega sistema in pravilnik o uporabi šolskega informacijskega sistema, ki ga morajo vsi uporabniki informacijskega sistema v šoli upoštevati. Organizacijsko varnost zagotavljamo z lastnimi sredstvi, saj smo ugotovili, da imamo dovolj znanja na tem področju.

Informacijsko varnost smo bistveno izboljšali z nekaterimi tehničnimi novostmi in izboljšavami. Med novostmi izstopa uporaba Open School Server-ja. Z uporabo Open School Server-ja oz. OSS, kot smo ga poimenovali smo izboljšali sistemsko varnost, varnost podatkov in omrežno varnost. Za izboljšanje sistemske varnosti smo za vse uporabnike izdelali ločene uporabniške račune z omejenimi uporabniškimi pravicami. Vsem uporabnikom smo omogočili zasebnost in varnost pri shranjevanju podatkov. Tudi omrežno smo izboljšali s pomočjo OSS. Naredili smo dodatno segmentacijo pedagoškega dela omrežja in omogočili filtriranje

spletnih strani. Pri zagotavljanju omrežne varnosti pa nam je v veliko pomoč tudi Arnes, ki nam je s svojimi strokovnimi nasveti in nastavitvami na omrežnih naprav vedno pripravljen pomagati.

Tudi z vidika skrbnika IKT smo dosegli veliko varnostnih izboljšav. Vzpostavili smo sistem centralnega hranjenja podatkov, ki omogoča enostavno izdelavo varnostnih kopij ter arhiviranje podatkov. Ločeno vodenje uporabniških računov omogoča skrbniku pregled nad uporabniškimi aktivnostmi. Z uporabo namestniškega strežnika pa lahko uporabnik nadzira in omejuje dogajanje v omrežju.

Čeprav smo večji del naloge namenili informacijski varnosti na področju kjer nastopajo pedagoški delavci in učenci, pa nismo pozabili ostalih zaposlenih (administrativno in tehnično osebje). S podobnimi posegi na tehničnem področju smo tudi ostalim zaposlenim zagotovili zasebnost in varnost podatkov. Vzpostavili smo sistem, ki omogoča centralno hranjenje ter s tem varnostno kopiranje in arhiviranje podatkov. Prav tako so ti zaposleni deležni enake pozornosti na področju organizacijske varnosti.

Poleg omenjenega smo izboljšali še fizično varnost vseh dobrin informacijskega sistema. Vse delovne postaje smo namestili na primerna mesta, dostop do ključnih naprav pa smo še dodatno zavarovali.

Zagotovo lahko na področju zagotavljanja informacijske varnosti še marsikaj izboljšamo in postorimo, ampak menimo, da smo s prenovo informacijskega sistema v OŠ Neznanih talcev Dravograd kljub majhnemu finančnemu vložku dosegli bistveno izboljšavo na tem področju. Z gotovostjo lahko trdimo, da bi pristop, ki smo ga uporabili na naši osnovni šoli, lahko uporabile tudi ostale osnovne šole v Sloveniji.

UPORABLJENA LITERATURA IN VIRI

Antič, M. (2005): Real Security Info, str. 22, april 2005.

Arnes (2009): Arnes - pregled aktivnosti 2009, dosegljivo na naslovu: http://www.arnes.si/fileadmin/dokumenti/zavod-arnes/publikacije/pregled-aktivnosti-2009.pdf, obiskano dne: 14. 12. 2010.

Arnes (2010a): Predstavitev zavoda Arnes, dosegljivo na naslovu: http://www.arnes.si/zavod-arnes/predstavitev.html, obiskano dne, 14. 12. 2010.

Arnes (2010b): Program dela in razvoja ter finančni načrt Arnesa za leto 2010, dosegljivo na naslovu: http://www.Arnes.si/fileadmin/dokumenti/zavod-Arnes/plan-2010.pdf, obiskano dne, 14. 12. 2010.

Arnes (2011a): Arnes - pregled aktivnosti v letu 2011, dosegljivo na naslovu: http://www.arnes.si/fileadmin/dokumenti/zavod-arnes/pregled-aktivnosti-2011.pdf, obiskano dne: 1. 3. 2012.

Arnes (2011b): Zloženka Arnes, dosegljivo na naslovu: http://www.arnes.si/fileadmin/dokumenti/zavod-arnes/publikacije/zlozenka-arnes-izobrazevalni-internet-tisk-2011.pdf, obiskano dne, 1. 3. 2012.

B2 (2004): Gradivo administracija Windows Server 2003, gradivo za računalniški tečaj, B2, Ljubljana.

Bierhals, G. (2009): Desktop4education: Bringing new environments to Austrian schools, dosegljivo na naslovu: http://www.osor.eu/studies/desktop4education-bringing-new-environments-to-austrian-schools, obiskano dne, 7. 4. 2011.

Brezavšček, A. (2007): Varnost informacijskega sistema, učno gradivo, Univerza v Mariboru, Fakulteta za organizacijske vede, Kranj.

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

CIO (2010): Are Your IT Folks Snooping Your Protected Data?, dosegljivo na naslovu: http://www.cio.com/article/598796/Are_Your_IT_Folks_Snooping_Your_Protected_Data, obiskano dne, 6. 3. 2011.

Djurdič,V. (2004): Varnost pred vsem, dosegljivo na naslovu: http://www.monitor.si/clanki.php?id=358, obiskano dne, 5. 2. 2010.

Duncan, N. (2000): Firewall Explained , dosegljivo na naslovu: http://www.orbit-computer-solutions.com/Firewall-Explained.php, obiskano dne, 5. 11. 2010.

EMC (2010): Generation Y Highly Susceptible to Threats Due to Risky Behavior Online, dosegljivo na naslovu: http://www.emc.com/about/news/press/2010/20100420-01.htm, obiskano dne: 6. 3. 2011.

Granger, S. (2010): Social Engineering Fundamentals, Part I: Hacker Tactics, dosegljivo na naslovu: http://www.securityfocus.com/infocus/1527, obiskano dne, 12. 6. 2010.

Harej, J. (2008): Priročnik za spoznavanje delovanja operacijskih sistemov, dosegljivo na naslovu: http://colos1.fri.unilj.si/eri/rac_sistemi_omrezja/html/UVOD_V_OS/index.html, obiskano dne, 10. 9. 2010.

Heise online (2006): Passwortdaten von Flirtlife.dekompromittiert, dosegljivo na naslovu: http://www.heise.de/newsticker/meldung/73396, obiskano dne, 15. 8. 2010.

