ZAGOTAVLJANJE INFORMACIJSKE VARNOSTI

/ dr. Samo Štraser / OŠ Neznanih talcev Dravograd
/ dr. Alenka Brezavšček / Univerza v Mariboru, Fakulteta za organizacijske vede

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. V članku bomo predstavili predstavili nekatere dobre prakse, ki se jih poslužujejo v tujini. V skladu z njimi 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.

Uvod

Zagotavljanje informacijske varnosti je aktualen problem, ki mu v splošnem namenjamo premalo pozornosti. Informacijsko-komunikacijska tehnologija (v nadaljevanju IKT) se namreč čedalje več uporablja, zaradi česar se povečujejo tudi možnosti za informacijske nevarnosti. Kljub ukrepom, ki jih izvajamo v praksi, se pogosto pokaže, da še nismo povsem dojeli pravega pomena informacijske varnosti. Tudi pri vodilnih v organizacijah 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. Največji problem pa se kaže v dojemanju varnosti. Vse preveč ljudi namreč naivno verjame, da je mogoče varnost preprosto kupiti v obliki izdelka, ki ga namestimo, malo preizkusimo in se tako zaščitimo pred vsemi nevarnostmi (Djurdjič 2004). Uporaba IKT je močno prisotna tudi v osnovnih šolah po Sloveniji. Čeprav država močno vzpodbuja uporabo IKT v šolstvu, se informacijski varnosti namenja premalo pozornosti. Osnovne šole po Sloveniji so pri zagotavljanju informacijske varnosti prepuščene lastnim interesom, zato je temu primerno to področje tudi urejeno. Ker ni sprejete niti predlagane kake enotne rešitve, je vsaka šola primorana zagotavljati informacijsko varnost po svoje, v okviru obstoječih znanj in zmožnosti. V prispevku bomo opisali stanje na področju zagotavljanja informacijske varnosti v slovenskem šolstvu. Predstavili bomo državne institucije, ki na tem področju delujejo. Na kratko bomo predstavili tudi rezultate raziskave, v kateri smo preverili stanje na področju zagotavljanja informacijske varnosti na slovenskih osnovnih šolah. Na podlagi dostopne literature bomo proučili, kakšne so dobre prakse v tujini, ki bodo osnova za oblikovanje splošnih smernic za zagotavljanje informacijske varnosti v slovenskih osnovnih šolah. V skladu s temi smernicami bomo strnjeno predstavili prenovo informacijskega sistema v OŠ Neznanih talcev Dravograd. Rešitev bo zajela vsa osnovna področja informacijske varnosti, in sicer: sistemsko varnost, varnost podatkov, omrežno varnost, fizično varnost in organizacijsko varnost. Upoštevali bomo različne vidike s strani uporabnikov (skrbnik IKT, učitelj in učenec). Poleg tega bomo upoštevali omejenost s sredstvi, zato bomo v čim večji možni meri planirali izrabo lastnih sredstev. Predstavljena rešitev bo primer dobre prakse, ki jo bo po našem mnenju možno aplicirati na katerokoli slovensko osnovno šolo.

IKT v slovenskem šolstvu

IKT je močno prisotna tudi v našem šolstvu. Slovenija je bila namreč ena izmed prvih evropskih držav, ki je v letu 1993 zagotovila pogoje za dolgoročni sistematični preskok na področju IKT pri poučevanju in učenju. V letu 1999 je bil ugotovljen vse večji prepad med tistimi učitelji, ki so IKT osvojili kot del življenja in del 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 katero 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, ipd.). 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 področju izobraževanja učiteljev, na področju opremljanja vzgojno-izobraževalnih zavodov (v nadaljevanju VIZ) in na področju raziskave in razvoja. Veliko rezultatov dosedanje informatizacije se lahko oceni kot uspešne, vendar pa proces informatizacije šolstva v Sloveniji še vedno živi vzporedno z običajnim 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 (Ministrstvo za izobraževanje, znanost, kulturo in šport 2006).

