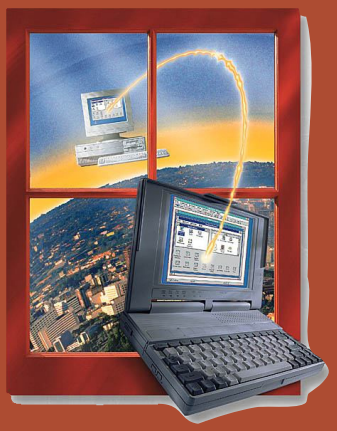
Kratek uvod v zanesljivo zaščito lokalnega omrežja, elektronske pošte in internetnega dostopa.

Zaradi vse bolj kontra-diktornih informacij v zvezi z varnostjo računalniških omrežij smo se odločili definirati osnovne pojme in predstaviti naše mnenje.



VARNO OMREŽENI

V podjetjih, tako velikih kot malih, si danes težko predstavljamo poslovanje brez krajevnega omrežja računalnikov in povezave v internet. Z uvedbo ADSL je postala stalna, hitra in zanesljiva povezava v internet dostopna vsem. Izmenjava informacij preko elektronske pošte pa je že odpravila primat telefaksov in znižala mesečne telefonske stroške.

Na žalost je poleg prednosti hiter dostop do interneta s seboj prinesel tudi težave. Poleg zoprnih reči, kot so neželeni oglasi za sumljive izdelke, so tu tudi prav resne nevarnosti, kot so vdori v lokalno omrežje ter vedno pronicljivejši in nevarnejši virusi.

Čeprav navidezno različne kategorije težav so to v resnici le različne plati istega problema - stranice istega trikotnika. Vsi že dobro poznamo scenarij, ko virus, ki smo ga prejeli po elektronski pošti, omogoči vdor do našega računalnika, tega pa potem zlorabijo kot odskočno desko za nadaljnje pošiljanje omenjenih neželenih reklamnih oglasov. To pa je le eden izmed mnogih scenarijev in razlogov, zakaj je potrebno vsako stalno povezavo do interneta še posebej pazljivo nadzorovati in varovati.

Seveda pa kakovostna zaščita tudi stane. Veliki proizvajalci nas že nekaj časa prepričujejo, da so edino njihovi (pre)dragi vdorobrani (firewall) dovolj varni. Prav tako trdijo, da se proti nezaželeni elektronski pošti (SPAM) in virusom lahko borimo le delno uspešno, pa čeprav uporabljamo drage komercialne programe z obvezno letno naročnino.

Na žalost pa praksa kaže, da nobena od teh trditev ne drži. Zato smo v našem podjetju še posebej veseli, da Vam lahko ponudimo kombinacijo izdelkov in programov, ki bodo varovali Vaše računalnike in omrežje bolje kot desetkrat – ali pa celo stokrat (!)- dražji sistemi.

Narediti popolnoma varno omrežje je namreč zelo enostavno. Dovolj je, da vse računalnike in njihovo povezovalno opremo zaklenemo v klet in da jih nikoli in pod nobenim pogojem ne vklopimo...

VDOROBRAN (Firewall)

Vdorobran, ki ga bolj poznamo pod njegovim angleškim imenom »Firewall«, je računalnik, ki filtrira in nadzira pretok podatkov med dvema računalniškima omrežjema. Vdorobran navadno »sedi« med internetom in našim krajevnim omrežjem, njegova naloga pa je, da preprečuje neželeni promet iz zunanjega sveta - interneta – v našo krajevno omrežje (LAN), hkrati pa prepušča želeni oz. legitimni promet v krajevno omrežje in iz njega.

Narediti popolnoma varno omrežje je namreč zelo enostavno. Dovolj je, da vse računalnike in njihovo povezovalno opremo zaklenemo v klet in da jih nikoli in pod nobenim pogojem ne vklopimo. In čeprav bi bilo takšno omrežje popolnoma varno, bi bilo prav tako popolnoma neuporabno. Izziv je narediti takšno obrambo, ki nam ne ovira vsakdanjega dela.

Pomembna lastnost vdorobranov ni samo, kako dobro in hitro filtrirajo promet, temveč tudi, kako odporen na zlorabe je tudi sam vdorobran.. Kakovostni vdorobrani omogočajo celo vrsto storitev in nudijo zelo sofisticirane načine filtriranja, ki pa so mogoči le na precej zmogljivih operacijskih sistemih. Problem je preprost: vdorobran naj varuje krajevno omrežje pred vdori, ki jih omogočajo pomanjkljivosti v operacijskih sistemih in programju – ali naj na vdorobranu teče isti luknjasti operacijski sistem, ki nam povzroča težave že na naših računalnikih?