IDC (2012): IDC - Press Release, dosegljivo na naslovu: http://www.idc.com/getdoc.jsp?containerId=prUS23347812, obiskano dne, 21. 5. 2012.

Jančigaj, R. (2007): Varnostno kopiranje podatkov za mala in srednja podjetja, Finance, junij 2007.

Kizza, J. (2009): A Guide to Computer Network Security, University of Tennessee - Chattanooga, ZDA.

Klančnik, J. (2007): Zagotavljanje varnosti v oddelku informacijske tehnologije NLB Koroške banke, Univerza v Mariboru, Fakulteta za organizacijske vede, Kranj.

Kos, A. (2004): Uvajanje sistema varovanja informacij v podjetju Paloma, d. d., diplomsko delo, Univerza v Mariboru, Ekonomsko - poslovna fakulteta, Maribor.

Kranjčič, D. (2004): Programiranje v operacijskem sistemu Linux, Monitor, Februar 2004.

Lampret (2009): On-line backup sistemi, varnostne kopije in arhiviranje, dosegljivo na naslovu: http://www.lampret.net/blog/on-line-backup-sistemi-varnostne-kopije-in-arhiviranje/, obiskano dne, 10. 10. 2010.

Lubej, R. (2006): Real Security Info, str. 8, maj 2006.

Meolic, R. (2009): Vzdrževanje sistemske programske opreme, učno gradivo, Višja strokovna šola Murska Sobota, Murska Sobota.

Merljak, J. (2009): Računalništvo v oblaku, diplomsko delo, Univerza v Ljubljani, Fakulteta za računalništvo in informatiko.

Ministrstvo za izobraževanje, znanost, kulturo in šport (2006): Akcijski načrt nadaljnjega preskoka informatizacije šolstva, dosegljivo na naslovu: http://www.mss.gov.si/fileadmin/mss.gov.si/pageuploads/podrocje/IKT/akcijski_nacrt_informatizacija_solstva_8_2006.pdf, obiskano dne, 14. 12. 2010.

Mitnick, K. (2002): The Art of Deception, John Wiley and Sons.

Mukherjee, B., Heberlein, L., Levitt, K. (1994): Network Intrusion Detection, IEEE Network , 8(3), str. 26-41, maj/jun 1994.

Nasvet za net (2010): Nasvet za net, dosegljivo na naslovu: http://www.nasvetzanet.si, obiskano dne, 14. 2. 2010.

Online Data Backup Solutions: Importance of Data Backup, dosegljivo na naslovu: http://www.onlinedatabackupsolutions.com/importance-of-data-backup.html, obiskano dne, 10. 10. 2010.

Orbanić, A (2006): Operacijski sistemi in omrežja, učno gradivo, Univerza v Ljubljani, Fakulteta za matematiko in fiziko, Ljubljana.

Pihler, M. (2007): Rootkits, NTK konferenca 2007, maj 2007.

Safe-si (2012): O projektu, dosegljivo na naslovu: http://www.safe.si, obiskano dne, 21. 5. 2012.

Samuelle, T.J (2009): Mike Meyers' CompTIA Security+ Certification Passport, Second Edition, McGraw-Hill, ZDA.

Saunders, P. (2009): ICT security in schools - results of Audit 2009, dosegljivo na naslovu: http://www.tamesideschoolssupport.net/index.php?option=com_content&view=article&id=1588:ict-security-in-schools-results-of-audit-2009&catid=13:security&Itemid=39, obiskano dne, 7. 4. 2011.

Simt (2007): Varnostno kopiranje podatkov za mala in srednja podjetja, dosegljivo na naslovu: http://www.simt.si/library_sl/pdf/FI_2007_110_28.pdf, obiskano dne, 10. 10. 2010.

Spletno oko (2012): Splošne informacije, dosegljivo na naslovu http://www.spletno-oko.si, obiskano dne, 21. 5. 2012.

Strosar E., (2006): ARP - Address Resolution Protocol - napadi in obramba, Monitor, oktober 2006.

Strosar. E. (2007): (Ne)varnost v javnih omrežjih WLAN, Monitor, april 2007.

Štrakl, M. (2003): Varnostna politika informacijskega sistema, Štirinajsta delavnica o telekomunikacijah VITEL, Brdo pri Kranju, maj 2003.

Šuc, E. (2002): Linux proti virusom, Guru, Informacijske tehnologije, Ljubljana

Telemach, Varnostno shranjevanje, dosegljivo na naslovu: http://www.telemach.si/sl/poslovni-uporabniki/varnostne-resitve/varnostno-shranjevanje, obiskano dne, 10. 10. 2010.

Varni na internetu (2010): Cilji projekta, dosegljivo na naslovu: http://www.varninainternetu.si, obiskano dne, 14. 12. 2010.

Verdonik I., Bratuša T. (2005): Hekerski vdori in zaščita, Pasadena, Ljubljana.

w3schools (2012): OS Platform Statistics, dosegljivo na naslovu: http://www.w3schools.com/browsers/browsers_os.asp, obiskano dne, 21. 5. 2012.

Wack, J., Tracy,M., Souppaya, M. (2003): Guidline on Network Security Testing, National Institute of Standards and Technology Gaithersburg, ZDA.

Zorko, M. (2007): Stikalno omrežje v industrijskem okolju, diplomsko delo, Univerza v Mariboru, Fakulteta za organizacijske vede, Kranj.

Žagar, G. (2006): Metode in tehnike napadov na informacijsko komunikacijske sisteme, Univerza v Ljubljani, Fakulteta za računalništvo in informatiko.

OSTALA LITERATURA IN VIRI

Arktur – Schulserver (2011): Arktur – Schulserver, dosegljivo na naslovu: http://arktur.shuttle.de/, obiskano dne, 16. 2. 2011.

CBT Nuggets (2011): Video training, dosegljivo na naslovu: http://www.cbtnuggets.com/, obiskano dne, 10. 1. 2011.

Debian Edu – Skolelinux Lenny (2011): Manual, dosegljivo na naslovu: http://maintainer.skolelinux.org/debian-edu-doc/en/debian-edu-lenny-manual.pdf, obiskano dne: 16. 2. 2011.

Douglas Ashbaugh, A. (2009): Security Software Development, CRC Press, ZDA.
Tulloch, M. (2003): Microsoft Encyclopedia of Security, Microsoft Press, Washington.

