EESTI INFOTEHNOLOOGIA KOLLEDŽ

Siim Adamson

E-POSTI TEENUSE UUENDAMINE EESTI MEREAKADEEMIA NÄITEL

Diplomitöö

INFOTEHNOLOOGIA SÜSTEEMIDE ARENDAMISE ÕPPEKAVA

Juhendaja: I. Rokk

Tallinn 2009

AUTORIDEKLARATSIOON

Deklareerin, et käesolev diplomitöö, mis on minu iseseisva töö tulemus, on esitatud Eesti Infotehnoloogia Kolledžile lõpudiplomi taotlemiseks Infosüsteemide administreerimise erialal. Diplomitöö alusel ei ole varem eriala lõpudiplomit taotletud.

Autor S. Adamson…….
(allkiri ja kuupäev)

Töö vastab kehtivatele nõuetele

Juhendaja I. Rokk……
(allkiri ja kuupäev)

Sisukord

Lühendite ja mõistete loetelu 5

Sissejuhatus 12

1. Akadeemia e-postilahenduse hetkeseisu analüüs 14

1.1. Akadeemia serveripargi analüüs 17

2. E-postilahenduse vajaduste analüüs 20

3. Akadeemiale jõukohaste turul saadaolevate e-postilahenduste võrdlevanalüüs 22

4. Realiseeritava e-postilahenduse kontseptsiooni analüüs 25

4.1. Lahenduse tehniline analüüs 27

4.2. E-postilahenduse viiruse kontrolli ja rämpsposti filtreerimise analüüs 29

4.2.1. MailScanneri eelse filtreerimise analüüs 32

4.2.2. MailScanneri poolt teostatava filtreerimise analüüs 33

4.2.3. MailScanneri filtreerimise järgne analüüs 38

4.3. E-lahenduse lõpp e-postiserveri analüüs 39

5. E-postilahenduse teostus 42

5.1. E-postilahenduse mailgateway teostus 43

5.2. E-postilahenduse lõpp e-postiserver teostus 45

6. Hinnang teostusele ning arengukava järgnevaks 5 aastaks 48

6.1. E-postilahenduse komponentidele lisatavad täiendused 49

6.2. E-postilahenduse arengukava järgnevaks 5 aastaks 50

Kokkuvõte 51

Estonian Maritime Academy e-mail services infrastructure upgrade 53

Viiteloetelu 54

Lisad 58

Lisa1 mailgw.testhost.ee konfiguratsioonifailid 58

Lisa2 mail.testhost.ee konfiguratsioonifailid 59

Joonis 1 e-postilahenduse komponentide üldskeem 26

Joonis 2 e-postiserverite teenuste tööpõhimõte 28

Joonis 3 Autori muudatus failis „/usr/bin/update-relay-recipients.sh“ 45

Joonis 4 Maildir postkastide tekitamise skript „/usr/sbin/maildirmake.sh” 47

Lühendite ja mõistete loetelu

Lühendi / mõiste nimetus	Lühendi / mõiste selgitus
<IFrame>; <Form>; <Script> tage	Tagid võimaldavad kirja sisu kujundust ja lisa funktsionaalust.
Active Directory	Microsofti kataloogiteenus, sisaldab domeeni kuuluvate kasutajate ja seadmete (printerid, arvutid, serverid) infot.
alias	E-postiaadress, mis viidatakse teisele tegelikule e-posti aadressile.
baassüsteem	Füüsiline server, mis sisaldab operatsioonisüsteemi ja virtualiseerimise keskkonda.
bash skripte	Linux Unix käsurealiideses kirjutatud programmid.
blacklist	Hajusvõrk serveritest, mis peavad arvestus rämpsposti saatvate IP-aadresside ja MTA-de üle.

ClamAV	Vabavaraline viirusetõrje tarkvara.
domain name system DNS	Teenus, mis peab registrit domeeni nimedele vastavate IP-aadresside kohta.
domeen	Inimsõbralik mingit üksust Eesti Mereakadeemia (emara.ee) iseloomustav nimetus.
Dovecot	Vabavaraline IMAP/POP3 server.
e-postilahendus	Terviksüsteem, mis ettevõttele tagab keskkonna e-posti saatmiseks, vastuvõtuks, talletamiseks.
Exim	Vabavaraline MTA.
F-Secure	Tasuline viirusetõrje tarkvara.
GMail	Google poolt pakutav veebipõhine e-posti lugemise liides.
handshake	Tegevuste jada, mille käigus lepitakse kokku suhtlust alaustava ja suhtlemisele vastava serveri vahel suhtlemisstandard, kiirus. Lisaks tehakse kindlaks mõlema osapoole „oskused“, et valida kõige efektiivsem suhtlemisstandard.

incomming queues	MTA sissetulevate kirjade järjekord.
internet message access protocol IMAP	Tegemist on protokolliga, mille abil MUA laeb MTA-st kirju alla. Antud protokoll laeb sõnumi päise serverist alla, sõnum ise jääb serverisse.
m4 macro	Programm, mis koostab Sendmaili konfiguratsiooni faili.
macro	Microsoft Office programmides kasutatav Visual Basic for Application programm lisafunktsionaalsuse võimaldamiseks.
mail transfer agent (MTA)	Tegemist on e-posti vahendava serveriteenusega.
mail user agent (MUA)	Programmiga, millega lõppkasutaja loeb kirju, laadides need e-posti vahendavast serverist alla.
mail.emara.ee	Mereakadeemia e-postiserveri serverinimi.
mail.merekool.ee	Merekooli e-postiserveri serverinimi.
Mailbox	E-posti postkasti formaat, kus sõnumeid, kirju hoitakse ühe failina (kõik kirjad on samas failis).

Maildir	E-posti postkasti formaat, kus sõnumeid, kirju hoitakse üksik failidena (iga kiri on eraldi fail).
Maildrop	Vabavaraline programm, mis teostab MTA-lt kirjade transpordi Maildir kataloogi.
mailgateway	E-postilahenduse komponent, mis teostab rämpsposti kontrolli, sisu filtreerimist, viirusekontrolli, ning salvestab e-posti liiklust etteantud ajalõikes.
mailgw.emara.ee	Mereakadeemia mailgateway serverinimi.
mailgw.merekool.ee	Merekooli mailgateway serverinimi.
MailScanner v4.68.6	Vabavaraline e-posti sisufilter versioon 4.68.6.
Messaging Application Programming Interface MAPI	Microsofti kinnine protokoll Microsoft Outlooki ja Microsoft Exchange serveri vaheliseks suhtluseks.
Modzilla Thunderbird	Vabavaraline mail user agent MUA.
MX-kirje	Mail exchange (MX) kirje DNS süsteemis, tähistab serverit, kes tegeleb antud domeeni kirjavahetusega.

NTbackup	Microsoft platvormi töövahend varukoopiate tegemiseks.
OpenVPN	Vabavaraline VPN server kasutab udp protokolli.
Outlook Web Access (OWA)	Microsoft Exchange serveri veebipõhine MUA.
outsourcing	Teenuse ettevõttesse sisseostmine.
phishing	Kiri sisaldab linke mitteusaldusväärsetele domeenidele, mis on kirjapildikujult üldlevinud domeenidega sarnased või sisaldab linke otse IP-aadressidele. Antud tegevuse eesmärk on kasutaja pahauskselt suunata võltslehel, mille abil on võimalik kergesukselt lõppkasutajalt isiklikku infot (panga koodid, isikukood) välja petta.
Postfix	IBM poolt välja töötatud vabavaraline MTA.
PostfixAdmin	Vabavaralise Postfix MTA veebipõhine haldamise liides.
postoffice protocol vesioon 3 POP3	Tegemist on protokolliga, mille abil MUA laeb MTA-st kirju alla. Antud protokoll laeb kogu sõnumi serverist alla.

Qmail	Vabavaraline MTA.
RAID5	Andmesalvestus lahendus, kus andmed salvestatakse liias arvutades kontrollsummat. Andmed ja kontroll summa on hargsalvestuse teel ketastele laialipaisatud.
secure socket layer SSL	Turvaline krüpteeritud tunnel, andmetevahetamiseks üle mitteturvalise keskkonna.
sender policy framework SPF	DNS süsteemi kirje, mis sisaldab infot serverite kohta, kes võivad antud domeeni kirju välja saata.
Sendmaili	Vabavaraline MTA.
service level agreement (SLA)	Kokkulepe teenuse kvaliteeti iseloomustavate põhiparameetrite kohta, mis sõlmitakse teenuse pakkuja ja teenuse tarbija (teenuse eest maksja) vahel.
simple mail transfer protokoll SMTP	Tegemist on MTA-lt MTA-le kirjade saatmise protokolliga. Kirjad saadetakse avatekstina. Protokoll pole turvaline.
small computer system interface SCSI	Antud juhul näitab SCSI andmesalvestaja liidese tüüpi.

SquirrelMail	Vabavaraline veebipõhine MUA.
Sysvol	Microsoft Server süsteemi kataloog, mis talletab infot grupi põhiste reeglite, alglaadimisel käivitatavate skriptide kohta
wild kirje	Tähistab suvalist väärtust, mis eelneb @domeen.tld kirjele.
winmail.dat	Microsoft Outlook saadab manuses olevad failid ühe winmail.dat failina.
virtualiseeritud guest süsteem	Loogiline emuleeritud keskkond, millesse on võimalik paigaldada operatsioonisüsteem koos teenustega.
VMware ESXi virtualiseerimise server	VMware poolt pakutav virtualiseerimise keskkond, baassüsteem, mille sisse moodustatakse virtuaalsed teenuste serverid.

Sissejuhatus

Käesoleva lõputöö valikus oli määravaks autori praktika Eesti Mereakadeemias (edaspidi akadeemias). Praktikakäigus sai selgeks Eesti Mereakadeemia hetke IT-alane olukord ja IT poolt pakutavad teenuste hetkeseis. Selgus, et e-postilahendus vajab kaasajastamist, kuna e-posti näol on tegemist akadeemia sisese ja välise infovahetuse seisukohalt kõige olulisema teenusega.

E-postiteenus ostetakse akadeemias hetkel teenusepakkujalt sisse, selline lahendus pole antud asutuse suurust arvestades kuluefektiivne, põhjused on toodud peatükis „Akadeemia e-postilahenduse hetkeseisu analüüs“. Antud lahenduse väljatöötamise teiseks eesmärgiks on muuta e-postiteenus vähem kulukaks ja teenuse sisseostmisele kuluvad vahendeid suunata akadeemia arvutipagi uuendamiseks.

Autori teemavalikut suunas ka isiklik huvi õppida paigaldama kergesti skaleeruvat e-postilahendust, mille igapäevahalduse saab delegeerida tavalisele kontoritöötajale (personaliosakond).

Diplomitöö koosneb 6 peatükist:

1. Akadeemia e-postilahenduse hetkeseisu analüüs käsitleb olemasoleva e-postilahenduse peamisi probleeme. Autor toob välja peamised turvalisuse ja teenusepakkuja usaldusväärsusega seotud probleemid. Lisaks leiavad käsitlust haldamisega seotud probleemid. Peatükis analüüsitakse põhjusi, mis on viinud sellise olukorrani.