Kdo bo varoval varovalca?

Zato smo se odločili za uporabo operacijskega sistema OpenBSD. Osnovno vodilo pri nastanku tega brezplačnega operacijskega sistema je bila želja po zanesljivem in varnem sistemu brez kompromisov. Njegovi avtorji zagovarjajo vnaprejšnji pristop k odpravi pomanjkljivosti ter stalno testiranje in iskanje možnih točk vdora. Rezultat njihovega truda je hiter in zmogljiv operacijski sistem, ki je idealna platforma za razne varnostne aplikacije. Več podrobnosti lahko najdete na spletnih straneh:

www.openbsd.org

www.openbsd.org/security.html

www.openbsd.org/press.html

Ena zanimivejših dodatnih storitev, ki jih omogoča vdorobran, zgrajen na operacijskemu sistemu OpenBSD, je Navidezno Zasebno Omrežje (NZO) ali VPN (Virtual Private Network). NZO vzpostavi varno (šifrirano) povezavo med dvema računalnikoma ali drugima zasebnima omrežjema preko javnega omrežja – interneta. To nam omogoča poceni in varno povezavo v naše lokalno omrežje, kjerkoli na svetu smo. Za povezavo potrebujemo le računalnik (PC, notesnik, PDA...) in krajevni dostop do interneta (telefonsko linijo, GSM, javni WLAN...) in že imamo na razpolago vse podatke in funkcionalnost našega zasebnega omrežja prav tako, kot če bi sedeli v svoji pisarni.

POŠTNI STREŽNIK (Mail Server)

Nudimo Vam popolno inštalacijo in podporo za poštni strežnik qmail. Po našem mnenju (in po mnenju naših strank) je qmail najboljši strežnik za elektronsko pošto: Brezplačen je, zelo učinkovit in zmogljiv, ima odlično varnost in široko bazo uporabnikov po vsem svetu, pa še odlično se ujema z varnostno usmerjenim operacijskim sistemom OpenBSD, na katerega ga nameščamo.

Nekaj največjih namestitev poštnega strežnika qmail po svetu: USA.net, Address.com, Rediffmail.com, Colonize.com, Yahoo! mail, Network Solutions, Verio, MessageLabs (preiskujejo preko 100 miljonov sporočil na teden v iskanju virusov in drugih škodljivih pošiljk), Ohio State University (največja univerza v ZDA), Yahoo! Groups, Listbot, USWest.net, RIPE, Telenordia, gmx.de, NetZero, Critical Path (15 miljonov elektronskih poštnih nabiralnikov), PayPal/Confinity.

Več informacij najdete na:
www.qmail.org
www.inter7.com

Qmail je idealna rešitev za začetni poštni strežnik za mala do srednje velika podjetja. Je modularen, prilagodljiv, predvsem pa omogoča kasnejšo širitev do velikega poštnega sistema za stranke z veliko količino pošte. Zaradi take zasnove je delovanje možno dopolniti s celovito zaščito pred širjenjem virusov preko elektronske pošte in filtriranjem nezaželenih elektronskih sporočil.