Državne institucije na področju zagotavljanja informacijske varnosti

V Sloveniji na srečo deluje tudi nekaj državnih institucij, ki šolam pomagajo skrbeti za informacijsko varnost. Največjo pomoč izobraževalnim ustanovam pri zagotavljanju informacijske varnosti nudi Akademska in raziskovalna zveza Slovenije (v nadaljevanju Arnes). V Sloveniji poteka še nekaj ostalih projektov, ki ozaveščajo o informacijski varnosti učitelje, učence ter njihove starše. Med temi so najbolj poznani:

- Projekt Center za varnejši internet SAFE-SI. 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.
- Projekt NASVET ZA NET. Projekt 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.
- Projekt VARNI NA INTERNETU. Projekt je zastavljen dolgoročno in naslavlja precej široko področje problematike informacijske varnosti. Aktivnosti projekta so usmerjene k višji stopnji zavedanja glede nevarnosti na spletu, informiranju o varni uporabi spletnega bančništva, informiranju o različnih oblikah spletnih prevar in o varstvu osebne identitete v socialnih omrežjih.

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. Ugotovili smo, da 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 v pomoč tudi pri spremljanju uporabniških aktivnosti, da bomo lahko ob nepravilnostih ustrezno ukrepali. Skrb za varnost podatkov je zelo pomembna, saj lahko vsaka njihova izguba povzroči 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.

Vidik učiteljev in učencev

Po rezultatih raziskave sodeč uporabljajo učitelji in učenci IKT vsakodnevno, poznajo osnovne nevarnosti, ampak jim ne posvečajo dovolj pozornosti. Menimo, da je zato potrebno v šoli organizirati program ozaveščanja o informacijski varnosti za učitelje in učence. 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. Za učence je potrebno pripraviti podoben program, vendar s prilagojenimi vsebinami. Seveda pa ozaveščanje učencev ni le naloga računalničarja in učiteljev, ampak tudi njihovih staršev.

Prenova informacijskega sistema v OŠ Neznanih talcev Dravograd

V skladu s predlaganimi smernicami za izboljšanje informacijske varnosti in z dobrimi praksami, ki se uporabljajo v tujini, smo želeli prenoviti informacijski sistem v OŠ Neznanih talcev Dravograd. Na šoli namreč zaznavamo, da največ groženj izvira od znotraj. Nekaj groženj je posledica slabo varovanega informacijskega sistema, nekaj pa jih s svojimi dejanji povzročajo uporabniki. Po analizi in preizkušanju najrazličnejših tehničnih 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.

Zagotavljanje sistemske varnosti

OSS smo namestili na zmogljivejši osebni računalnik, za višjo varnost pa smo v računalnik vgradili dva identična trda diska, ki omogočata zrcaljenje podatkov (RAID 1). Med namestitvijo smo izbrali le najbolj nujne storitve, saj več storitev pomeni tudi več nevarnosti za sistem. Za optimalno delovanje in upravljanje smo omogočili naslednje:

- 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 lokalnega omrežja, zato le-te ne predstavljajo dodatnih nevarnosti za sistem ter omrežje. Številni podatki (uporabniški

podatki, nastavitve omrežja, nastavitve sistema, ipd.) 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. Skrbi torej 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. 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. Uporabili smo predpisane uporabniške profile. To je posebna vrsta profila, shranjenega na strežniku, ki ima onemogočeno možnost spreminjanja. Profil je se pri prijavi uporabnika naloži na delovno postajo. Uporabnik lahko začasno spremeni nastavitve, vendar se pri odjavi spremembe ne shranijo. Za zaščito pred virusi smo uporabili odprtokodni protivirusni program ClamAV, ki ga OSS že privzeto vsebuje. 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.