2. E-postilahenduse vajaduste analüüsi peatükis, loetletakse loodava e-postilahenduse funktsionaalsuse nõuded, seal hulgas selgitatakse välja vajalikud mahud (minimaalne vajalik kettapind, muutmälu maht) e-postilahenduse jaoks.

3. Akadeemiale jõukohaste turul saadaolevate e-postilahenduste võrdlevas analüüsis, valitakse akadeemiale e-postilahenduse realiseerimiseks finantsiliselt ja funktsionaalsuselt sobiv riistvara ning tarkvara.

4. Realiseeritava e-postilahenduse kontseptsiooni analüüsis tuuakse välja antud e-postilahenduse tugevad ja nõrgad küljed. Peatükis analüüsitakse lahendust töökindluse ja haldusmugavuse seisukohalt. Kirjutatakse lahti e-postilahenduse erikomponentide ülesanded.

5. E-postilahenduse teostus peatükk keskendub tegeliku realisatsiooni probleemide kajastamisele. Peatüki alguses on ära toodud realisatsiooni ettevalmistudega seotud probleemid ja lahendused. Selles peatükis käsitletakse lahenduse erikomponentide paigaldamisel tekkinud probleeme. Peatükis käsitletakse eraldi rämpsposti ja viirusetõrjega tegeleva mailgateway paigaldamist ning eraldi on ära toodud lõpp e-postiserveri seadistamine. Et mailgateway'd mailgw.emara.ee ja mailgw.merekool.ee või lõpp e-postiserverid mail.emara.ee ja mail.merekool.ee on sarnaste seadistustega ja erinevad üksteisest vaid IP-aadressi ning serveri nime poolest, siis kirjelduses tuuakse üldpõhimõtted, kuidas vastav e-postilahenduse komponent on seadistatud.

6. Hinnang teostusele ning arengukava järgnevaks 5 aastaks. Hinnangu peatükis käsitletakse probleeme, mis jäi lahendamata ning analüüsitakse tulemust. Kuidas etteantud eesmärgid on realiseeritud, mis on teostamata ja mida võiks ette võtta antud lahendusega tulevikus. Antud peatüki teine pool käsitleb võimalike e-postilahenduse tuleviku arengusuundi. Käsitlemist leiavad eesmärgid, mida planeeritakse realiseerida tulevikus.

1. Akadeemia e-postilahenduse hetkeseisu analüüs

Eesti Mereakadeemia koosneb IT mõttes 2 suuremast struktuuriüksusest:

1. Merendusalast rakenduslikku kõrgharidust pakkuvast Eesti Mereakadeemiast ja
2. merendusalast keskeriharidust pakkuvast Merekoolist.

Eesti Mereakadeemias on kasutusel 2 domeeni emara.ee ja merekool.ee. Domeen emara.ee on kasutusel akadeemias ja merekool.ee on kasutusel Merekoolis.

Eraldi domeenid on pärit ajast, kui tegemist oli kahe erineva õppeasutusega. Hetkel akadeemia ostab e-postiteenust sisse Elion Ettevõtted AS-ist ja Merekool DataKood OÜ-st. Lisaks on varasemast ajast Merekoolis kasutusel Microsoft 2000 Exchange server.

Merekoolis kasutusel Microsoft 2000 Exchange server teenindab domeeni merekool.edu.ee. Antud domeen pole enam kasutusel – ei reklaamita ametliku e-postina välja, aga teenus töötab ja saabuvad kirjad võetakse vastu.

Autor leiab, hetke olukorra ülevaatest lähtud, et probleemiks on e-postiteenuse sisseostmine mitmelt eripakkujalt. Järgnevat loetletakse teenuse sisseostmise positiivsed ja negatiivsed küljed:

Teenuste sisseostmise – outsourcing'u positiivsed küljed on:

1. On kindlaksmääratud teenuse omadused, võimalused,
2. Teenust saab kindla kuutasu eest,
3. Ettevõtte ei pea omama IT-töötajat,

Teenuste sisseostmise – outsourcing'u negatiivsed küljed on:

1. Sisseostetud teenus pole paindlik, tegemist on karbitootega, mis ei vasta 100% ettevõtte vajadustele.

2. Tehnilise poole pealt ei saa kirju kätte Maildir või Mailbox formaadis failidena Linux lahenduse korral.
3. Ettevõttel puudub täielik ülevaade, kes saavad tema kirjavahetusele ligi ja kes mitte,
4. Teenuse hinnas sisalduvad ka teenusepakkuja üldkulud (kontori ülalpidamise kulud),
5. Tõrgete korral pole ettevõtte IT töötajal võimalik muud teha, kui helistada teenusepakkujale ja sõltuvalt teenustaseme kokkuleppes (service level agreement edaspidi SLA) lubatud ajajooksul on teenuse toimimine häiritud.
6. Tõrge ei pruugi olla teenusepakkuja poolne, tõrge võib olla ka kolmanda osapoolest tingitud, ja kolmanda osapoolega sõlmitud lepingus võivad olla leebemad SLA nõuded (pikem teenuse taasteaeg).
7. Tavaliselt kasutatakse ettevõtte siseselt igapäevatöös serveriteenuseid intensiivselt, seega on mõistlik, kui serverid asuvad kohtvõrku piires. Muidu IT-osakonna pealt kokkuhoitud kulud lähevad kulukate andmeside teenuste katteks.

Autor peab e-postiteenuse sisseostmisel suurimateks riskiteguriteks:

1. Teenusepakkuja usaldusväärsust – ettevõtte sisene e-post (ettevõtte siseinfo) liigub läbi kolmanda osapoole. Antud küsimus kerkib eriti päeva korda, kui on käimas kaupade või teenuste hangete läbirääkimised, e-postiteenust pakkuva ettevõttega ja konkureerivate teenusepakkujatega. Veel küsitavam on teenusepakkuja usaldusväärsus, kui on käimas kohtuvaidlus e-postiteenust pakkuva ettevõtte vastu.
2. Teenusserverid asuvad ettevõttest väljas, sidekulude kasv.
3. Sõltumine kolmandatest osapooltest (võrguteenuse pakkuja).
4. Liigne sõltumine teenusepakkujast.

Lõppkasutajad kasutavad peamiselt Outlooki, Modzilla Thunderbirdi, Outlook Expressi. Lisaks on kasutusel veebipõhised e-posti lugemise keskkonnad RoundCube ja Horde2. Täpne mail user agent'ite (MUA) kasutamise osakaal pole välja selgitatud, sest puudub ka korralik audit IT-inventari kohta.

Puudub adekvaatne ülevaade arvutitesse paigaldatud tarkvarast. Puudub ühtne

kokkulepitud protokoll mail transfer agent (MTA) ja MUA vahel. Hetkel on kasutusel POP3, IMAP või Microsofti MAPI.

Turvalisuse seisukohalt on suureks riskiks akadeemia siseseks kasutuseks mõeldud e-posti lugemine läbi kolmandate teenusepakkujate - asutuse siseseks kasutamiseks mõeldud info lekib akadeemiast välja. Näiteks GMail kasutajad suunavad oma töö e-posti GMaili või seadistavad GMaili IMAP või POP3 abil alla laadima GMaili tööalaseid kirju.

Lisaks MUA ja MTA vaheline liiklus kasutab SMTP protokolli kirjade saatmisel MTA-sse ja POP3 või IMAP protokolli kirjade allalaadimisel MTA-st MUA-sse. Nii SMTP, POP3 kui IMAP saadab sõnumeid avatekstina ja on pealtkuulatavad [1]

Akadeemias ja Merekooli puudub igal tudengil, õpilasel oma e-postiaadress. Eelnimetatud puudus takistab Akadeemias ja Merekoolis teostada kaasaegset suhtlemist tudengite ja õppeasutuse vahel. e-posti puudumise üheks põhjuseks on mahuhalduse puudulikkus. Pole piisavalt kettapinda, et igale kasutajale vähemalt 100 MB e-posti pinda tagada.

Puudub e-posti varundamine, põhjus on selles, et lõppkasutaja kasutab POP3 teenust, mis laeb kõik kirjad MTA-st MUA-sse, samas kasutajate profiilist varukoopiaid ei tehta, seega 100% e-postist pole varundatud. Varundatakse vaid teenusepakkuja juures olevaid kirju.

Hetkel on sisseostetud e-postiteenuse puhul probleemiks ka postkasti maksimaalse mahu piir 120 MB kasutaja kohta, lisaks on probleemiks maksimaalne postkastide arv - 120 hetkel. Antud piirangud on tingitud teenusepakkuja poolsest piirangust antud tootele. Tegemist karbitootega, mis ei vasta Akadeemia tegelikele vajadustele, kus kantselei vahetab 50 ja enam kirja päevas, millest suurem osa tuleb säilitada vähemalt 7 aastat.

Allüksuste kaupa on e-postiteenuse kasutajaid järgnevalt:

1. Eesti Mereakadeemia 50 inimest administratsiooni poolelt, 150 õppejõudu, lisaks 600 tudengid, kes akadeemia e-postiteenust hetkel ei kasuta.
2. Merekoolis 10 inimest administratsioonist ja 15 õppejõudu, lisaks 200 õpilast, kes akadeemia e-postiteenust hetkel ei kasuta.

Järgnevalt on ära toodud põhjused, mis on viinud hetke olukorrani:

1. Akadeemias pole olnud piisavalt pädevat IT töötajat 2-3 aastat.

2. Akadeemiasse IT inventari soetamisest peale on toimunud liigne teenuste, ka IT hooldusteenuse, väljas sisse ostmine.
3. Puudub kulude põhine prognoosimine, planeerimine.
4. Tegeletakse vaid hetkel probleemide lahendamisega, samas pole oluline, et juba probleemide lahendused kokku ka moodustaks mingi terviku – mingi eelnev lahendus oleks eelduseks, või aitaks järgnevaid probleeme vältida, kergemini lahendada.
5. IT osakond on vahepeal üldse õppeasutuse tegevuse vältel ära kaotatud ja siis uuesti moodustatud.
6. Tõsine probleem on ka, nn „telefoni õigus“, kus minnakse rektori jutule ja siis plaani väliselt tehakse suuri prioriteetide muutusi.

Autori hinnangul on kogu akadeemia IT-inventarist ülevaate saamiseks kulub 1 aasta. Alles seejärel on võimalik hakata tegema kulupõhiseid prognoose ja planeerida oste vastavalt arengukavale.

1.1. Akadeemia serveripargi analüüs

Akadeemias on kasutusel 800MHz Pentium 3, Dual Xeon 2,4GHz, Quad Core Xeon. Merekoolis on kasutusel 677MHz Pentium 3. Nimekirjas nähtub, et kasutada on 2 uuemat ja 2 vanemat serverit. Hetkel on probleemiks ka kettapinna maht. Antud serveripargi korral on kettaressurss hajutatud erinevatesse serveritesse, mis ei võimalda efektiivselt moodustada RAID5 tasemel mahukaid kettamassiive.

Seega tuleb koondada hädavajalikud teenused uuele serverile vabastades hetkel kasutusel olevad masinad. Teiseks tuleb ümber paigutada kettad, et sama mahuga kettad oleks samas serveris – viimane võimaldab moodustada suuremaid RAID5 kettamassiive kasutades efektiivsemalt ära üksikuid kettaid.