Gerlič, I. (2005): Uporaba informacijske in komunikacijske tehnologije v slovenskih šolah, Univerza v Mariboru, Pedagoška fakulteta, Maribor.

Pavlinič Krebs, I. (2010): Priporočila informacijske varnostne politike javne uprave, dosegljivo na naslovu: http://www.mpju.gov.si/fileadmin/mpju.gov.si/pageuploads/DIES/IVPJU_01.pdf, obiskano dne, 30.5.2012

Rakuš, J. (2002): Varovanje informacij: Standard ISO 17799 in varovanje gesel, Medicinska fakulteta, Inštitut za biomedicinsko informatiko, Ljubljana.

Ray, J. (2001): Maximum Linux Security, Second Edition, Sams Publishing, Indiana.

Linux – Schulserver (2011): Linux – Schulserver, dosegljivo na naslovu: http://www.linux-schulserver.de/, obiskano dne, 16. 2. 2011.

Novak Vukšinič, N. (2009): Uporaba informacijsko komunikacijske tehnologije v

osnovnih šolah, Diplomsko delo, Univerza v Mariboru, Fakulteta za organizacijske vede, Kranj.

Open School Server (2011): Open School Server, dosegljivo na naslovu: http://www.openschoolserver.net/, obiskano dne, 16. 2. 2011.

Skolelinux (2011): Skolelinux, dosegljivo na naslovu: http://www.slx.no/, obiskano dne, 16. 2. 2011.

Siddiqui, S. (2002): Linux Security, Premier Press, ZDA.

The SANS Institute (2002): Securing Linux Step By Step.

KAZALO SLIK

KAZALO TABEL

PRILOGE

PRILOGA 1: Anketni vprašalniki za skrbnike in uporabnike šolskega informacijskega sistema

ANKETNI VPRAŠALNIK ZA SKRBNIKE ŠOLSKEGA INFORMACIJSKEGA SISTEMA

Informacijska varnost je pereča tema na vseh ravneh, od posameznikov do podjetij. Kljub ukrepom, ki jih izvajamo v praksi, se pogosto pokaže, da še nismo povsem dojeli pravega pomena informacijske varnosti. Število nezgod zaradi neustrezne informacijske varnosti se iz leta v leto povečuje, vzroki pa so različni, kot so različne tudi rešitve, ki jih uporabljamo.

Z anketo želim izvedeti, kakšno je stanje informacijske varnosti na slovenskih osnovnih šolah.

1. Koliko računalnikov imate na šoli?
a) do 50
b) od 50 do 100
c) od 100 do 150
d) več kot 150

2. Kateri operacijski sistem v večini uporabljate na računalnikih?
a) Windows XP
b) Windows Vista
c) Windows 7
d) Linux
e) Drugo, napišite

3. Kdo na vaši šoli skrbi za informacijsko komunikacijsko tehnologijo (IKT)?
a) Računalničar
b) Učitelji
c) Zunanji izvajalec
d) Drugi

4. Katero vrsto zaščite uporabljate na računalnikih?
a) Radix
b) DeepFreeze
c) Protivirusni program
d) Omejene pravice uporabnikov in protivirusni program
e) Požarni zid operacijskega sistema
f) Ne uporabljam posebne zaščite
g) Drugo, napišite

5. Kako imate organizirane uporabniške račune?
a) Vsi uporabniki imajo enotno geslo z omejenimi pravicami
b) Vsaka skupina uporabnikov (učitelj, učenec..) ima svoje geslo
c) Vsak učitelj ima svoje geslo, učenci pa ga ne potrebujejo ali pa imajo enotno geslo
d) Vsak uporabnik ima svoje geslo
e) Za prijavo ne uporabljamo oz. skoraj ne uporabljamo gesel

6. Ali uporabnikom kdaj svetujete o pravilni izbiri gesel (dolžina, zahtevnost...)

a) Da
b) Ne

7. Kje vidite največjo problematiko pri upravljanju z gesli?

a) Pozabljanje gesel
b) Enostavna gesla
c) Zapisovanje gesel na vidna mesta

8. Kdo na vaši šoli skrbi za varnost omrežja?

a) Računalničar
b) ARNES
c) Računalničar in ARNES
d) Drugi

9. Kakšno topologijo omrežja imate?

a) Enotno omrežje, povezano v centralno vozlišče
b) Ločena omrežja (VPN), povezana v centralno vozlišče
c) Topologijo Client - Server z enotnim omrežjem
d) Topologijo Client - Server z ločenimi omrežji
e) Drugačno, napišite

10. Ali v omrežju uporabljate strežnik?

a) Da
b) Ne

11. Kdo vam vzdržuje strežnik?

a) Sami
b) Zunanji izvajalec
c) Nimam strežnika
d) Sami ob zunanji podpori

12. Kateri operacijski sistem teče na strežniku?

a) Windows
b) Linux
c) Nekaj drugega
d) Nimam strežnika

13. Katere storitve vam omogoča strežnik?

a) Domenski strežnik
b) DHCP strežnik
c) Podatkovni strežnik
d) Poštni strežnik
e) Spletni strežnik
f) Namestniški (proxy) strežnik
g) Tiskalniški strežnik
h) Požarna pregrada
i) Nimam strežnika
j) Druge storitve, napišite

14. Kako imate poskrbljeno za shranjevanja podatkov?
a) Podatki se shranjuje klasično na privzeto particijo
b) Podatki se shranjujejo na particijo, ki je ločena od sistemske
c) Podatki se shranjujejo na strežnik
d) Podatki se shranjujejo na nosilec v omrežju
e) Drugače, napišite

15. Kdo na šoli skrbi za varnost podatkov?
a) Računalničar
b) Vsak skrbi za svoje podatke
c) Zunanji izvajalec
d) Drugi

16. Kako izvajate varnostno kopiranje podatkov?
a) Tega ne izvajamo
b) Vsak uporabnik si sam dela varnostne kopije
c) Podatki se dnevno kopirajo na ustrezne nosilce
d) Podatki se tedensko kopirajo na ustrezne nosilce
e) Podatke 1 - 2 x letno kopiram
f) Drugače, napišite

17. Ali izvajate arhiviranje podatkov?
a) Da
b) Ne

18. Na katere nosilce arhivirate podatke?
a) CD, DVD
b) Zunanji mediji (HD, flash...)
c) Tračni nosilci
d) Podatkov ne arhiviram
e) Drugo, napišite