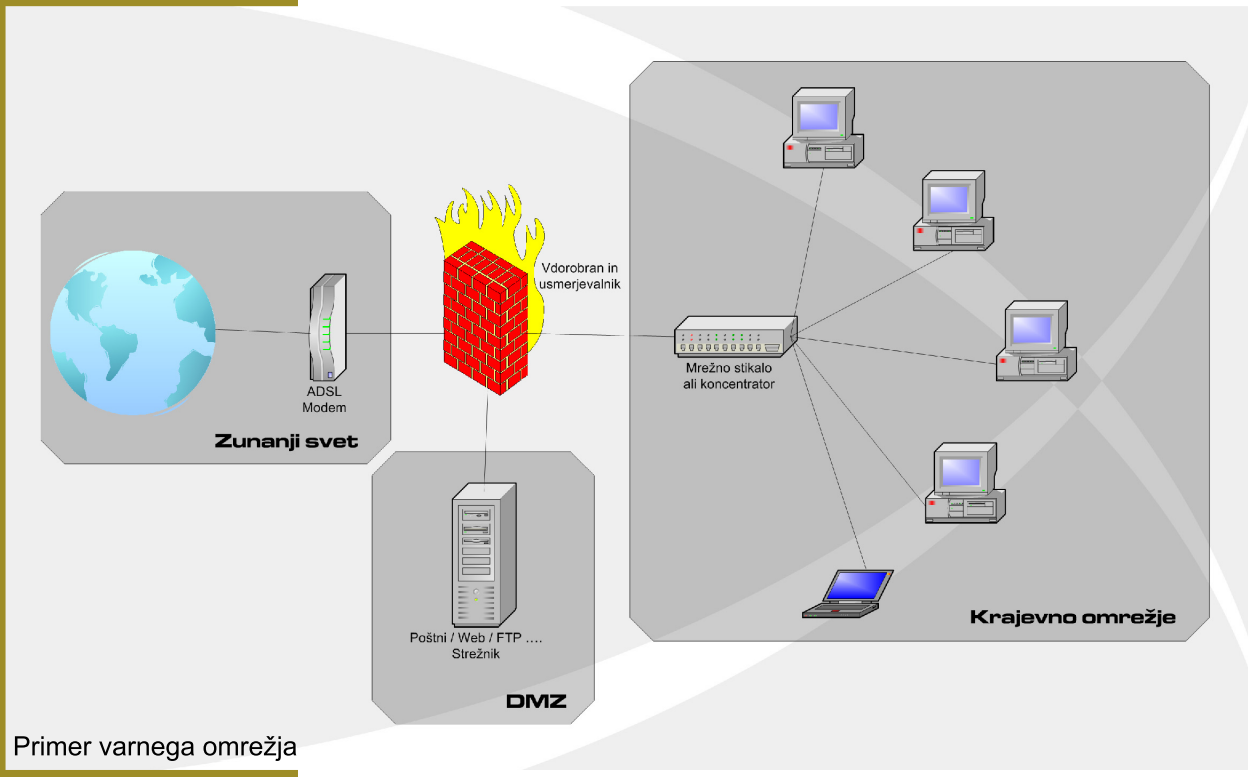
Seveda pa vam strežnika ne le postavimo, temveč nudimo celotno paleto vzdrževalnih in nadzornih storitev v podporo našim inštalacijam. Uporabniki verjetno ne bodo niti opazili, da ima vaše podjetje lasten poštni strežnik – ugotovili bodo le, da naenkrat lahko počnejo veliko bolj koristne zadeve s svojo elektronsko pošto.

Prednosti lastnega poštnega strežnika so številne, ogledali si bomo le nekatere očitnejše. Morda že sedaj uporabljate lastno domeno kot del elektronskega naslova, kar nekateri ponudniki elektronske pošte omogočajo (Siol, Softnet in drugi). Lastni strežnik vam omogoča, da ste od takega ponudnika elektronske pošte neodvisni – sami določate velikost predalov elektronske pošte (kolikor želite!); sami ustvarjate nove elektronske naslove hitro, preprosto in brezplačno; pošiljanje in prejemanje pošte je izredno hitro, saj vaš računalnik pošto v trenutku preko krajevnega omrežja odda strežniku, ta pa jo dostavlja tako hitro, kot to zmore vaša internetna povezava. Nobenih ovir ni, da tak poštni strežnik uporabljate kot zmogljiv interni sistem elektronske pošte – tista 400MB datoteka prispe do sodelavca prej, preden sploh najdete prazen CD, na kateri bi mu jo nesli !

Qmail je idealna rešitev za začetni poštni strežnik za mala do srednje velika podjetja. Je modularen, prilagodljiv, predvsem pa omogoča kasnejšo širitev do velikega poštnega sistema za stranke z veliko količino pošte.

ANTIVIRUSNI FILTER

Pri namestitvah poštnega strežnika qmail uporabljamo antivirusni program Clam Antivirus (www.clamav.net). Clam je vodilni nekomercialen antivirusni program, ki ga odlikujejo hitrost, zmogljivost in fleksibilnost. Nameščen je skupaj s strežnikom qmail, tako da pošto pregleda takoj, ko ta pride v strežnik; tudi arhivske datoteke v priponkah sporočil zanj niso ovira. Za prepoznavanje virusov uporablja lastno knjižnico podatkov o virusih, ki se samodejno obnavlja preko interneta nekajkrat dnevno. Od dragih komercialnih izdelkov (Symantec/Norton, Kaspersky Labs in drugi) se razlikuje v tem, da za knjižnico podatkov o virusih skrbijo prostovoljci - vseeno uspešno prepozna preko 20.000 različnih virusov.