E-postilahenduse väljatöötamiseks tuleb teha järgnevaid ettevalmistustöid:

1. Quad Core Xeon serverilt tuleb migreerida kasutusel olev emara.ee domeen Dual Xeon serverisse.
2. Quad Core Xeon serverist tuleb migreerida jagatud kaustad Dual Core Xeon serverisse.
3. Paigaldada Quad Core Xeon serverisse VMware ESXi virtualiseerimise server.

4. Paigaldada Quad Core Xeon serverisse 3 Linux serverit ja 2 Microsoft Windows 2003 server.
5. Migreerida emara.ee domeen Dual Xeon serverist ühte kahest Quad Core Xeon serverisse paigaldatud Microsoft Windows 2003 serverisse.
6. Migreerida Akadeemia raamatupidamine (kasutab Sybase ASA andmebaasi ja Microsoft 2000 server operatsioonisüsteemi ning töötab 800MHz Pentum3 serveris) Quad Core Xeon serverisse teise kahest Microsoft Windows 2003 serverist.
7. Eraldi on vaja üle tuua merekool.ee kasutajad merekool.ee domeenist emara.ee domeeni. Seega vabaneks Merekooli server Pentium3 667 MHz.
8. Eraldi tuleb paigutada 5 x 36 GB SCSI kettad Dual Xeon masinasse saades sinna RAID5 massiivina 147 GB kettapinda.
9. Sammuti tuleb koondada 5 x 18 GB SCSI kettad Pentium 3 800MHz serverisse saades sinna 74 GB RAID5 kettapinda.
10. Lisaks tuleb uuendada Pentum3 800MHz server CPU 2 x Pentium 3 1GHz CPU-de vastu.
11. Sammuti tuleb uuendada Pentium 3 667 MHz serveri CPU Pentium 3 800 MHz CPU vastu.

Eelloetud muudatustega on loodud tingimused võtmaks kasutusele uus e-postilahendus. Riistvara poolelt on autor arvestanud, et Quad Core Xeon suudab teenindada kolme e-postilahenduse komponenti viiest. Ja Dual Xeon suudab teenindada 1 komponenti viiest.

Viis e-postilahenduse komponenti on:

1. mailgw.emara.ee – mailgateway teostab kontrolli rämpsposti ja viiruste suhtes, võtab kirju akadeemiasse vastu ja edastab kirju akadeemiast välja. Tegemist on Linux serveriga, mis on virtuaalmasinas.
2. mailgw.merekool.ee - mailgateway teostab kontrolli rämpsposti ja viiruste suhtes, võtab kirju akadeemiasse vastu ja edastab kirju akadeemiast välja. Tegemist on Linux serveriga, mis on virtuaalmasinas.
3. mail.emara.ee – e-postiserver teostab majasisesele kirjavahetusele kontrolli

rämpsposti ja viiruste suhtes, edastab majasiseseid kirju mailgateway'dele ja sisaldab lõppkasutaja postkaste.

4. mail.merekool.ee – e-postiserver teostab majasisesele kirjavahetusele kontrolli rämpsposti ja viiruste suhtes, edastab majasiseseid kirju mailgateway'dele ja sisaldab lõppkasutaja postkaste.
5. Viies komponent on 2 Microsoft Exchange 2000 serverit, mis võetakse kasutusse tulevikus ja antud diplomitöös nende seadistamist ei käsitleta. Antud serverid hakkavad tegelema akadeemia töötajate, õppejõudude e-posti talletamisega.

E-postilahenduse üldskeem (kasutab eelloetletud komponente) on toodud joonisel 1.

Ettemõtlevalt on autor mõelnud ka võimalusele, et mis saab siis kui Quad Core Xeoniga peaks midagi juhtuma. Kuidas asendada e-postilahenduse puuduvad kolm komponenti neljast? Autor on ettenäinud oma lahenduses, et:

1. Kasutatakse ainult 32bitseid virtualiseeritud guest süsteeme, mida on võimalik migreerida vanematele 32bit CPU-ga serveritele.
2. Lisaks on plaanis kirjade kaust „/vmail" paigutada eraldi virtuaalsele kõvakettale. Selline lahendus võimaldab eraldada e-posti ja e-postiserveri süsteemi osa. Süsteemi osa on planeeritud kuni 8GB serverikohta. Nii on võimalik kergesti teha varukoopiaid „/vmail" kaustast ja varu virtuaalsüsteemid, mida põhisüsteemide vea korral minutite jooksul püsti tõsta ei muutu koormavalt mahukateks.

2. E-postilahenduse vajaduste analüüs

Antud analüüsis on võetud arvesse 2009 aasta reaalseid võimalusi soetada piisavalt kettapinda. Lisaks on võetud arvesse e-postikasti mahtude planeerimisel Elioni poolt pakutavaid mahtusid postkasti kohta kuni 500MB [2]. Summaarselt tuleb arvestada 1000 postkastiga, mis vajab kettapinda 500 GB.

Planeeritav e-postilahendus peab tagama kirjade kohalejõudmise mingi lahenduse komponendi vea korral. Lahenduse väljatöötamisel tuleb rakendada vabavaralisi vahendid, et hoida kulud kontrolli all ja mahtuda eelarve raamidesse. Lahendus peab sisaldama rämpsposti filtrit ja viirusetõrje võimalust.

Administratiivtöötajatel ja õppejõududel peab olema võimalus kasutada jagatud kaustu, ühiseid kalendreid. Et akadeemia kontori pool kasutab Outlooki, siis kontoritöötajatel ja õppejõududel peab lõppkasutaja süsteemiks jääma Outlook ja kodust kirjade vaatamiseks Outlook Web Access (OWA). Microsoft Exchange versioonide võrdlusest selgub, et OWA üle SSL tunneli on kindlalt toetatud Microsoft Exchange 2008 versioonist, seega Exchange võetakse antud e-postilahenduses kasutusele tulevikus, kui on selge akadeemia litsentsi poliitika, on täielik ülevaade olemasolevatest litsentsidest ja on konsulteeritud Microsoft Eesti spetslitsidega, kuidas antud olukorras on kõike kuluefektiivsem hankida Exchange 2008 uuendus [3].

Antud diplomitöö ei käsitle Outlooki seadistamist ega Microsoft Exchange serveri seadistamist. Microsoft Exchange server lisatakse e-postisüsteemile tulevikus, sest hetkel puuduvad rahalised vahendid soetamaks tasulist tarkvara. Kui olemasolev Exchange 2000 serveri funktsionaalsus katab ära Akadeemia vajadused lisatakse Microsoft Exchange server ka süsteemi. Kuid Exchange 2000 serveri seadistamist antud diplomitöös ei käsitleta.

Tudengitele ja õpilastele tuleb luua veebipõhise juurdepääsuga e-postilahendus, mis baseerub vabavaralisel lahendusel.

Tuleb luua Akadeemia sisene e-postiloendite süsteem, hetkel on kasutusel 15 erinevat e-postiloendit. Tulevane lahendus peab ühtima olemasoleva süsteemiga. Administratsiooni poolel tuleb lahenda järgnevad probleemid:

1. Hetkel Outlookis, Outlook Expressis või Modzilla Thunderbirdis säilitatud kirjad tuleb üle viia Akadeemia töötajatele mõeldud Microsoft Exchange serverisse. Antud diplomitöökäigus selle probleemiga ei tegeleta, sest puuduvad vahendid soetamaks Exchange 2003 või Exchange 2008 serverit.
2. Tuleb kasutusele võtta üle akadeemia üks kindel MUA programm. Et Akadeemias on soetatud piisavalt Microsoft Office litsentse ja lõppkasutaja on harjunud kasutama Microsoft Office tooteid, siis keskseks MUA programmiks saab Outlook.
3. Tulevane e-postilahendus peab võimaldama kirjade sisu filtreerimist.
4. E-postilahendus peab võimaldama Akadeemiast väljuva ja akadeemiasse sissetuleva kirjavahetuse säilitamist 1 kuu. Peab olema tagantjärgi kindlaks tehtav, kes misssuguse sisuga kirja asutusest välja saatis.
5. Peab olema realiseeritud kirjavahetusest regulaarne varukoopiate tegemise võimalus.
6. Realiseeritava e-postilahenduse igapäevane haldamine peab olema jõukohane personaliosakonna kontoritöötajale.
7. Realiseeritava e-postilahenduse rämpspostifiltrile peab selleks määratud lõppkasutajad ligi pääsema. Lisaks peab kindlaks määratud kasutajatel (näiteks allüksuste juhid ja sekretärid) olema võimalik seadistada nende allüksusega seotud töötajate rämpsposti filtrit vastavalt allüksus vajadustele.
8. E-postilahendus peab olema koormuse kasvades kergesti laiendatav.

3. Akadeemiale jõukohaste turul saadaolevate e-postilahenduste võrdlevanalüüs

Analüüsides vajadusi ja võimalusi on võrdlevas analüüsis käsitletud Microsoft Exchange võimalusi ja vabavaraliste vahendite võimalusi. Vabavaralistest vahenditest on MTA võrdlusesse võetud Postfix. Postfix osutus valituks, sest:

1. autoril on Postfixi seadistamise kogemus, Postfixi seadistamise failid on kergemini mõistetavad [4] [5].
2. Postfix võrreldes Sendmailiga turvalise, modulaarsem, lihtsam seadistada (jääb ära m4 macrodga opereerimine). Teiseks Sendmail ei toeta Maildir postkasti formaati [6].
3. Postfix vs Qmail vs Sendmail vs Exim jõudlus testis on ära toodud, et Postfix suudab edastada 11,5 kirja sekundis, Sendmail 6,6 kirja sekundis. Exim edastab 8,8 kirja sekundis ja Qmail 5,4 kirja sekundis, kusjuures on ära toodud, et Exim ja Qmail on ebaturvalised, sest MTA veakorral lähevad kirjad kaotsi [7].
4. Erinevad vabavara tarkvara tootjad näiteks Ubuntu on oma foorumites üles riputanud õpetused, kuidas Postfixi baasil e-postilahendust püsti panna [8].

Eelnimetatud põhustel valisin vabavaralistest vahenditest MTA-ks Postfixi. Tasulistest vahenditest on Akadeemias ja tema allüksustes kasutusel Microsoft Exchange 2000. Et olemasolevat Exchange süsteemi pole hallatud, 2-3 aastat, siis on antud süsteem tegelikult kasutusest maas. Samas on litsentsid olemas.

Microsoft Exchange 2000 puudub veebiliides ja otse avalikku internetti välja jagada MAPI protokolli pole turvaline. Artiklis [9] on turvalisuse kohapealt Microsoft Windows Serveril baseeruva Exchange lahendusele antud hinnang 3 5 palli süsteemis. Turvalisuse peatükis mainitakse, et Windowsi turvaauke rünnatakse sagedamini, seega on teada ka

Windowsi puhul rohkem turvaauke. UNIX/Linux süsteeme rünnatakse kräkkerite poolt vähem. Antud artikli kohaselt on Windowsil hea tehniline tugi, mis teavitab turvaaukudest lõppkasutajat [9].