19. Ali kdaj preverjate berljivost medijev?
a) Da
b) Ne

20. Katera internetna storitev po vašem najbolj ogroža informacijsko varnost?
a) Brskanje po internetu
b) Elektronska pošta
c) Spletne klepetalnice

21. Kateri dejavniki in dogodki po vašem najbolj ogrožajo varnost informacijskega sistema?
a) Človeški dejavniki (virusi, vdori...)
b) Naključni dogodki (odpoved opreme..)
c) Izredni dogodki (poplave, požari...)
d) Drugo, napišite

22. Kdo na šoli je tisti, ki povzroča največ preglavic na tem področju?
a) Učitelji
b) Učenci
c) Administrativno osebje
d) Tehnično osebje

e) Ostali uporabniki

23. Kaj so po vašem mnenju najpogostejši vzroki groženj?
a) Slaba zasnova sistema
b) Neznanje in neizkušenost uporabnikov
c) Napake uporabnikov
d) Neznanje in neizkušenost skrbnika
e) Pomanjkanje časa
f) Pomanjkanje sredstev
g) Drugo, napišite

24. Ali se z učenci, učitelji in ostalimi uporabniki kdaj pogovarjate o varni rabi računalnika in spletnih storitev?
a) Da
b) Ne

25. Ali imate izdelano varnostno politiko informacijskega sistema?
a) Da
b) Ne
c) Deloma

26. Ali menite, da na šoli namenjate dovolj pozornosti tej tematiki?
a) Da
b) Ne

27. Ali menite, da imamo računalničarji dovolj podpore na tem področju?
a) Da
b) Ne

28. Z oceno od 1 do 5 ocenite stanje informacijske varnosti na vaši šoli
a) 1
b) 2
c) 3
d) 4
e) 5

ANKETNI VPRAŠALNIK ZA UPORABNIKE (UČITELJE) ŠOLSKEGA INFORMACIJSKEGA SISTEMA

Omenjena anketa je anonimna in je namenjena zgolj za potrebe raziskave. Anketa se nanaša na uporabo računalnika, internetnih storitev in ostalega, kar nam računalnik omogoča. Poudarek ankete je na nevarnostih uporabe informacijsko-komunikacijske tehnologije.

1. **Ali uporabljate računalnik?**
   a) DA b) NE

2. **Kako pogosto ga uporabljate?**
   a) Vsak dan b) Nekajkrat tedensko c) Nekajkrat na mesec
   d) Ga ne uporabljam

3. **Za kaj vse uporabljate računalnik? (obkrožite lahko več odgovorov)**
   a) Za internet
   b) Za razvedrilo
   c) Za delo
   d) Drugo, napišite:
   _____.

4. **Za kaj vse uporabljate Internet? (obkrožite lahko več odgovorov)**
   a) Brskanje po spletu b) Elektronska pošta c) Klepetalnice d) Spletni forumi
   e) Igranje iger f) Drugo,
   napišite:_____.

5. **Ali veste, da ima lahko uporaba računalnika in interneta tudi določene nevarnosti?**
   a) DA, napišite katere:_____. b) NE

6. **Ali ste na vašem računalniku že kdaj imeli virus?**
   a) DA b) NE

7. **Ali poznate razliko med računalniškim virusom, črvom in trojanskim konjem?**
   a) DA b) NE

8. **Ali poznate kakšno spletno stran, kjer si lahko preberete kaj o računalniških virusih?**
   a) DA, zapišite katero:_____. b) NE

9. **Ali lahko geslo zaupate ostalim?**
   a) DA b) NE

10. Kako dolgo geslo uporabljate ? (npr. za prijavo v računalnik, elektronsko pošto,…)

a) 3 – 5 znakov b) 6 – 10 znakov c) več kot 10 znakov

11. Ali menite, da bi bilo na šoli potrebno imeti kakšen tečaj o varni rabi računalnika in Interneta?

a) DA, bilo bi koristno b) NE, tega ne potrebujemo c) NE VEM

12. Ali ste sami že kdaj razmišljali o nevarnostih na Internetu in o varnosti vaših podatkov na računalniku?

a) DA, pogosto b) Redkokdaj c) Še nikoli nisem pomislil(a) na to

ANKETNI VPRAŠALNIK ZA UPORABNIKE (UČENCE) ŠOLSKEGA INFORMACIJSKEGA SISTEMA

Omenjena anketa je anonimna in je namenjena zgolj za potrebe raziskave. Anketa se nanaša na uporabo računalnika, internetnih storitev in ostalega, kar nam računalnik omogoča. Poudarek ankete je na nevarnostih, ki jih uporaba računalniške tehnologije lahko povzroči.

1. **Ali uporabljate računalnik?**
   b) DA b) NE

2. **Kako pogosto ga uporabljate?**
   b) Vsak dan b) Nekajkrat tedensko c) Nekajkrat na mesec
   d) Ga ne uporabljam

3. **Za kaj vse uporabljate računalnik? (obkrožite lahko več odgovorov)**
   e) Za internet
   f) Za pisanje besedil, izdelavo predstavitev
   g) Za igranje iger
   h) Za učenje
   i) Za poslušanje glasbe in gledanje video vsebin
   j) Drugo, napišite:
   _____.

4. **Za kaj vse uporabljate internet? (obkrožite lahko več odgovorov)**
   b) Brskanje po spletu b) Elektronska pošta c) Klepetalnice d) Spletni forumi
   e) Igranje iger f) Drugo,
   napišite:_____.

5. **Ali veste, da ima lahko uporaba računalnika in interneta tudi določene nevarnosti?**
   b) DA, napišite katere:_____. b) NE

6. **Ali ste že kdaj izgubili podatke (besedilo, slike...), ki ste jih imeli shranjene na računalniku?**
   a) DA b) NE

7. **Ali ste na vašem računalniku že kdaj imeli virus?**
   b) DA b) NE

8. **Ali bi znali odstraniti računalniški virus?**
   a) DA, napišite kako:_____. b) NE

9. **Ali doma uporabljate protivirusno zaščito?**
   a) DA b) NE c) NE VEM, KAJ JE TO

10. Ali poznate kakšno spletno stran, kjer si lahko preberete kaj o računalniških virusih?
b) DA, zapišite katero:_____. b) NE

11. Ali menite, da je lahko uporaba klepetalnic in elektronske pošte nevarna?
a) DA b) NE

12. Ali lahko na internetu objavite svoje osebne podatke (ime, priimek, naslov bivanja…)?
a) DA b) NE

13. Ali ste svoje osebne podatke že kdaj objavljali na internetu?
a) DA b) Redko c) Nikoli

14. Ali veste kaj je geslo?
a) DA b) NE

15. Kako dolgo geslo uporabljate ? (npr. za elektronsko pošto, MSN…)
b) 3 – 5 znakov b) 6 – 10 znakov c) več kot 10 znakov