Primer varnega omrežja

FILTER PROTI NEŽELJENI POŠTI (Anti SPAM)

Nezaželeno elektronsko pošto prepoznava program SpamAssassin (www.spamassassin.org). Tako kot antivirus tudi antispam program pregleda vsako elektronsko sporočilo, ki prispe v poštni strežnik. Za prepoznavanje ne uporablja knjižnice nezaželenih sporočil, saj to ne bi bilo smiselno – reklame za viagro in podobna sporočila se namreč nenehoma spreminjajo. SpamAssassin uporablja zbirko pravil, s katerimi skuša oceniti, ali ima elektronsko sporočilo tipične elemente neželene pošte – neobičajna ločila v naslovu, čudne naslovnike, nepravilnosti v zaglavju (header) sporočila, omenjanje viagre ali kup dolarskih znakov in podobno. Vsak najden element prispeva k skupni oceni in če ta presega določeno mejo, sporočilo razglasimo za spam. Ta mehanizem seštevanja preprečuje, da bi en sam sumljiv element povzročil, da sporočilo po krivem proglasimo za spam. Dva zdravnika si zato mirno lahko dopisujeta o klinični rabi viagre, ne da bi zato sporočilo razglasili za spam.

Sporočilo smo prepoznali kot spam, kaj sedaj? Najekstremnejši ukrep je seveda takojšnje brisanje, preden prejemnik to sporočilo sploh vidi. To ni najboljša rešitev, saj je prepoznavanje nezaželene pošte po vsebini mnogokrat še za človeka zapleteno, kaj šele za program. Po načelu, da

je bolje izpustiti sto krivcev kot zapreti nedolžnega, uporabljamo metodo označevanja. Spam dostavimo k naslovniku, le v polje »Zadeva« (Subject) dodamo označbo SPAM. Uporabnik si preprosto nastavi pravilo, ki mu takšno elektronsko pošto premakne v posebno mapo, ki jo občasno preleti in izprazni. Običajna pošta bo tako očiščena nesnage, če pa je bilo pošteno sporočilo po krivici prepoznano kot spam, ga bo uporabnik lahko rešil pred izbrisom.

POGOSTA VPRAŠANJA (FAQ)

Zakaj je OpenBSD zastonj, če je tako dober?

OpenBSD je odprtokodni (Open Source) operacijski sistem, kar pomeni, da ga razvija skupnost prostovoljcev za lastne potrebe. Programska oprema je brezplačna, saj so se avtorji odrekli plačilu, vendar sam sistem ni zastonj, saj plačujete podjetju, ki Vaš sistem postavlja in vzdržuje, za njihove storitve in znanje in ne za programsko opremo samo. Torej plačujete resnično – otipljivo – dodano vrednost oz. storitev in ne le provizije za preprodajo licence za programje. Model, pri katerem uporabnik ni vezan na nakup licence, nudi veliko varnost investicije – če s sistemom ali storitvami vzdrževalca kupec ni zadovoljen, ga lahko brez posledic ali izgube denarja zaradi zgrešenega nakupa licence odslovi, zamenja z drugim ali celo sistem postavi in upravlja sam.

Zakaj izdajo novo verzijo OpenBSD vsakih 6 mesecev?

OpenBSD je izrazito usmerjen v varnostne aplikacije. Grožnje in varnostna tveganja se spreminjajo iz dneva v dan. Razvojni cikel je temu prilagojen, nove različice izhajajo vsakih šest mesecev zato, da tem trendom sledijo. Pri večini drugih operacijskih sistemov izide nova različica takrat, ko imajo programerji pripravljenih dovolj temeljnih novosti ali pa jo celo zahteva marketing, kar lahko traja leta. Pri OpenBSD-ju je naslednja različica evolucijsko nadaljevanje prejšnje, prilagojene trenutnim varnostnim razmeram. Razvijalci menijo, da šestmesečni razvojni cikel nudi najboljše razmerje med aktualnostjo izdelka in kakovostjo razvoja.

Kaj je DMZ in zakaj ga rabimo?