Microsoft Exchange integreerub paremini Outlookiga, lõppkasutajal on võimalik kasutada jagatud kaustasid, ühiseid kalendreid. Oluline on integreeritus Microsoft Active Directoriga, viimane vähendab administreerimisele kuluvat aega. Vabavaralise lahenduse korral tuleb eraldi LDAP abil e-postisüsteem integreerida Microsoft AD-ga.

Eesti Mereakadeemia näol on tegemist haridusasutusega, mis võimaldab Microsofti tooteid saada soodustingimustel. Lisaks on lõppkasutajad harjunud kasutama Outlooki, mis ühildub kõige paremini Microsoft Exchange serveriga. Lõppkasutaja e-post oleks Exchange serveris. Ainult serveris paiknevat e-posti on tehniliselt lihtsam varundada. Outlooki lahenduse puhul on oluline ka hea integreeritud teiste Microsoft Office toodetega, mis omakord hõlbustab õppeasutuse igapäeva tööd.

Vabavaralise lahenduse korral on oluline aspekt turvalisusel, vabavaraline e-postilahendus töötab vabavaraliselt kättesaadaval BSD/Linux operatsiooni süsteemil, mille TCP/IP stackile on kirjutatud vähem viiruseid. Paljud troojalased ei tööta BSD/Linux keskkonnas [9].

Autoril on oma praktiline kogemus praktikal olles Mereakadeemias, et isegi kui Linux lahendus on virtualiseertud kujul guest süsteemina baassüsteemiks oleva Microsoft Windows süsteemi eest on rünnakud võimalikud just tänud Windows süsteemi võrguliidese (TCP/IP stacki) vigadele. Seega autor on otsustanud, et Eesti Mereakadeemias tuleb kasutada nii vabavaralist lahendust kui tasulist tarkvara Microsoft Exchange näol. Samas ei saa turvalisuse kaalutlustel Microsoft lahendusi otse avalikku võrku (internetti) ühendada. Lisaks vabavaralistele tulemüüridele peab Microsoft Exchange serverile eelnema vabavaraline Linux server, mis teostab rämpsposti filtreerimist ja viiruste kontrolli.

Et hoida kulusid kontrolli all tuleb tudengite e-postiteenus lahendada vabavaraliste vahenditega. Autor pooldab, et Eesti kõrgkoolides on kasutusel veebipõhise e-post liidesena sarnased süsteemid. Näiteks on Tartu Ülikoolis on kasutusel SquirrelMail [10]. Autoril omab 5 aastast SquirrelMail kogemust, seega tudengite e-posti lugemine veebipõhiselt hakkab toimuma SquirrelMail abil. SquirrelMail omab tõlget rohkem, kui 50 keelde ja SquirrelMail on kasutusel oma hea turvalisuse tõttu ametliku e-posti

kliendina India peaministri büroos [11]

Täiendav rämpsposti filter ja ClamAV viirusetõrje tuleb vabavaralise lahendusena realiseerud e-posti serveritesse.

Töötavale personalile tuleb kasutusse Microsoft Exchange 2000 või 2003, sest viimane võimaldab kasutada Outlookis lisateenustena ühiseid kalendreid, jagatud kaustasid. Microsoft Exchange lahenduse puhul rakendatakse viirusetõrje tarkvarana F-Secure Microsoft serveri ja F-Secure Exchange versioone.

Hetkel vajab veel selgitamist, kuidas viia töötajate Outlookidest, Outlook Expressidest, Modzilla Thunderbird'dest ja teistest MUA-dest Exchange'i ja seega rakendatakse töötajate e-posti süsteemi üleviimist antud projekti järgmistes etappides, mis tõttu antud diplomitöös ei käsitleta põhjalikumalt võimaliku Exchange serveri seadistamist ja lõppkasutajate MUA-de seadistamist.

4. Realiseeritava e-postilahenduse kontseptsiooni analüüs

Kontseptsiooni analüüsi peatükis paneb autor kokku nõuetele vastava lahenduse üldise ülesehituse. Analüüsi käigus toob autor ära põhjuste loetelu, miks nii või teisiti antud lahendus tehtud sai.

Et tagada kerge hallatavus, siis otsustati kasutada e-posti lahendust, mille konfiguratsioon (e-posti aadressid, e-posti aliased, domeenid) on paigutatud andmebaasi. Vastavast andmebaasist küsib Postfix vajaliku info. Haldamine toimub PostfixAdmin abil veebiliidese kaudu.

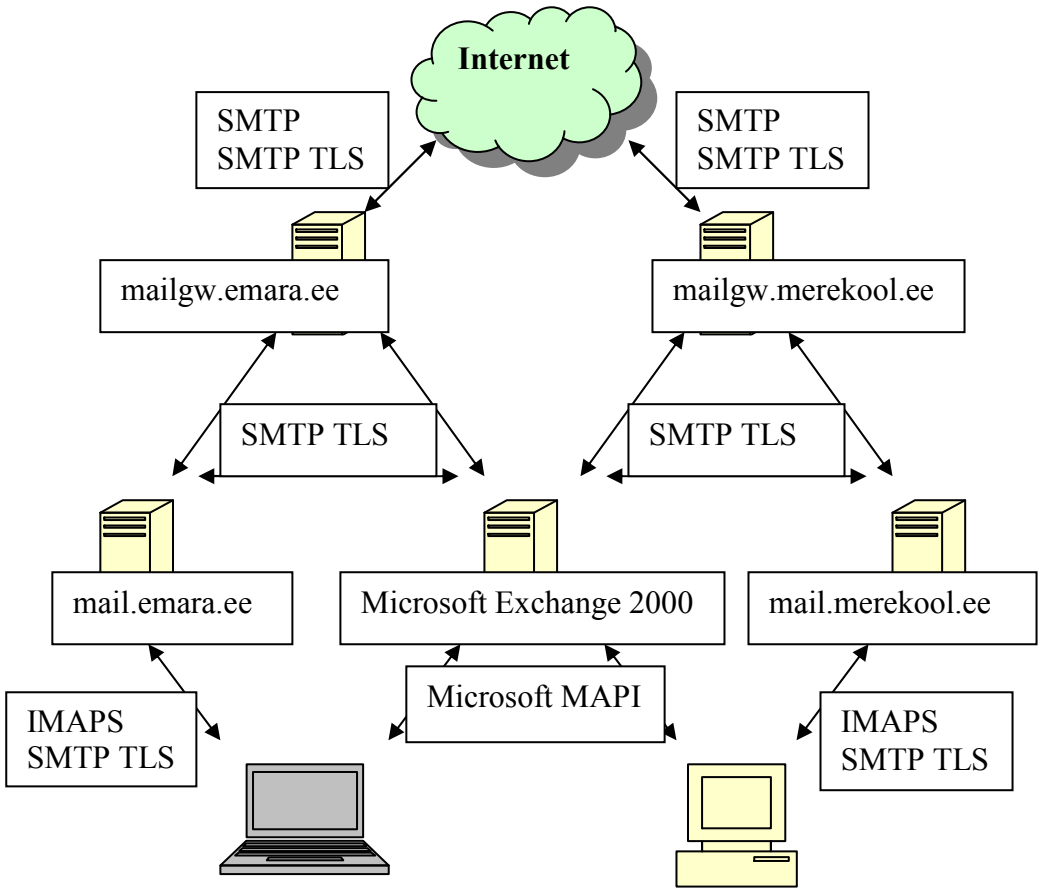
Teiseks, et tagada veakindlus mingi komponendi vea korral, siis kontseptsioon näeb ette domeenisüsteemi (DNS) tasemel varu e-postiserveri (MX-kirjete) olemasolu.

Seega kontseptsiooni kohaselt oleks vähemalt 2 mailgateway'd. Et on 2 domeeni, siis üks mailgateway tegeleks merekool.ee kirjadega, aga samas oleks ka Akadeemia domeeni emara.ee kirjadele tagavara serveriks, juhuks kui Akadeemia mailgateway on kätte saamatu. Sarnane lahendus aga vastupidi on kasutusel emara.ee domeeni jaoks.

Kontseptsiooni kohaselt mailgateways toimub rämpsposti filtreerimine ja esmane kontroll viiruste suhtes. Mailgatewayid nimedega mailgw.emara.ee ja mailgw.merekool.ee.

Sellise lähenemine võimaldab kergesti eraldada e-postiliikluse majasiseseks e-postiliikluseks ja asutuste vaheliseks e-postiliikluseks. Lisaks võimaldab selline lahendus erinevale liiklusele rakendada erinevaid poliitikaid. Näiteks saab täpselt reguleerida, milline kasutaja võib majast üldse kirju välja saata, samas säilib antud kasutajal võimalus saata E-kirju maja siseselt.

Kontseptsiooni illustratiivne joonis on toodud järgnevalt.



Joonis 1 e-postilahenduse komponentide üldskeem

SMTP tähistab kommunikatsiooni ilma SSL tunnelita ja SMTP TLS tähistab kommunikatsiooni ainult SSL tunneliga. Lõppkasutajad kasutavad ainult IMAPS protokolli, tegemist on turvalise IMAP protokolliga, mis kasutab SSL tunnelit.

Eraldi toob autor välja võimaluse kehtestada erinevaid rämpsposti filtreerimise reegleid akadeemiasse saabuvale ja väljuvale liiklusele võrreldes akadeemia sisese e-postiliiklusega. Samamoodi võib piirata ka sisufiltreerimist erinevalt ja lubada asutuse sisese e-posti puhul suuremaid kirju saata. Lubada saata macrosid sisaldavaid Microsoft Office dokumente asutuse siseselt, samas keelata vastavate dokumentide saatmine asutusest välja või asutusse sisse.

Mailgatewayid on seadistatud saatma kirju vastavalt adressaadile erinevatele sisemistele e-postiserveritele. Sisemisteks e-postiserveriteks on esialgu plaanitud merekooli.ee domeenile eraldi server ja emara.ee domeenile eraldi server.

Praktika käigus selgus, et vormiliselt liidetud Merekool ja Eesti Mereakadeemia

soovivad sisuliselt eksisteerida erineva asutusena (Merekool põhjendab seda sellega, et nemad on keskeriõppeasutus ja liigse integratsiooni korral kaotaks Merekool oma näo ja jääks konkurentsis õpilasele kaotajaks pooleks).

Vastu tulles Merekooli soovidele näebki antud lahenduse kontseptsioon 2 erinevat e-postiserverit eraldi Merekoolil ja Mereakadeemial oma serverit. Tehnilise poole pealt räägib antud lahenduse kasuks ka koormuse jaotumine. Lisaks on tulevikus võimalik kergelt lahutada 2 süsteemi, kui vastavad allüksused peaks eraldi organisatsioonidena jätkama.

Lisaks hallataks erinevat e-postiserverite seadistus eraldi vastava allüksuse töötaja poolt.

4.1. Lahenduse tehniline analüüs

Antud lahenduse kõik komponendid kasutavad virtualiseeritud baassüsteeme. Autor leiab, et selline lahendus tagab teenuse komponentide kiire taastatavuse.