16. Ali so vam učitelji povedali kaj o varni rabi računalnika in interneta?
a) DA b) NE

17. Ali menite, da bi bilo na šoli potrebno imeti kakšen tečaj o varni rabi računalnika in interneta?
b) DA, bilo bi koristno b) NE, tega ne potrebujemo c) NE VEM

18. Ali ste se starši kdaj pogovarjali o nevarnostih rabe računalnika in interneta?
a) DA b) NE

19. Ali ste sami že kdaj razmišljali o nevarnostih na internetu in o varnosti vaših podatkov na računalniku?
b) DA, pogosto b) Redkokdaj c) Še nikoli nisem pomislil(a) na to

PRILOGA 2: Predlog varnostne politike informacijskega sistema v OŠ Neznanih talcev Dravograd

Namen in cilji

1. člen

Varnostna politika šolskega informacijskega sistema je namenjena varovanju in zaščiti informacijskega sistema na šoli. Dokument morajo upoštevati vsi zaposleni, učenci ter zunanji sodelavci in izvajalci, ki imajo do informacijskega sistema dostop.

Namen varnostne politike je postaviti osnovna varnostna izhodišča za zaščito informacijskih sredstev pred nevarnostmi, bodisi notranjimi ali zunanjimi, namernimi ali naključnimi.

Kršitev politike

2. člen

V informacijskem sistemu mora biti zagotovljeno zaznavanje kršitev varnostne politike.

3. člen

Ob morebitni kršitvi ukrepa vodstvo šole.

Skrbnik IKT (v nadaljevanju računalničar) oz. zunanji sodelavec ima po dogovoru z vodstvom šole pravico, da ustrezno spremeni ali prepove določene storitve.

1. Politika fizičnega varovanja

Fizični dostop

4. člen

Vsi zaposleni na šoli morajo poskrbeti za ustrezno varovanje svojih prostorov.

5. člen

V prostorih, opremljenih z več računalniki, kot sta npr. računalniška učilnica in knjižnica, se redno vodi evidenca prisotnosti.

6. člen

Učenci lahko prostore z računalniki uporabljajo samo ob prisotnosti učitelja, računalničarja ali drugega takrat prisotnega izvajalca.

7. člen

Prihod zunanjih oseb v času šolskega pouka redno evidentira dežurni učenec. Dežurni učenec mora zabeležiti ime in priimek osebe, čas prihoda in odhoda ter namen obiska.

8. člen

Prostori s pomembno opremo so varovani z dodatnimi fizičnimi sredstvi.

9. člen

Vsa komunikacijska oprema in strežniki morajo biti nameščeni v zaklenjeni komunikacijski omarici.

Varovanje sredstev za dostop

10. člen

Sredstva za fizični dostop do prostorov in opreme (ključi, kartice) in elektronska sredstva morajo uporabniki varno in skrbno shraniti, jih imeti vedno pod nadzorom ter jih ne smejo posojati.

11. člen

Dokumentacija za dostop do sistemov (uporabniška imena, gesla, certifikati) mora biti shranjena v sefu oz. ustrezni drugi pred naravnimi katastrofi zaščiteni omarici. Ključ za dostop do dokumentacije ima samo za to pooblaščena oseba.

Varovanje opreme

Varovanje računalnikov in opreme

12. člen

Uporabniki morajo z računalniki in ostalo pripadajočo opremo ravnati skrbno in pazljivo.

13. člen

Uporabniki ne smejo fizično posegati v sam računalnik ali opremo.

Namestitev opreme

14. člen

Vsa nameščena oprema mora biti ustrezno zaščitena, da so nevarnosti iz okolja in priložnosti za nepooblaščeni dostop kar najbolj odpravljene.

15. člen

Vsi računalniki morajo biti nameščeni v prostoru, dvignjenem od tal, da se preprečijo okvare ob morebitnem izlitju vode oz. drugih tekočin.

16. člen

Dodatna oprema računalnika (tipkovnica, miška, ožičenje…) mora biti nameščena tako, da se karseda zmanjša možnost fizičnih poškodb.

Protipožarno varovanje

17. člen

Protipožarno varovanje naprav in opreme mora biti izvedeno v skladu s predpisi, ki urejajo to področje.

Zaščita ožičenja

18. člen

Ožičenje morajo vedno načrtovati in nameščati ustrezno usposobljeni izvajalci ter mora biti izvedeno skladno z veljavnimi standardi in predpisi ter priporočili naročnika.

19. člen

Varnost ožičenja je treba načrtovati že pri vzpostavljanju računalniških prostorov in tako pri namestitvi opreme.

20. člen

Pri vsaki nadgradnji ali spremembi omrežja ali vanj vključenih naprav mora biti preverjena varnost ožičenja.

21. člen

Električni in telekomunikacijski kabli (ožičenje), po katerih se prenašajo podatki oziroma, ki podpirajo informacijske storitve, morajo biti zaščiteni pred prestrezanjem ali poškodbami.

22. člen

Vsi priključki morajo biti dokumentirani. Posebej morajo biti dokumentirani porabljeni oziroma aktivni priključki, bodisi na aktivni opremi bodisi na priključnih panojih.

23. člen

Prosti priključki ne smejo omogočati nepooblaščenega dostopa, zato morajo biti »neaktivni« ali blokirani.

24. člen

Popravila na ožičenju lahko izvajajo samo skrbniki omrežja ali pod njihovim nadzorom strokovno usposobljeni izvajalci.

Okvare in poškodbe opreme

25. člen

Uporabniki morajo vsako okvaro in namerno ali nenamerno poškodbo opreme nemudoma sporočiti računalničarju ali vodstvu šole.

26. člen

Za vsako poškodbo opreme, ki je posledica neprimernega ravnanja, je odgovoren uporabnik.

2. Politika primerne rabe informacijskega sistema

Uporaba opreme šolskega informacijskega sistema

27. člen

Šolska informacijska oprema je v prvi vrsti namenjeni izvajanju delovnih in pedagoških procesov. Uporaba v zasebne namene je dovoljena le v primeru, ko ti ne ogrožajo informacijske varnosti ter ne motijo procesov, ki takrat potekajo v šoli.