Zagotavljanje omrežne varnosti

Višjo omrežno varnost smo zagotovili s primerno postavitvijo OSS v omrežje. 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 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. Za omejevanje dostopa do nekaterih spletnih strani uporabljamo namestniški strežnik Squid in program SquidGuard. 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.

Na vseh komunikacijskih napravah, do katerih imamo dostop, imamo nastavljena močna gesla, za dostop pa omogočene samo varne komunikacijske kanale. Poleg tega je dostop omogočen samo točno določenim IP naslovom.

Varnost podatkov

Zagotavljanje podatkovne varnosti 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«. 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. 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.

Zagotavljanje fizične varnosti

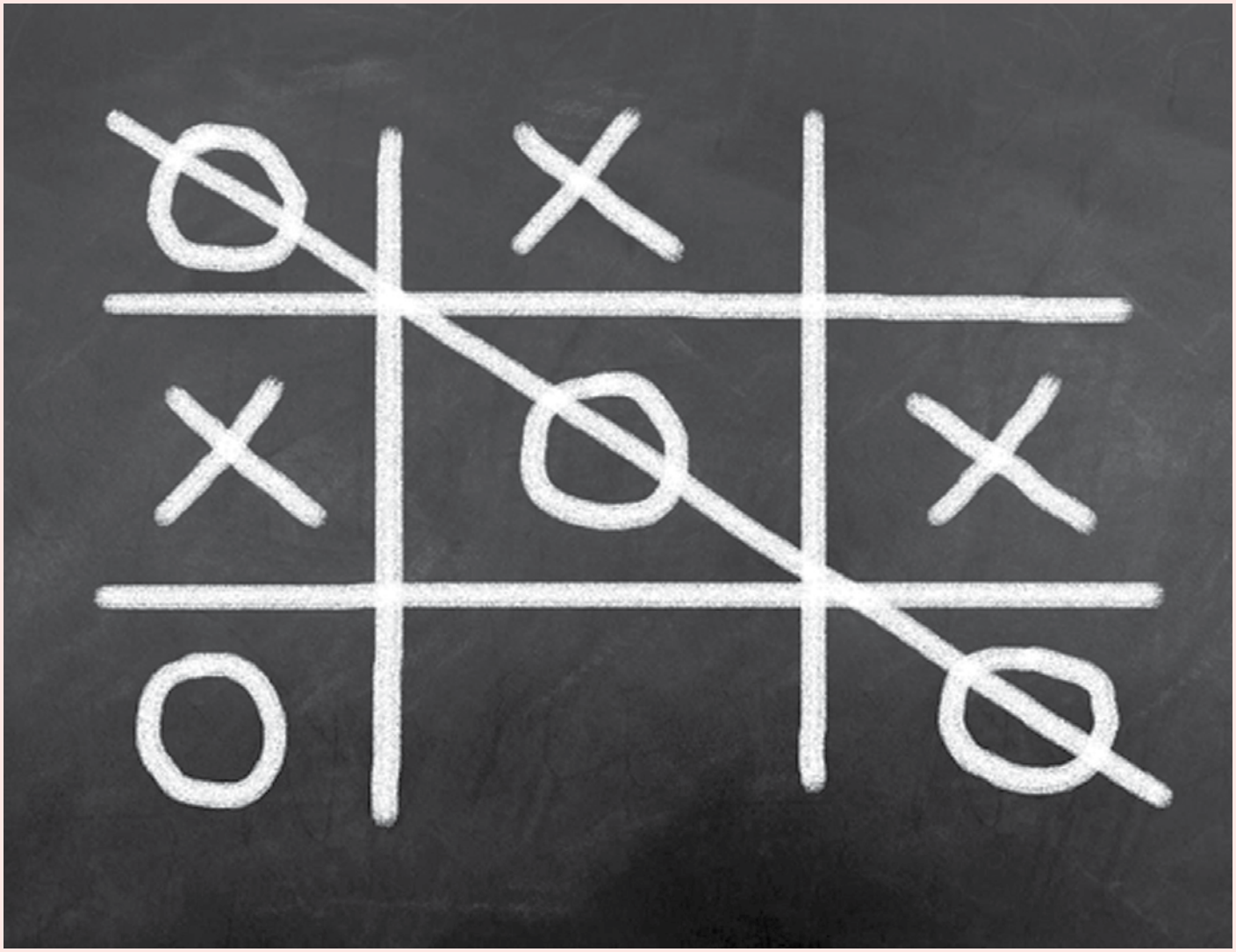
Za zagotavljanje fizične varnosti smo strežnik in ostale komunikacijske naprave namestili v varovano komunikacijsko omaro. Dostop do omare ima skrbnik IKT in ravnatelj šole. Prostor ni klimatiziran, zato ga v poletnem času ustrezno zračimo. Strežniku in komunikacijskim napravam smo zagotovili brezprekinitveno napajanje. Naprava za brezprekinitveno napajanje omogoča ob trenutni porabi nekje do pol ure samostojnega delovanja. To zadošča za varen izkop strežnika ter preprečuje morebitne izgube podatkov ali druge okvare na strežniku ob izpadu električnega omrežja. 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 nam omogočajo v primeru požara varno gašenje električnih naprav.