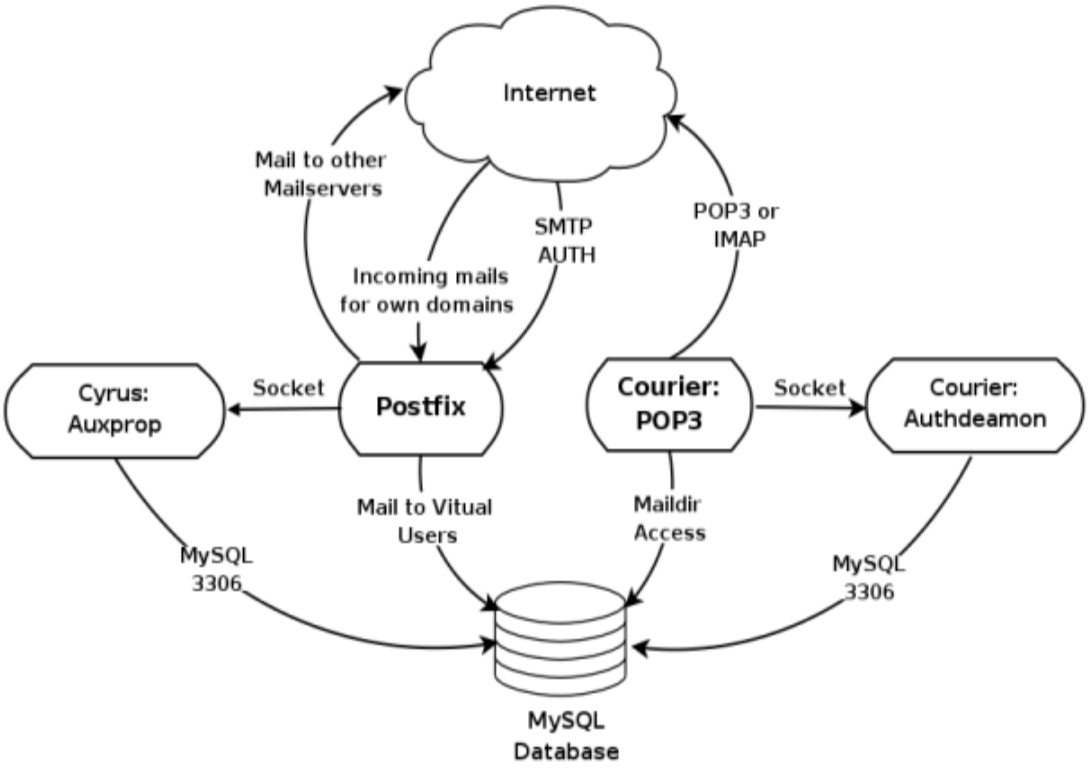
Teiseks tagab virtualiseerimine sõltumatuse konkreetsest baassüsteemi riistvarast.

Mereakadeemia puhul tuleb kindlasti arvestada finantsiliste piirangutega. Hetkel pole eelarves vahendeid 3-4 uue serveri ostmiseks, seega autori soov on paigutada hetkel 3 komponenti uuemasse Quad Core Xeon serverisse ja 1 komponendi Dual Xeon serverisse. Eraldi serveritesse on plaanis paigutada e-postiserverid.

Hetkel on Quad Core Xeon serverisse võimalik paigutada nii 64 kui 32 biti operatsioonisüsteem, kuid Dual Xeon on 32 bitine. Seega e-postilahenduse komponentide operatsioonisüsteemid tulevad hallatavuse huvides 32 bitised. Miinimum mälunõuetega 512 MB mälu virtualiseeritud serveri kohta.

Kettapinna nõuded sõltuvad kasutajate hulgast. Virtuaalsesse serverisse tehakse eraldi süsteemi ketas ja eraldi e-posti infot talletav ketas. Virtuaalserveri kettanõuded on 8 GB virtualiseeritud süsteemi kohta. e-posti talletava kettapinna nõuded sõltuvad mahust näiteks 100 e-posti mahuga 500 MB teeb mahuks 50 GB kettapinda e-posti talletamiseks.

Järgneval joonisel on toodud e-postiserverite tööpõhimõtte skeem. Antud skeem iseloomustab mail.emara.ee ja mail.merekool.ee serverite ülesehitust.



Joonis 2 e-postiserverite teenuste tööpõhimõte [12]

Postfix Mail Transfer Agent (MTA) võtab kirju vastu SMTP protokoll abil ja edastab kirjad sissetulnud kirjade järjekorda. Maildrop võtab kirjas sissetulnud kirjade ootejärjekorrast ja edastab kirjad vastavalt MySQL tabelis olevale infole õigesse virtuaalsesse Maildir formaadis postkasti. Maildrop teeb päringu MySQL baasi saamaks teada, mis kausta kiri edastada.

MySQL andmebaasiserver talletab infot e-posti domeeni, kasutajate, aliaste, e-posti aadresside ja edastamise reeglite kohta. MySQL baasis teeb muutusi ka PostfixAdmin veebiliides. Antud lahendus võimaldab nii teha muutusi Postfixi seadistuses omamata juurdepääsu serveri käsureale.

Courier on eraldi seisev MTA sarnaselt Postfixile antud e-postilahenduses on Courier kasutusel POP3/IMAP serverina ning Courieri ülesanne on tagada POP3 või IMAP klientidel juurdepääs e-postile, mis talletatakse Maildir tüüpi postkastides.

SASL on Cyrus library, mis tegeleb teistest võrkudest (võrgud, mis pole usaldusväärsete võrkude nimekirjafailis mynetworks) kasutajate autentimisega, lisab autentimise SMTP sõnumile.

E-postilahenduses kasutatakse asutuse sisevõrgus MUA-sid, mis kasutavad IMAPS

protokolli kirjade MTA-st allalaadimisel ja SMTP TLS protokolli kirjade MTA-sse saatmisel. Kirju saab välja saata vaid mailgw.emara.ee või mailgw.merekool.ee. Teiste serverite jaoks pannakse tulemüürist väljuv 25 port, SMTP teenuse port, kinni. Lisaks seadistatakse e-postiserverid saatma kõik väljuvad kirjad edasi mailgatewaydele (mailgw.emara.ee või mailgw.merekool.ee).

Iga e-postiserver ja mailgateway omab iseseisvat DNS serverit. Selline lahendus tagab DNS teenuse kätte saadavuse teiste komponentide mitte kätte saadavuse korral. Lisaks tagab eelnimetatud lahendus ka paindlikkuse ja DNS teenuse koormuse jaotumise mitme serveri vahel. Miinuseks on administreerimise mahu kasv.

Teiseks oluliseks põhjuseks on vajadus eraldada välised DNS süsteemid (asuvad mailgw.emara.ee ja mailgw.merekool.ee) akadeemia sisevõrgu DNS süsteemidest.

4.2. E-postilahenduse viiruse kontrolli ja rämpsposti filtreerimise analüüs

Rämpsposti filtreerimisel ja viiruste kontrollil on kogu süsteem viidud kaheastmeliseks. Kirja saabumisel mailgatewaysse toimub esmane ja põhjalikum kontroll. Teise astme moodustab e-postiserveri sisene kontroll viiruste ja rämpsposti suhtes.

Mailgatewaydes kasutatakse Ubuntu 8.04 LTS (long time support) Linux distributsiooni.

Ubuntu 8.04 TLS osutus valituks sest:

1. omab progressiivset repositooriumit,
2. omab head paketihaldust, paljud programmid on eelkompileeritud ja ei vaja täiendavat kompileerimist lähtetekstist,
3. oluliseks põhjuseks on korralike õpetuste olemasolu HowtoForge õpetuste keskkonnas. E-postilahenduse mailgatewayde seadistamisel kasutasin The Perfect SpamSnake - Ubuntu 8.04 LTS õpetust [13].

E-postilahenduse mailgaewayle on paigaldatud järgmised programmid:

1. Veebiserver Apache 2.2 koos PHP 5.2.4 ja Ruby toega,
2. Andmebaasiserver on MySQL 5.0,
3. MTA on Postfix,

4. DNS teenus töötab BIND9 abil,
5. PHP on toetatud PHP5 abil,
6. E-posti sisufiltriks on MailScanner v4.68.6
7. MailWatch v1.0.4 abil on teostatud MailScanneri kasutajasõbralik veebipõhine seadistamine,
8. ClamAV – vabavaraline viirusetõrje programm,
9. Spamassassin – vabavaraline rämpsposti filter,
10. Pyzor – Spammassassin lisa moodul, mis, kasutab rämpsposti tõrjumisel hajusvõrksüsteemi ja kontrollib sõnumi tunnussõna [14],
11. Razor – Spammassassin lisa moodul, mis, kasutab rämpsposti tõrjumisel hajusvõrksüsteemi ja kontrollib kirja vastu Razor Kataloogi, mida uuendatakse vastavatest kataloogiserveritest [15],
12. DCC-Client – hajus rämpsposti vastane süsteem, mis kontrollib sõnumite kontrollsummat ja jagab infot masspostitajate kohta [16].
13. SPF Checks – moodul, mis teostab kontrolli, vastu SPF kirjet DNS süsteemis, kus on kirjeldatud millised serverid võivad antud domeeni kirju välja saata [17],
14. FuzzyOcr – Spammassassin lisa moodul, mis, otsib gif, jpeg, png piltidelt kindlaks määratud sõnu. Antud moodul kasutab sama tarkvara, mis on kasutusel dokumentide skaneerimisel tekstiks. Antud moodul võimaldab ära tunda piltidena saadetud rämpsposti [18],
15. PDF/XLS/Phishing Sanesecurity Signatures – ClamAV lisamoodul, mis võimaldab leida rämpsposti kirja manuses olevatest xls, pfd ja zip failidest [19],
16. Postfix-GLD (Greylisting) – moodul, mis teatab uuelt tundmatult domeenilt kirju saades, et saada uuesti olen hõivatud, nii tehes saab lahti pea 90% rämpskirjadest, sest rämpspostisaatja ei saada kirja uuesti erinevalt korralikust MTAst, kes jätab kirja ootele ja saadab kirja uuesti sihtpunkti teatud aja näiteks 1 tund möödumisel. Antud tehnoloogia tekitab viiteid kirjade saabumises, kuid on uudne ja tõhus meetod rämpsposti peatamiseks [20],
17. Logwatch Statistical Reporting – moodul, mis koostab süsteemi logidest raporti ja saada selle kindlaks määratud e-postiaadressile. Kasulik moodul süsteemi

komponentide tööst ülevaate saamiseks [21],

18. Outgoing Disclaimer with alterMIME – moodul mille abil saab automaatselt lisada hoiatus teateid väljuvatele kirjadele. Näites: „Antud kiri sisaldab konfidentsiaalset infot ja kui kiri juhuslikult on läinud valele adressaadile, siis on kirjasaajat hoiatatud konfidentsiaalse materjali avalikustamisega kaasnevatest tagajärgedest“ [22],
19. Bayesian Filtering, Anti-Backscatter (Relay Recipients) lisa moodul teostab, mis filtreerib välja non-delivery reports (DNR) ja delivery status notifications (DSN) sõnumid [23].