28. člen

Uporabniki morajo z informacijsko opremo šole ravnati gospodarno in preudarno, po priporočilih proizvajalca in skrbnika sistema. Posege vanjo lahko opravljajo samo za to pooblaščene osebe.

29. člen

Uporabniki ne smejo sami nameščati programske opreme. Nameščanje in vzdrževanje te opreme je v domeni računalničarja ali pooblaščenih zunanjih sodelavcev.

30. člen

Računalničar mora poskrbeti, da so informacijski sistemi ustrezno zaščiteni pred neavtorizirano ali zlonamerno programsko opremo.

Na vsakem računalniku mora biti nameščen vsaj protivirusni programi in omogočen požarni zid operacijskega sistema.

31. člen

Zagotovljeno mora biti redno posodabljanje operacijskega sistema in pomembnih programov.

32. člen

Vsak uporabnik mora imeti dodeljene pravice, ki so nižje od administratorskih.

Škodljiva programska oprema

33. člen

Nameščanje ali uporaba škodljive programske opreme ali njeno širjenje je kršitev varnostne politike.

34. člen

Namerno nameščanje, uporaba in širjenje take opreme se najprej kaznuje z opozorilom, nato pa z začasno ali trajno prepovedjo uporabe šolskega informacijskega sistema.

35. člen

Uporabniki:

- morajo, če sumijo, da na informacijskem sistemu deluje škodljiva programska oprema, takoj nehati delati z njim in obvestiti računalničarja;
- morajo, če sumijo, da je na informacijskem sistemu škodljiva programska oprema, takoj obvestiti računalničarja in upoštevati njegova navodila;
- ne smejo zaganjati programov, ki niso del šolskega informacijskega sistema (npr. s svetovnega spleta, elektronske pošte, pomnilniških medijev);
- ne smejo zaganjati dokumentov (npr. s svetovnega spleta, elektronske pošte, pomnilniških medijev), če so sumljivi, če ne vedo, čemu so takšni dokumenti ali programi namenjeni, ali če ne poznajo njihovega izvora;
- morajo, če sumijo ali ugotovijo, da sistem za protivirusno zaščito ne deluje ali ni ustrezno posodobljen, takoj nehati uporabljati informacijski sistem, obvestiti računalničarja in upoštevati njegova navodila;

Informacijski sistemi

36. člen

Informacijski sistemi morajo biti nadzorovani. V nadzorovanih sistemih morajo biti vključeni ustrezni dnevniki, ki zagotavljajo spremljanje dogodkov.

37. člen

Dnevniki morajo omogočiti identifikacijo uporabnika, ki je bodisi dostopal do podatkov ali jih spreminjal. Tudi izpis ali izvoz podatkov iz dnevnikov mora ostati pod nadzorom in nespremenjen.

38. člen

Podatke iz dnevnika je mogoče pridobiti v primeru, ko sumimo, da gre za ogrožanje informacijske varnosti.

39. člen

Podatki iz dnevnika se lahko uporabljajo tudi za odkrivanje napak v informacijskem sistemu ali za izboljšanje njegovega delovanja.

40. člen

Uporaba zasebne opreme v informacijskem sistemu šole ni dovoljena.

Dostop do informacijskih sistemov

41. člen

Dostop do šolskega informacijskega sistema in njegovih delov smejo imeti samo zaposleni in učenci OŠ Neznanih talcev Dravograd.

42. člen

Zunanji uporabniki lahko šolski informacijski sistem in njegove dele uporabljajo le z odobritvijo vodstva šole, računalničar pa mora zagotoviti, da njihova uporaba ne bo ogrožala informacijske varnosti.

43. člen

Za vse uporabnike mora biti vzpostavljen postopek dodelitve, sprememb in prenehanja dostopnih pravic.

44. člen

Na podlagi potreb poslovnega procesa se odobri dostop do informacijskega sistema v obsegu, ki je potreben za opravljanje delovnih nalog.

45. člen

Dostop do šolskega informacijskega sistema mora biti mogoč le na podlagi overjanja, minimalno z uporabo uporabniškega imena in gesla.

46. člen

Sredstva za dostop do informacijskega sistema so neprenosljiva. Posojanje ni dovoljeno.

47. člen

Uporabnik mora skrbno varovati sredstva za dostop do informacijskih sistemov, da se ne odtujijo ali zlorabijo. Vsak sum zlorabe ali odtujitve je treba takoj prijaviti računalničarju.

48. člen

Dostop do storitev in upravljanja informacijskih sistemov ter omrežja je mogoč po sistemu pravic. Te dodeljuje računalničar ali po njegovem naročilu ARNES.

49. člen

Pravico dostopa do podatkov v omrežju lahko odobri lastnik podatkov.

50. člen

Pravico dostopa do informacijskega sistema lahko pridobijo uporabniki na podlagi potrebe in odobritve vodstva šole. Če potreba po dostopu preneha, je treba to pravico odvzeti.

51. člen

Postopek upravljanja pravic dostopa do informacijskega sistema mora biti dokumentiran, dodeljene pravice pa redno pregledovane.

52. člen

Uporabniške in administratorske pravice dostopa do informacijskih sistemov so ločene.

Načelo čiste mize

53. člen

Uporabniki ne smejo puščati dokumentov z občutljivimi podatki (dokumenti z gesli, elektronski mediji) na odprtih površinah pisarniške opreme ali drugih mestih, kjer bi lahko bili dostopni nepooblaščenim osebam.

54. člen

Ko uporabnikov ni v prostoru, morajo biti nosilci podatkov varno shranjeni.

55. člen

Zunaj delovnega časa mora biti vsa pisarniška oprema, kjer se hranijo nosilci podatkov, ki niso javni, zaklenjena ali drugače varovana.

Načelo praznega zaslona

56. člen

Ob uporabnikovi prisotnosti ali odsotnosti na delovnem mestu mora biti onemogočen vpogled na zaslon oziroma onemogočena uporaba informacijsko-komunikacijske opreme nepooblaščenim osebam.

57. člen

Omogočeni morajo biti mehanizem, ki po določenem času neaktivnosti uporabnika samodejno odjavijo iz sistema. Ob krajših prekinitvah mora za odjavo poskrbeti uporabnik.

Oddaljeni dostop

58. člen

Oddaljeni dostop do informacijskega sistema je dovoljen le na podlagi odobrene metode z ustrezno ravnjo varnosti, in sicer za tiste uporabnike, ki dostop potrebujejo zaradi opravljanja delovnih nalog, vendar le v omejenem obsegu. Treba je upoštevati tudi načelo praznega zaslona.