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. Do sedaj smo oblikovali predlog varnostne politike informacijskega sistema in pravilnik o uporabi šolskega informacijskega sistema.

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 prispevku smo na kratko opisali stanje na



področju zagotavljanja informacijske varnosti v slovenskem šolstvu in predstavili državne institucije, ki na tem področju delujejo.

Na podlagi dobrih praks, ki se uporabljajo v tujini, smo oblikovali splošne smernice za zagotavljanje informacijske varnosti v osnovni šoli. V skladu temi smernicami smo prenovili informacijski sistem v OŠ Neznanih talcev Dravograd. S tehničnega vidika smo informacijsko varnost bistveno izboljšali z uporabo Open School Serverja oz. OSS, kot smo ga poimenovali. Gre za sistem, ki omogoča enostavno upravljanje ter zagotavlja visok nivo informacijske varnosti, ki je primeren za osnovne šole. Organizacijsko varnost zagotavljamo z lastnimi sredstvi, saj smo ugotovili, da imamo dovolj znanja na tem področju. Menimo, da smo s prenovo informacijskega sistema OŠ Neznanih talcev Dravograd kljub majhnemu finančnemu vložku dosegli bistveno izboljšavo na področju zagotavljanja informacijske varnosti. Z gotovostjo lahko trdimo, da bi pristop, ki smo ga uporabili na naši osnovni šoli, lahko uporabile tudi ostale osnovne šole v Sloveniji.

Literatura

- Arktur – Schulserver (2011): Arktur – Schulserver, dosegljivo na naslovu: http://arktur.shuttle.de/, obiskano dne, 16. 2. 2011.
- Arnes (2010): Predstavitev zavoda Arnes, dosegljivo na naslovu: http://www.arnes.si/zavod-arnes/predstavitev.html, obiskano dne, 14. 12. 2010.
- 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.
- 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.
- Djurdič,V. (2004): Varnost pred vsem, dosegljivo na naslovu: http://www.monitor.si/clanki.php?id=358, obiskano dne, 5. 2. 2010.
- Linux – Schulserver (2011): Linux – Schulserver, dosegljivo na naslovu: http://www.linux-schulserver.de/, obiskano dne, 16. 2. 2011.
- 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.
- Open School Server (2011): Open School Server, dosegljivo na naslovu: http://www.openschoolserver.net/, obiskano dne, 16. 2. 2011.
- Samuelle, T.J (2009): Mike Meyers' CompTIA Security+ Certification Passport, Second Edition, McGraw-Hill, ZDA.
- Skolelinux (2011): Skolelinux, dosegljivo na naslovu: http://www.slx.no/, obiskano dne, 16. 2. 2011.