Mailgateway'sse paigaldatud programmide loetelule järgneb loetelu peamistest põhjustest, miks sai just selline valik tehtud:

1. Autor omab varasemat MailScanneri seadistamise kogemust.
2. Lisaks omab MailScanner korraliku veebiliidest MailWachi näol.
3. Lahenduse üks oluline nõue on viia rohkem administreerimist lõppkasutaja kätte. MailScanneri veebipõhine liides MailWatch võimaldab kindlaksmääratud kasutajatel (allüksuste juhid, allüksuste sekretärid jne) juurdepääsu rämpsufiltrile.
4. Lisaks võimaldab veebiliides igal kasutajal keskfilter seadistada omakäejärgi just nii nagu vaja. Oluline on ka lõppkasutaja võimalus vabastada filtrisse jäänud kirjad iseseisvalt.
5. ClamAV sai valitud, sest vabavaraline viirusetõrje aitab tulevikus vähendada jooksvaid kulutusi litsentsidele.
6. ClamAV täiendab oma viiruste andmebaasi kiiremini, kui tasulised tarkvarad [24].
7. Lisaks on autoril 5 aastane ClamAV haldamise kogemus.
8. Spamassassin rämpsposti filtrina on MailScanneri poolt hästitoetatud.
9. Tarkvara valikus oli oluline ka seadistamise mugavuses, nii Postfix, ClamAV, MailScanner, MySQL omavad arusaadavat seadistuse failide süntaksit ja korralikult on kommenteeritud konfiguratsiooni failide sisu.
10. Pyzor, Razor, DCC-Client, SPF Checks, FuzzyOcr, PDF/XLS/Phishing Sanesecurity Signatures, Postfix-GLD (Greylisting) ja Bayesian Filtering, Anti-Backscatter (Relay Recipients) on paigaldatud, et tõhustada rämpsposti filtri

Spamassassin ja ClamAV viirusetõrje tööd.

11. MySQL on vajalik MailWatchi seadistuste talletamiseks.
12. MySQL baasi kasutab ka FuzzyOcr moodul, mis skaneerib pildid vektorgraafikas andmebaasi ja pildi teistkordsel kontrollil pole vaja enam teostada täiendavas skaneerimist. FuzzyOcr tunneb ära ka sama pildid veidi moonutatud kujul. Rämpsposti saatjate levinud tegevus on saata sarnast pilti [25].

4.2.1. MailScanneri eelse filtreerimise analüüs

Kirjade edastamisega tegeleb Postfix, mis kontrollib kohe saatja domeeni olemasolu, saatja serveri nime olemasolu ja vastavust DNS süsteemis olevale serveri nimele, ning teostab päringu blacklist serveritele, et kas antud IP pole mustas nimekirjas. Selline eelkontroll aitab vähendada kirjade hulka, mida järgmises etapis MailScanner kontrollima peaks hakkama, sammuti vähendab mustanimekirja kohene kontroll võimalust, et sissetulevatele kirjadele ettenähtud maht incomming queues saab ülekoormatud.

Lisaks kontrollitakse saaja aadressi olemasolu kohalike kasutajate nimekirjas. Pole mõistlik kasutada nn wild kirjet @domeen.tld, sest siis edastatakse ja kontrollitaks kõik kirjad mis tulevad domeeniga domeen.tld. Selline lahendus koormab mailgatewayle järgnevat e-postiserverit.

Postfix kontrollib 2 faili:

1. esimene on vastu võetavate domeenide loetelu failis „/etc/postfix/relay_domains“, mille sisu on domeen.tld OK tähistab, et kui saaja aadressil on märgitud domeeniks vastav domeen tagastatakse vastus OK (Postfix aktsepteerib antud domeenile saabuvaid kirju),
2. teine kontroll on vastu faili „/etc/postfix/relay_recipients“ kus paikneb nimekiri kõigi saaja e-postiaadresside kohta. Antud faili oleks mõistlik defineerida kindlad lõppkasutajate e-postiaadressid (antud konfiguratsiooni faili formaat näeb ette seadistamist kujul „kasutaja@domeen.tld OK“, kuis soovitakse kõik antud domeeniga seotud kirjad edasi suunata, siis võib kasutada wild kujul „@domeen.tld OK“ (viimane pole soovitav)), muidu koormatakse e-postiserveri (paikneb mailgateway taga) kirjadega olematule adressaadile.

Autori järeldus on, et mida rangem ja täpsemalt on seadistatud mailgatway, seda

tulemuslikum on mailgateway rämpsposti ja viiruste tõrjumine ja seda vähem koormatum on e-postiserver.

Antud domeenilt esmakordse kirja saamisel antakse teada Postfix-GLD GrayListing mooduli poolt, et saada kiri uuesti.

Lisaks kontrollib Postfix, et kiri koos manusega poleks suurem, kui 10 MB. Pole mõtet saata suuremaid kirju edasi, sest ClamAV kustutaks sellised kirjad ära. ClamAV on seadistatud selliselt toimima, sest serveri mälu ressurss on piiratud.

Üks e-postiserveri rünnaku moodus on saata „pommkirju“, mille manuses on suuremahuline fail, mille kontrollimine võtab liigselt mälu ressurssi ja selliste kirjade laviin muudab serveri kätte saamatuks ülekoormuse või mälu täitumise tõttu.

Kirjad, mis on pärit mailgateway serverist ei läbi mailgateway rämpspostifiltrit ega viirusetõrjet vaid edastatakse kohe lõpp e-postiserverisse. Sellisteks kirjadeks on näiteks e-posti teel saadetavad raportid, mis koostatud Logwatch Statistical Reporting teenuse poolt MailScanneri ja/või teiste mailgateways töötavate teenuste kohta.

Postfix kontrollib enne kirja vastu võtmist kirja vastavust SMTP nõuetele:

1. Kas SMTP „handshake“ on nõuete kohane,
2. Kas e-posti saatja server teatas oma mine,
3. Kas kirjas on olemas MAIL FROM:,
4. Kas kirjas on olemas RCPT TO:,
5. Kas kirja SMTP DATA osa, mis sisaldab manust on nõuete kohane (pole näiteks 0 bait mahuga).

Postfix teostab PERL postfix-policyd-spf-perl mooduli abil SPF kontrolli, et kas kirja saatnud server võib saata antud domeenilt kirju välja.

Postfix edastab kirjad „/var/spool/postfix/hold“, mille sisu MailScanner kontrollib.

4.2.2. MailScanneri poolt teostatava filtreerimise analüüs

MailScanner kontrollib 6 korda sekundis „/var/spool/postfix/hold“ kausta sisu. Skaleeruvuse kohapealt on oluline, et MailScanner oskab ära kasutada mitme CPU tuge, on võimalik reguleerida samaaegselt töötavate MailScanneri protsesside arvu CPU kohta.

MailScanner teostab kirjade kontrolli „/etc/MailScanner/rules/scan.messages.rules“

failis olevate reeglite suhtes. Antud failis on nimekiri mitte korrektsetest domeeninimedest ja ignoreeritavatest domeeninimedest. Lisaks kontrollitakse et kirjal poleks üle 200 faili manuses.

MailScanner asendab winmail.dat faili manuses olevate failide loeteluga, selline asendus võimaldab teistel MUA-del vaadata Outlookga saadetud manuseid.

Maksimaalne manuse suurus on 10MB kirja kohta, sest suuremad manused vajavad kontrolliks rohkem mälu ja on koormavad serverile.

Lisaks kokkupakitud manuseis pakitakse lahti 2 tasandit, selline piirang väldib tüüpilist rännakut e-postiserveritele, kus saadetakse 10 kuni 100 korda kokkupakitud mahukate manustega kirju. Kui lahtipakkimisel kokkupakitud faili mahu ja arhiivi rekursiivselt sissemineku piirangut pole pakitakse kontrolliks manus lahti kuni mälu on täis, seejärel täitub saale ala ja lõpuks e-postiserver mäluressursi lõppemisel hangub.

MailScanner kasutab viiruste kontrolliks etteantud viirusekontrollitarkvara abi, antud lahenduse puhul on viirusetõrje programmiks ClamAV.

ClamAV antiviirus on seadistatud antud lahenduses mitte teavitama saatjat, et tema kiri sisaldas viirust, selline lähenemine on mõistlik, viirust sisaldava kirja saatja aadress võib olla võltsitud. Igale kirjale teadet saates, eriti veel, kui tegemist on vale aadressiga on MTA-l oht sattuda mustanimekirja (blacklisti).

ClamAV teostab kirja sisu kontrolli vastu „content.scanning.rules“ failis olevaid reegleid. Tõhustamaks rämpsposti filtri tööd on lisatud curl moodul, mis võimaldab otsida rämpsposti ka kirjadega kaasa pandu .pdf ja .xls failides isegi, kui failid on peidetud kokkupakitult .zip (kokkupakitud) faili. Antud moodul kasutab selleks ClamAV abi, viimane kasutab pakitud failide lahtipakkimiseks mailgateway’sse paigaldatud pakkijate abi. Antud mailgateway’sse on paigaldatud järgnevad pakkimise programmid: unzip, zip, bzip2, unzoo, arj, unarj, lzop, arc, zoo.

Antud mailgateway puhul on ära keelatud poolikud manused, sest puudub võimalus kontrollida erikirjade manuseid samaaegselt ja seega on võimalus et viirus pääseb läbi osadekaupa, kui poolikud manused on lubatud.

MailScanner on seadistatud kontrollima kirja sisus ja päises paiknevate domeenide tegeliku olemasolu, et avastada võimalikke „phishing“ skeeme, mis seisneb kirjade saatmises kirjapildilt sarnaselt domeenilt. Kontrolli teostatakse „phishing.safe.sites.conf“

failis olevate reeglite alusel.

MailScanner kontrollib kirja teise ja kolmanda taseme domeenide vastavust domeeninimekirjaga. Kontroll teostatakse „country.domains.conf“ olevate reeglite alusel.

Lisaks on MailScanner seadistatud modifitseerima (muudab mitte töötavaks) Outlooki turvaaukusid ärakasutavaid <IFrame> tage.

Ka <Form> tagid modifitseeritakse (muudetakse mitte töötavaks), sest antud tagide abil saadetud vormidega püütakse tavaliselt lõppkasutajalt teada saada tema krediitkaardi numbreid.

Turvalisuse kaalutlusel modifitseeritakse (muudetakse mitte töötavaks) <Script> tagid, mis tavaliselt sisaldavad programmi lõike häirimaks veebimootori või MUA tööd.

MailScanner on seadistatud modifitseerima (muudab mitte töötavaks) <Img> tagid, millega saadetakse väga väikesed pildid E-kirjaga kaasa (on kasutusel kui „web bugs“, mida kasutatakse saamaks teada, kas kirja on loetud). Antud MailScanner konfiguratsioonis on lubatud järgnevaid „web bug“ faili nimed „spacer pixel.gif pixel.png gap“. Antud „web bugid“ on kasutusel lehe kujunduse õigeks näitamiseks. Kui web bug leitakse küsitakse aadressilt „http://www.sng.ecs.soton.ac.uk/mailscanner/images/1x1spacer.gif“, kuidas on õige antud web bugi korrektselt modifitseerida (dokumendi originaal kujundus, ei tohi muutuda).