59. člen

Po končanem delu se je treba obvezno odjaviti iz sistema in zagotoviti, da občutljivi podatki in sledi ne ostanejo na delovni postaji.

60. člen

Promet, ki zahteva višjo varnost, se šifrira.

3. Politika primerne rabe internetnih storitev

Dostop do svetovnega spleta in storitev v svetovnem spletu

61. člen

Dostop do svetovnega spleta je omogočen vsem šolskim uporabnikom za njihovo delo, izobraževanje in informiranje.

62. člen

Uporabniki morajo uporabljati svetovni splet v skladu s pravili za uporabo internetnih storitev, ki so bila sprejeta v OŠ Neznanih talcev Dravograd.

63. člen

Na podlagi ocene tveganja je mogoče omejiti dostop do določenih vsebin, ki ogrožajo informacijsko varnost ali kršijo etične in moralne norme.

64. člen

V omrežju šole se lahko za namen preiskave suma nezakonitih dejanj beležijo dostopi uporabnikov do spletnih strani in s tem povezani podatki o dodeljenih IP naslovih. Te podatke lahko računalničar posredujejo vodstvu šole, ki ustrezno ukrepa.

65. člen

V omrežju šole se lahko izdeluje statistika obiskanih spletnih strani, ki se lahko uporablja za načrtovanje in varovanje informacijskega sistema.

Uporaba elektronske pošte

66. člen

Uporabniki morajo uporabljati elektronsko pošto v skladu s pravili o internetnih storitvah, ki so bila sprejeta v OŠ Neznanih talcev Dravograd.

67. člen

Z elektronskimi sporočili za službene namene je treba ravnati v skladu z veljavnimi pravili poslovanja z dokumentarnim gradivom.

68. člen

Vse pravice na sistemu elektronske pošte in vseh elektronskih sporočilih, ki niso zasebna, pripadajo OŠ Neznanih talcev Dravograd.

69. člen

Uporabnik ne sme uporabljati elektronskega poštnega naslova, ki je bil dodeljen drugemu uporabniku.

70. člen

Uporabniki po elektronski pošti ne smejo pošiljati zaupnih podatkov oz. se ti pošiljajo v šifrirani obliki.

71. člen

Elektronska sporočila, ki jih sprejme uporabnik na svoj elektronski poštni naslov, sme odpirati samo ta uporabnik ali s strani uporabnika pooblaščena oseba.

72. člen

Elektronska sporočila, ki prihajajo na enotne namenske elektronske poštne naslove (npr. splošni naslov šole), odpirajo za to pooblaščene osebe.

73. člen

Če uporabnik prejme elektronsko sporočilo, ki ni namenjeno njemu, vsebine tega sporočila ne sme shraniti ali kakor koli uporabiti. O tej pomoti mora obvestiti pošiljatelja, sporočilo pa mora nemudoma izbrisati ali kako drugače uničiti. Pred uničenjem ga lahko pošlje pravemu naslovniku, če je iz sporočila nedvoumno razvidna njegova identiteta.

74. člen

Vsi uporabniki se morajo zavedati, da lahko elektronsko pošto, odvisno od tehnologije, prestrežejo in obdelujejo nepooblaščene osebe.

75. člen

Uporabnik mora spoštovati avtorske pravice in pravila intelektualne lastnine, še zlasti tako, da ne uporablja sistema elektronske pošte za pošiljanje avtorsko zaščitenih informacij ali računalniških programov.

Šifriranje in podpisovanje elektronskih sporočil

76. člen

Šifriranje in podpisovanje elektronskih sporočil se izvaja le za posebne namene in z uporabo metod sprejetih v OŠ Neznanih talcev Dravograd.

Brisanje elektronskih sporočil

77. člen

Vsak uporabnik mora vsa elektronska sporočila, ki jih ne potrebuje več, občasno brisati iz svojega predala. Pri shranjevanju elektronskih sporočil morajo uporabniki upoštevati načelo racionalnosti in se izogibati hranjenju dokumentov v multimedijskih podatkovnih formatih, ki zavzamejo veliko prostora (filmi, slike visoke resolucije, zvočni zapisi).

78. člen

Elektronska sporočila, ki so zasebne narave, morajo uporabniki brisati sproti.

79. člen

Nezaželeno pošto ima pravico brisati računalničar.

4. Politika varovanja podatkov

Dostop do podatkov

80. člen

Vzpostavljeni morajo biti mehanizmi, ki preprečujejo nepooblaščeni dostop do podatkov, ter organizacijski in tehnični postopki, ki preprečujejo nepooblaščeno obdelavo podatkov, vključno s spreminjanjem oziroma uničenjem.

81. člen

Računalničar ima lahko vpogled do podatkov v primeru, ko je lastnik podatkov to odobril ali pa obstaja sum, da kateri izmed podatkov ogroža informacijsko varnost.

82. člen

Dostop do podatkov v elektronski obliki mora biti zaščiten z ustreznimi dostopnimi pravicami (npr. uporabniško ime in geslo).

83. člen

Ostalim uporabnikom lahko odobri dostop do podatkov le lastnik podatkov.

84. člen

Dostopne pravice morajo biti urejene tako, da omogočajo posamezniku dostop do najmanjšega možnega nabora podatkov, ki so potrebni za opravljanje nalog.

85. člen

Uporabniška imena, gesla, kartice za preverjanje dostopa, certifikati in drugi odobreni dostopni mehanizmi ter s tem pridobljene pravice dostopa do informacijskih sistemov in zbirk občutljivih podatkov so vedno izdani na eno osebo in so neprenosljivi. Posojanje ni dovoljeno.

86. člen

Prostori, v katerih se obravnavajo podatki, morajo biti varovani z organizacijskimi, fizičnimi in tehničnimi ukrepi, ki nepooblaščenim osebam onemogočajo dostop do podatkov in sredstev informacijske tehnologije, s katero se slednji obdelujejo.

87. člen

Uporabniki se morajo zavedati, da lahko kljub varovanju podatkov pride do njihove izgube, zato morajo za varnost pomembnih in občutljivih podatkov skrbeti tudi sami.

Upravljanje izmenljivih nosilcev podatkov

Zagotovljena morata biti ustrezno varovanje in zaščita pri upravljanju izmenljivih nosilcev podatkov.

88. člen

Na računalnikih mora biti onemogočena možnost samodejnega zaganjanja programske opreme z izmenljivih nosilcev.