DMZ je kratica za demilitarizirano cono (DeMilitarized Zone). DMZ je posebno krajevno omrežje, ki je ločeno od našega krajevnega omrežja in od interneta. Med sovražno cono - internetom - in absolutno varno cono - krajevnim omrežjem - smo postavili še vmesno sivo cono. Dostop iz interneta v varno cono - krajevno omrežje - ni možen, v DMZ pa je možen omejeno in pod skrbno nadzorovanimi pogoji. V to posebno omrežje povežemo strežnike, ki morajo biti dostopni iz interneta, kot sta npr. poštni ali pa spletni strežnik. Kljub temu, da so tovrstni strežniki skrbno izdelani in preverjeno varni, izhajamo iz predpostavke, da se vendarle lahko najde kakšna ranljivost, pa čeprav je možnost za to izredno majhna. Z uporabo omrežja DMZ dosežemo princip omejene škode, saj tudi v primeru kompromitiranja javnosti dostopnih strežnikov v DMZ napadalec ne prodre v naše veliko bolj pomembno krajevno omrežje.

Ali se lahko povežemo v OBSD tudi iz drugih operacijskih sistemov?

Da, do strežnika z operacijskim sistemom OpenBSD lahko dostopamo tudi iz drugih operacijskih sistemov. Tradicionalne internetne storitve, kot sta denimo www, mail in ftp, so od vrste uporabljenih računalnikov ali operacijskega sistema, ki na njih teče, povsem neodvisne. Nenazadnje je to tudi temeljna ideja Interneta! OpenBSD poleg tega pozna še podporo za protokol SMB, s katerim se lahko povezujemo znotraj omrežja Microsoft Windows (prenos datotek, skupna raba datotek in tiskalnikov ipd.) in protokol Appletalk, s katerim se lahko povezujemo v omrežje Apple/Macintosh.

Kdo lahko dostopa in upravlja z vdorobranom in kako varni so naši podatki?

Za dostop do vdorobrana postavimo sistem upoorabnikov z individualnimi gesli in pooblastili. Za preprečitev zlorab moramo poznati oba načina dostopanja do vdorobrana: Prvi je preko konzole na vdorobranu samemu, kamor se preko serijskega kabla priključimo z drugim računalnikom. Pri naših inštalacijah je to edini dostop, ki dovoljuje prijavo kot administrator, saj mora biti tisti, ki na ta način dostopa do vdorobrana, fizično v istem prostoru. Torej je varovanje takšnega dostopa zelo preprosto – zaklenemo vrata!

Drugi način je preko omrežja - zasebnega ali javnega – z uporabo Secure Shell (ssh) povezave. Promet med vdorobranom in računalnikom, s katerega dostopamo, je šifriran in onemogoča prisluškovanje naši povezavi. Naša odločitev pri postavitvi sistema je, da se vsi varnostno občutljivi ukazi samodejno beležijo v sistemskih dnevnikih, kar omogoča natančen nadzor nad delom upravljalcev omrežja.

Kaj je VPN?

Navidezno zasebno omrežje (VPN, Virtual Private Network) je koncept, ki opisuje, kako dve zasebni (krajevni) omrežji povežemo v eno veliko navidezno omrežje preko javnega, nevarnega omrežja. V praksi to pomeni, da lahko prek interneta povežemo dve omrežji v eno samo in se tako izognemo stroškom fizične povezave ali telefonskega klica. Povezava je šifrirana, varna in za uporabnika povsem transparentna – videti je, kot da smo v oddaljeno omrežje povezani s kablom. NZO je lahko preprosto poslovnežev prenosnik, ki je povezan v omrežje podjetja, ali pa velik sistem omrežij več podjetij.

Kako lahko uporabljam VPN z mojega notesnika ali domačega računalnika?

Če ima notesnik ali domači računalnik operacijski sistem Microsoft Windows 2000 ali XP, potem je osnovna podpora za VPN že vgrajena. Namestiti je treba le datoteke z nastavitvami, ki jih pripravi vzdrževalec vdorobrana. Če uporabljamo katero starejših različic Windows ali če želimo zmogljivejšo in za uporabo udobnejšo podporo za VPN, je potrebno namestiti programski paket (priporočamo SSH Sentinel), ki pa žal ni brezplačen. Operacijski sistem Mac OS X prav tako že vsebuje osnovno podporo, zanj pa tudi obstaja zmogljivejši komercialni odjemalec za VPN.

Ali deluje Qmail tudi z Microsoft Outlook-om?