MailScanner on seadistatud modifitseerima (muudab mitte töötavaks) ka <Object Codebase=...> or <Object Data=...> tage kirjadest. Antud tagid kasutavad ära Microsofti turvaauke.

Lisaks turvalisuse huvides on MailScanner seadistatud modifitseerima ohtlikud tage sisaldavad HTML kirjad lihtteksti kujul kirjadeks. Antud seadistuse negatiivseks pooleks on kirjades graafilise komponendi kaotamine.

Manuses olevad failid kontrollitakse „filename.rules“ failis olevate reeglite järgi.

MailScanner on seadistatud mitte talletama:

1. nakatunud sõnumeid, selline seadistus aitab karantiini hoida viirustest puhtana,
2. modifitseeritud kirju ega „peidetud“ viirusi sisaldavaid sõnumeid.

MailScanner on seadistatud:

1. kogusõnumi talletama (nii päis, kui sisu), et oleks võimalik teada saada kirjavahetus 1 kuu lõikes.
2. Hoidma viirustest puhtana Spami ja Message Content Protection (MCP) arhiivi.

MailScanner on seadistatud modifitseerima kirjade päist:

1. lisab MailScannerit kasutava asutuse (serveri omanik) nime,
2. lisab SPAMi korral rea päisesse, et kiri loetakse SPAMiks,
3. lisab arvutatud SPAMi skoori,
4. toob eraldi päises välja SPAMi saatja aadressi,

MailScanner edastab kõik viiruste vabad (puhtad kirjad) ja kahjutuks tehtud kirjad (disinfected). Kirjad, mis sisaldavad viirust ja mida ei suudetud kahjutuks teha on määratud kustutamisele turvalisus kaalutlustel.

MailScanner on seadistatud mitte teavitama kirjasaatjat kui:

1. on avastatud kirjas viirus,
2. on avastatud mittekorrektne failinimi või keelatud failitüüp,
3. on avastatud keelatud manus, või kirja sisus on keelatud sõnu, tage või muud ohtlikku, mida tuli modifitseerida.

Igasugune saatja teavitamine on keelatud esitaks et mailgateway või e-postiserver ei satuks mustanimekirja (saates rämpsposti saatjate olematutele aadressidele sadu kirju vastuseks päevas) ja teiseks on mõistlik mitte jagada infot, millist sisu antud filter keelab või kas üldse filter eksisteerib.

MailScanner on seadistatud modifitseerima kirjade subject (pealkirja) rida järgnevalt:

1. Normaalsetele teadetele ei lisata midagi pealkirja,
2. Viirust sisaldavatele kirjadele lisatakse {Virus?} pealkirja algusesse. Antud MailScanner selliseid kirju edasi ei saada, seega lõppkasutaja selliseid kirju ei näe,
3. Kui on muudetud, kirja manuses faile, siis pealkirja alguses {Filename?},
4. Kui kiri sisaldab ohtlikku sisu tagide, vormide näol ja seda tuli kahjutusk teha on pealkirja algusesse lisatud hoiatus {Dangerous Content?}
5. Kui kirjaga on kaasas liiga suur manus, mis MailScanner ära keelas, on pealkirja

algusesse lisatud {Size} hoiatus.

6. Ohtlikud HTML tage sisaldavate kirjade modifitseerimisel lisatakse teade {Disarmed},
7. Kui avastatakse kirja sisust võimalikku phishingut, siis hoiatatakse kasutajat lisades pealkirja algusesse teate {Fraud?},
8. Rämpsposti lahterdatakse kaheks on SPAM ja High SPAM. Antud MailScanner teisendab vastavalt kirja pealkirja {Spam?} või {High Spam?}. MailScanner on seadistatud salvestama karantiini ja mitte edastama High SPAM staatusega kirju. SPAM staatusega kirjad säilitatakse karantiinis ja edastatakse.

MailScanner on seadistatud arhiveerima 1 kuu e-postiliikluse „/var/spool/MailScanner/archive“ kataloogi. Antud lahenduses teavitatakse administraatorit viirusega nakatunud kirja avastamisel. SPAMi ja viirusetõrje programmide kohta käivat infot hoiab MailScanner failides vastavat siis „spam.lists.conf“ ja „virus.scanners.conf“. MailScanner on sedaistatud kuulama järgmisi DNS blocklists servereid:

1. spamhaus-ZEN – ZEN on DNS blacklist serverite kombineeritud võrk [26],
2. spamcop.net – SpamCop on hajussüsteem, mis teavitab teenusepakkujaid rämpspostist [27],
3. SBL+XBL – The Spamhaus Block List (SBL) on reaalaja andmebaas rämpsposti edastavate serverite IP aadressidest [28] ja Exploits Block List (XBL) on reaalaja andmebaas troojalast, usside ja viiruste poolt nakatatud lõppkasutaja arvutite IP aadressidest [29].

Antud e-postilahenduses kasutatakse SPAMi avastamiseks Spamassassint ja tema lisa mooduleid Pyzori hajusandmebaasi, Razor hajusandmebaasi ning DDC-client hajusandmebaasi. Spam skoor on vaikimisi märgitud 6 ja High Spami skoor on märgitud 10. Antud väärtuste puhul on tegemist subjektiivsete väärtustega ja täpne häälestus on iga ettevõtte spetsiifiline ning seadistatakse ajajooksul vastavalt ettevõtte spetsiifikale.

Autor leiab, et mida täpsemalt on paika määratud antud väärtused, seda tõhusam on rämpspostifiltri töö.

Antud seadistuses on musta ja valge nimekirja seadistused muudetud dünaamiliseks ja neid on võimalik muuta MailScanneri veebiliidese MailWatchi abil. Musta ja valge

nimekirja sisu hoitakse MySQL baasis.

Lisaks kasutatakse antud mailgateway'des Bayesian andmebaasi (Bayesian rämpsposti filtreerimine baseerub statistilisel analüüsil, et kui suur on tõenäosus saada mingilt IP-aadressilt või domeenilt rämpsposti. Arvesse võetakse eelnevalt samalt IP-aadressilt või domeenilt tulnud rämpsposti osakaal) [30]. Saadud tulemusi hoitakse antud lahenduses MySQL baasis, mis kiirendab kirjade skaneerimist.

Mailgateway'des kasutatakse FuzzyORC moodulit, mis võimaldab otsida etteantud sõnu, fraase (paiknevad failis „/etc/mail/spamassassin/FuzzyOcr.words") kirjaga saabuvatelt piltidelt. Antud lahenduses hoitakse pildi skaneerimisel tekkiv paisktabel MySQL baasis. Selline lähenemine võimaldab pildi faili sisu võrrelda MySQL baasis oleva paisktabeliga. Nii saab vahele jätta sama pildi teistkordsel kontrollil ressursimahuka pildi skaneerimise.

Edastatavad kirjad saadab MailScanner kausta „/var/spool/postfix/incoming".

4.2.3. MailScanneri filtreerimise järgne analüüs

Postfix on seadistatud kirju edastama, mitte lokaalselt talletama, seega on

Postfix main.cf konfiguratsiooni failis on kirjeldatud:

1. veateade „local_transport = error:No local mail delivery", juhuks kui keegi soovib edastad kirju kohalikku arvutisse,
2. "mydestination = " Postfix teab siis et antud server pole kirjadele lõppserver,
3. "local_recipient_maps = " on jäätud tühjaks, Postfix teab siis, et serveris kohalikke postkaste pole.

Antud Postfix server tegeleb vaid e-posti skaneerimisega rämpsposti ja viiruste suhtes ning edastamisega. Kuidas kirju edastada on kirjeldatud failis „/etc/postfix/transport". Antud faili formaat näeb ette kuju domeen.tld protokoll, milles kirju edastatakse ja sihtpunkt server (kas IP-aadress või serveri täis pikk domeeni nimi FQDN). Seega antus näiteks siis domeen.tld smtp:[IP.AD.DR.ESS] või domeen.tld smtp:[hostname.domeen.tld], kui on vaja saata smtp protokolliga kirjad muul pordil kui 25, siis on standardi järgi kirjapilt domeen.tld smtp:[IP.AD.DR.ESS]:pordi number [31]

Seega Postfixi seisukohast on mailgateway's sissetulevate kirjade järjekord (Inbound Mail Queue ja väljuvate kirjade järjekord Outbound Mail Queue).

Kogu MailScanner haldamine on viidud veebipõhiseks läbi MailWatchi. MailWatch talletab konfiguratsiooni MySQL baasi ja MailScanneri konfiguratsiooni failis „/etc/MailScanner/MailScanner.conf“ failis on viidatud konfiguratsiooni failide asemel kataloogi „/etc/MailScanner/CustomFunctions/“. Antud kataloogis paiknevad PERL skriptid, mis koostavad MySQL baasi poole päringu ja kostavad baasi vastuse põhjal MailScannerile vajalik konfiguratsioonifaili.

4.3. E-lahenduse lõpp e-postiserveri analüüs

Mailgatewayle järgnev e-postiserver on paigaldatud CentOS 5.3 distributsioonile. Autor on kasutanud paigaldusjuhendina „Virtual Users With Postfix, PostfixAdmin, Courier, Mailscanner, ClamAV On CentOS” [32] juhendit.

Kasutatakse virtuaalseid postkaste. MTA-na on kasutusel Postfix. Viirusetõrjega tegeleb ClamAV, Sisufiltreerimisega tegeleb MailScanner ja rämpsposti filtreerimisega tegeleb Spamassassin. Kirjade liikumine põhijoontes ja MailScanneri seadistus on sama, mis mailgateways.

E-posti serveripuhul on tegemist lõpp serveriga, mis talletab kirjad. Vastav Postfixi konfiguratsioon on talletatud MySQL baasis. Postfix pöördub MySQL baasi järgnevate päringutega:

1. relay_domains = mysql:/etc/postfix/mysql_relay_domains_maps.cf. Fail „mysql_relay_domains_maps.cf“ sisaldab päringut, millega küsitakse MySQL baasist nimekiri domeenikohta, mille kirju aktsepteeritakse edastamiseks, [31]
2. relayhost = mailgw.testhost.ee määrab ära, et antud server edastab kõik väljuvad kirjad kindlale mailgatewayle.
3. virtual_alias_maps = mysql:/etc/postfix/mysql_virtual_alias_maps.cf fail „mysql_virtual_alias_maps.cf “ sisaldab päringut, millega küsitakse MySQL baasist nimekiri e-posti aadressi aliastest, mille kirju aktsepteeritakse ja edastatakse kindlale lõppkasutajale, mis saadakse teada läbi kasutusel olevate postkastide nimekirja, mis saadakse järgneva päringuga, [31]
4. virtual_mailbox_maps = mysql:/etc/postfix/mysql_virtual_mailbox_maps.cf [31]
5. Kasutusel olevate domeenide kohta annab infot päring virtual_mailbox_domains = mysql:/etc/postfix/mysql_virtual_domains_maps.cf faili „mysql_virtual_domains_maps.cf“. Vastuseks on kindel domeenile vastav

kataloog [31].