89. člen

Na voljo morajo biti ustrezna sredstva, ki uporabnikom omogočajo varnostni pregled izmenljivih nosilcev ter morebitno odstranitev škodljive programske opreme.

90. člen

Izgubo ali krajo izmenljivih nosilcev podatkov je treba prijaviti računalničarju ali vodstvu šole.

91. člen

Najdeni ali kako drugače zaseženi nosilci podatkov morajo biti nemudoma izročeni računalničarju ali vodstvu šole.

5. Politika storitev zunanjih izvajalcev

92. člen

Dostopi in posegi zunanjih izvajalcev v informacijski sistem šole morajo biti evidentirani.

93. člen

Zunanji sodelavci morajo v primeru dela na daljavo, uporabljati ustrezno varovano povezavo.

6. Politika upravljanja informacijskega sistema

Časovna uskladitev

94. člen

Za sinhronizacijo dnevniških zapisov v informacijskih sistemih je obvezno treba uporabljati sistem enotnega izvora časa.

Nadzor dostopa do omrežja

Ločevanje v omrežjih

95. člen

Omrežji za pedagoške in administrativne delavce morata biti ločena. Vse spremembe na tem delu omrežja upravlja Arnes.

Dostop do omrežja internet

96. člen

V omrežju morajo biti vzpostavljeni mehanizmi, ki omogočajo omejevanje dostopa do spletnih strani.

Upravljanje incidentov pri varovanju informacij

97. člen

Računalničar ter morebitni zunanji sodelavci morajo zagotoviti, da se dejavnosti in dogodki v informacijskih sistemih beležijo. Na podlagi ugotovljenih dogodkov morajo izvajati ustrezne ukrepe.

98. člen

Vzpostavljen mora biti sistem nadzora nad delovanjem informacijskih sistemov. Vsak od njih mora vključevati postopek obveščanja zaradi morebitnih izpadov in težav v delovanju, pa tudi postopek obveščanja po odpravi težav.

Dnevniški zapisi

99. člen

Redno se izdelujejo dnevniški zapisi o spremembah in posegih v informacijskem sistemu.

100. člen

Zagotovljeni morata biti celovitost in nespremenljivost dnevniških zapisov, ki jih lahko pregleda računalničar ali katera druga za to pooblaščena oseba za potrebe informacijskega sistema ali omrežja.

Oskrba z električno energijo

101. člen

Pomembna oprema, kot so strežniki, usmerjevalnik ter omrežna stikala morajo biti priključena na sistem brezprekinitvenega napajanja.

Klimatski pogoji

102. člen

Pomembna oprema, kot so strežniki, usmerjevalnik ter omrežna stikala morajo biti nameščeni v prostorih z ustreznimi klimatskimi razmerami.

Varnostne kopije

103. člen

Vzpostavljeni morajo biti mehanizmi za varnostno kopiranje in arhiviranje podatkov ter dnevniških datotek.

104. člen

Varnostne kopije morajo biti varno hranjene na primernem mestu.

105. člen

Varnostne kopije in postopke za njihovo izdelavo je potrebno redno preverjati.

7. Politika vzdrževanja informacijskega sistema

Vzdrževanje opreme

106. člen

Za vso opremo mora biti zagotovljeno vzdrževanje, ki ga lahko opravlja računalničar ali pooblaščeni izvajalci.

107. člen

Če vzdrževanje opravijo zunanji izvajalci, morajo biti podatki zavarovani tako, da je onemogočen nepooblaščeni dostop do njih.

108. člen

Za vsak kos opreme, ki zapusti šolo zaradi vzdrževanja, je treba imeti prevzemni dokument.

Vzdrževalna dela

109. člen

Pri načrtovanih vzdrževalnih delih na programski ali komunikacijski opremi mora računalničar oz. zunanji izvajalec predhodno obvestiti uporabnike o morebitnih motnjah, ni pa odgovoren za motnje, ki nastanejo zunaj njegove pristojnosti.

8. Politika varnostnih elementov, povezanih s človeškimi viri

Ozaveščanje uporabnikov

110. člen

Šola oz. odbor za zagotavljanje informacijske varnosti mora poskrbeti za ozaveščanje uporabnikov.

Izobraževanje uporabnikov

111. člen

Šola mora uporabnikom omogočiti izobraževanja, ki so povezana z uporabo informacijsko komunikacijske tehnologije (IKT).

PRILOGA 3: Pravilnik o uporabi informacijskega sistema v OŠ Neznanih talcev Dravograd

Pravilnik u uporabi računalnikov

- Učenci lahko računalnike uporabljate le ob prisotnosti učitelja.
- Prepovedano je vsakršno fizično poseganje v računalnik.
- Uporaba računalnikov je dovoljena samo z osebnim uporabniškim imenom in geslom.
- V računalnik se morate vedno prijaviti s svojim uporabniškim imenom in geslom.
- Uporabniških podatkov za prijavo v računalnik ni dovoljeno posojati.

Pravilnik o uporabi programske opreme

- Na računalnike ni dovoljeno nameščati nobene programske opreme.

Pravilnik o ravnanju s podatki

- Svoje podatke vedno shranjujte v predpisano mapo.
- V svojo mapo lahko shranjujete samo podatke, potrebne za šolo.
- Podatkov, pri katerih vsebina ni preverjena ter obstaja možnost okužbe s škodljivo programsko opremo, ne smete shranjevati.
- Podatkov večjega obsega, kot so npr. filmi, igre... ni dovoljeno shranjevati.

Pravilnik o ravnanju z izmenljivimi nosilci podatkov

- Nosilci podatkov neznanega ali sumljivega izvora se ne smejo uporabljati.
- Preden se uporabi vsebina izmenljivega nosilca podatkov, se mora vselej preveriti njegova morebitna okuženost s škodljivo programsko opremo.

Pravilnik o uporabi internetnih storitev

- Za internet morate uporabljati brskalnik Mozilla Firefox.
- Uporaba spletnih strani z nasilno, spolno ali kakšno drugo neprimerno vsebino je strogo prepovedana.
- Uporabniki ne smete odpirati pošte in priponk neznanih pošiljateljev.
- Če sumite, da gre za nezaželeno pošto, jo nemudoma izbrišite.
- Zaupanja vrednih podatkov, kot so npr. gesla ne smete pošiljati po elektronski pošti.
- Uporabnik ne sme spreminjati nastavitev svojega elektronskega poštnega predala.