Da, programi za prebiranje in pisanje elektronske pošte, med katere sodi tudi Microsoft Outlook, se do poštnega strežnika povezujejo preko standardnih internetnih povezav (protokola POP3 in SMTP). Programu zato ni potrebno vedeti za tip ali proizvajalca poštnega strežnika, s katerega pobira elektronsko pošto. Velika verjetnost je, da vaš trenutni ponudnik elektronske pošte uporablja Qmail ali soroden poštni strežnik, ne da bi vi to vedeli ali opazili.

Ali lahko uporabljam svoj poštni predal tudi od doma oz. izven krajevnega omrežja?

Da, lahko. Upravitelji poštnih strežnikov tradicionalno niso dopuščali dostopa do poštnih predalov izven krajevnega omrežja, saj je pri površni nastavitvi poštnega strežnika obstajala možnost, da nepooblaščeni strežnik zlorabijo denimo za množično pošiljanje neželene elektronske pošte, upravitelji zato niso hoteli tvegati. Žal se je ta praksa iz zgodnjih dni interneta ohranila do današnjih dni, čeprav zanjo ni več nobenega razloga. Zagotovimo lahko, da pravilno nastavljen sodoben poštni strežnik, kot je qmail, povsem varno omogoča dostop do poštnega predala od kjerkoli, seveda, če imate veljavno uporabniško ime in geslo. Obstaja pa še druga možnost, to je uporaba spletnega vmesnika za prebiranje pošte (webmail), s katero lahko do svoje pošte dostopimo resnično povsod, tudi na tujih ali javnih računalnikih.

Kaj pa, če že imam elektronski naslov pri kakšnem drugem ponudniku internetnih storitev (Siol, Amis...)?

Vaš dosedanji naslov lahko še naprej nemoteno uporabljate, seveda pa izgubite vse omenjene prednosti lastnega poštnega strežnika. Pomagamo vam lahko, da svoj dosedanji elektronski naslov prenesete na lastni strežnik. Obstaja pa tudi metoda, po kateri vaš poštni strežnik samodejno pobira vašo pošto iz obstoječega naslova pri drugem ponudniku in jo naloži v vaš poštni strežnik. Ob tem vašo pošto poštni strežnik tudi pošlje skozi antivirusni in antispam filter.

Zakaj potrebujem Antivirusni filter, če že imam antivirusni program na svojem računalniku?

Antivirusni program na vašem računalniku virus prestreže, ko sporočilo že pride do vašega računalnika in je že v vašem programu za branje elektronske pošte. Čeprav je bil virus verjetno prestrežen, ste zapravljali čas za prenos tega sporočila in da ste ga zbrisali iz arhiva vseh sporočil. V navalu sodobnih poštnih virusov in črvov je lahko takih sporočil tudi nekaj sto na dan in s svojo številčnostjo povsem zasenčijo morebitno legitimno pošto. Antivirusni filter na poštnem strežniku poskrbi, da okuženega sporočila sploh ne vidite. Naj bo antivirusni program na vašem računalniku vaša zadnja in ne edina obramba!

Kaj pa, če AntiSPAM zamenja legitimno sporočilo za neželenega?

Sporočilo bo prestavljeno v mapo z nezaželenimi sporočili, ki jo mora uporabnik sam redno prazniti. Ob tem bo legitimno sporočilo verjetno opazil in rešil pred izbrisanjem. Oglejte si naš podrobni opis delovanja Spam Assassin na strani 4.

Ali imam lahko tudi svoj spletni strežnik? Kako?

Preprosto. Operacijski sistem OpenBSD vsebuje spletni strežnik Apache, ki velja za najbolj razširjen svetovni spletni strežnik – poganja namreč preko 75% spletnih mest širom po svetu. Uporaba ustrezno pripravljenega spletnega strežnika je enostavna, saj vsebino pripravljamo in postavljamo na strežnik kar preko krajevnega omrežja.

Kaj še lahko počnem s svojim novim, varnim omrežjem?

Vaše varno omrežje lahko skrbi za točen čas vseh računalnikov v njem (protokol NTP), streže datoteke tako interno kot tudi v internet (ftp), shranjuje datoteke in njihove varnostne kopije (file server/backup), prikazuje stanje strežnikov (symon), nadzoruje sistem neprekinjenega napajanja (UPS – nut) in še mnogo drugega. Pravzaprav, sistem lahko počne skoraj vse, kar si zaželite, saj je to odprta platforma, ki jo lahko prilagodimo vašim željam in potrebam!

KERBEROS d.o.o.
Cikava 15, SI-1290 GROSUPLJE
info@kerberos.si

Kontaktna oseba: Mitja Muženič, GSM: 040 39 00 39