6. Järgmisena on vajalik teada saada kindel lõppkasutaja Maildir formaadis kataloog. Otsitav kataloog on eelnevalt kindlaks tehtud domeeni tähistava kataloogi alamkataloog. Selleks tehakse pärin virtual_mailbox_maps = mysql:/etc/postfix/mysql_virtual_mailbox_maps.cf faili „mysql_virtual_mailbox_maps.cf“. Antud fail sisaldab päringut MySQL baasi, mis annab seose lõppkasutaja e-posti ja lõppkasutaja Maildir/ formaadis kausta vahel [33].

Järgnevalt on lahti kirjutatud teiste parameetrite tähendused /etc/postfix/main.cf failis. E-postisüsteem hoiab kasutajate infot virtuaalselt MySQL baasis ja reaalseid e-kirju Maildir formaadis kettal. Järgnev parameeter virtual_mailbox_base = /srv/vmail kirjeldab ära, mis kaustas asuvad postkastid on. Parameeter virtual_uid_maps = static:1001 määrab ära postkastide süsteemse kasutaja ID ja parameeter virtual_gid_maps = static:1001, määrab ära süsteemse kasutaja kasutajagrupi ID [34].

Lisaks parameetriga virtual_mailbox_limit = 51200000 määratakse virtuaalse postkasti maksimaalne maht [34].

Parameeter virtual_minimum_uid = 1001 määrab, et väiksema ID-ga kui 1001 ei saa olla süsteemis kasutajaid, kes omaks virtuaalset postkasti [34].

Antud lahenduses saab hallata e-postiserverit (MTA Postfix)läbi PostfixAdmin veebiliidese. PostfixAdmin veebiliides teeb muutusi MySQL baasis ja Postfix küsib MySQL baasist konfiguratsiooni.

Postfix konfiguratsiooni failis main.cf parameeter virtual_transport = maildrop määrab, et Maildir tüüpi (formaadis) postkastidest reaalsete sõnumite edastamisega tegeleb Maildrop. Maildrop töötab vmail kasutaja õigustes ja edastab tegelikult MTA-lt (Postfix) saadud kirja õigesse Maildir formaadis postkasti [35].

E-postiserver MTA Postfix on sarnaselt mailgateway MTAle (Postfix) seadistatud rakendama saaja piiranguid smtpd_recipient_restrictions järgnevalt:

1. permit_mynetworks – lubatakse usaldusväärsest võrgust (ettevõtte lokaalvõrk) vastu võtta kirju[36],
2. permit_sasl_authenticated – lubatakse kirju vastu võtta, kui teine osapoolt on autenuditud Simple Authentication and Security Layer (SASL) for SMTP abil

[37].

3. reject_non_fqdn_hostname – keeldub vastu võtmast kirju, kui saatja täis pikk domeeni nimi (FQDN) pole RFC nõuetega kooskõlas [36]
4. reject_non_fqdn_sender - keeldub vastu võtmast kirju, kui kliendi MAIL FROM käsk pole (FQDN) nõuetele vastav [36].
5. reject_non_fqdn_recipient - keeldub vastu võtmast kirju, kui kliendi RCPT TO käsk pole (FQDN) nõuetele vastav [36].
6. reject_unauth_destination - keeldub vastu võtmast kirju, kui sihtpunkt ei ühti antud serveri (sihtpunkt serveri) domeenidega, mis on kirjeldatud $mydestination, $inet_interfaces, $virtual_alias_domains, or $virtual_mailbox_domains või ei ühti $relay_domains antud dommenide alamdomeenidega [36].
7. reject_unauth_pipelining – keeldub kirju vastu võtmast, kui saatja püüab kasutada SMTP protokolli laiendust PIPELINING veendumate kas saaja MTA toetab PIPELINING laiendust. PIPELINING võimaldab saata terve grupi SMTP protokolli sõnumeid ja ei vaja iga sõnumi järel TCP kinnitust – selline meetod kiirendab sõnumite edastamist [38].
8. reject_invalid_hostname - keeldub kirju vastu võtmast, kui saatja HELO ja EHLO käsk sisaldab RFC nõuetele mitte vastavat serveri nime.

Postfix on asustuse sisesel suhtlemisel seadistatud kasutama SMTP protokolli koos TLS tunneliga. TLS tunnel tekitatakse kahe MTA vahel, et vahetada turvaliselt kirju. SMTP protokoll on olemusel ebaturvaline ja saadab kirju avatekstina.

Lõppkasutaja kasutab SquirrelMail veebipõhist MUA-d, mis suhtleb virtuaalsete postkastidega IMAP teenust kasutades. Courier-IMAP koos Courier autentimise teenusega tagab kasutajal juurdepääsu kirjadele. Courier autentimise teenus kontrollib kasutajanime ja parooli vastavust MySQL baasis oleva kasutajanime ja parooliga. Juurdepääsu korral (autentimine õnnestus) valib Courier-IMAP MySQL baasist saadud info põhjal õige Maildir kausta ja vahendab kaustas olevad kirjad SquirrelMaili veebiliidesele.

Analüüsipeatükk on käsitlenud seadistamise teoreetilist külge. Järgmine peatükis tuleb juttu e-postilahenduse praktilisest realisatsioonist, mille käigus ei räägita enam üle teoreetiline baas, miks nii või teisiti midagi seadistatud sai.

5. E-postilahenduse teostus

Teostuse peatükis käsitletakse kõigepealt realisatsioonile eelnenud ettevalmistustöid. Peatüki „Akadeemia e-postilahenduse hetkeseisu analüüs“ alapeatükis „Akadeemia serveripargi analüüs“ on toodud loetelu töödest, mis on eelduseks antud e-postilahenduse realisatsioonile. Nendest töödest on teostatud:

1. emara.ee domeeni migreerimine Quad Core Xeon serverist Dual Xeon serverisse,
2. jagatud kaustade migratsioon Quad Core Xeon serverist Dual Xeon serverisse,

Antud migratsioon ei kulgenud tõrgeteta, domeeni migratsioon oli poolik Active Directory (AD) sisu migreerus. Samas Sysvol sisu koos startup skriptide sisuga ei migreerunud. Lahenduse leidmisel pöördusime Microsoft Suppordi poole saades Microsoft Eesti esinduse juhilt Rain Laanelt „Quick assistance“ pileti. Järgnes kirjavahetus ja telefoniteel probleemi selgitamine nii eesti, kui inglise keeles. Lahenduseks oli Windows registri tasemel parameeri muutus – migratsioon käivitati uuesti. Igaks juhuks sai migratsiooni ajaks eemaldatud serverid muust võrgust ja tulemüürid sai ja viirusetõrjed sai väljalülitatud. Teistkordselt migratsioon õnnestus. Siin kohal tänud Microsoft support meeskonnale ja Microsoft Eesti esindusele.

Domeeni migratsiooni järgselt oli vaja üleviija ka jagatud kaustad. Tallinna Tehnika Ülikooli majandusteaduskonna IT-spetsialist Kalev Jõgi soovitas xcopiga öösel kopeerida jagatud kaustad üle ka kõik õigused oleks pidanud ülekäima käsitsi. Selline teostus tundus autorile, liiga töömahuks, seega autor uuris Microsot Pressi väljaantud raamatut „Windows Server 2008 Inside Out“ [39], selgus, et alates Windows Server 2003 versioonist on toetatud Distribute File System (DFS) jagatud kaustade süsteem, mis seisneb selles, et 2 ja enamas serveris on jagatud kaust, mida jagatakse sama nime alt välja, lisaks on ettenähtud Microsoft lahenduses ka kausta sisu automaatne sünkroniseerimine. Seega sai jagatud kaustad lahendatud DFS lahenduse abil. Ühe

ööpäeva jooksul sünkroniseeriti jagatud kaustade sisud. Oluline on siinjuures mainida, et teenused polnud kordagi maas. Kogu migratsioon toimus reaalajas. Lisaks toodi ka üle kõik õigused.

Väga oluliseks peab autor antud lahenduse korral ka veakindlust, sest DFS jagatud kaustad ja mitu AD domeeni kontrollerit tagavad tõrgeteta töö ka lahenduse ühe komponendi (serveri) hävimise korral. Tavakasutaja ei saa midagi aru nii kaua, kui kasvõi üks AD kontroller ja üks DFS süsteemil baseerub failiserver töötab.

Hetkel pole VMware ESXi baasil lahendust virtualiseeritud, sest viibis emara.ee domeeni migratsioon. Seetõttu autor pani püsti pilootprojektina kaks serveri. Antud serverid baseerusid tavalistel tööjaamaks mõeldud riistvaral. Parameerid on toodud järgnevalt:

1. mailgateway test arvurti CPU Pentium 4 1,8 GHz, mälu 1024 MB DDR333 MHz, kõvaketast 40 GB,
2. lõpp e-postiserver testarvuti CPU Pentium 4 1,6 GHz, mälu 1024 MB DDR333 MHz, kõvaketas 20 GB.

Baas operatsiooni süsteemina jäi eelpaigaldatud Windows XP Professional. Tagantjärgi leiab autor, et kiiruse ja turvalisus huvides oleks pidanud baassüsteemina paigaldama Linux lahenduse.

Linux operatsioonisüsteemid paigaldati virtualiseeritult. Virtualiseerimiseks kasutati VMware Server 1.0.8 versiooni. Virtualiseeritud serveritele eraldati 8 GB kettapinda, 512 MB mälu. Mailgateway operatsiooni süsteemiks valiti Ubuntu 8.04 LTS (long time support), sest mailgateway seadistamise õpetus oli baseerus antud Ubuntu distributsioonil [11]. E-postiserveri operatsioonisüsteemiks valiti CentOS 5.3 versioon, autoril on kogemus, et SquirrelMail veebipõhine e-posti lugemise liides on korralikult eestikeelselt töötav CentOS distributsioonide korral.

5.1. E-postilahenduse mailgateway teostus

Antud e-postilahenduse mailgateway teostusel järgiti The Perfect SpamSnake - Ubuntu 8.04 LTS [11] õpetust. Järgnevalt on ära toodud antud õpetuse järgi paigaldades õpetuses olnud vead ja autoripoolsed lahendused.

Ubuntu 8.04 LTS distributsioon baseerub Debian Linuxil. Baas konfiguratsioonis paigaldati vaid OpenSSH server. Lisaks süsteemi ketas 8 GB jagati 3 primaarseks jaoks:

1. /boot – maht 47 MB, vormindati ext3 failisüsteemi. „/boot“ kettajaol hoitakse süsteemi käivitamiseks vajalikke faile.
2. swap – maht 510 MB, vormindati Linux swap failisüsteemi. Saale ala näol on tegemist operatiivmälu laiendusega kõvakettal.
3. lvm – maht 7,48 GB, vormindati Linux LVM pinnaks
4. / - maht 7,41 GB, vormindati ext3 failisüsteemi. „/“ kettajaol hoitakse süsteemi faile. / kettajagu kasutab kasutajate ja kasutaja gruppide põhist kettakasutuse limiidi arvestust – Quotas.

Võrk seadistatid paigalduse käigus järgnevalt:

1. IP 192.168.5.21,
2. mask 24 biti,
3. võrgulüüs 192.168.5.254,
4. nimeserver 192.168.5.254
5. serveri nimeks pandi mailgw.testhost.ee (tegemist on pilootprojektiga).

Juhendijärgi tehes tekkis Bind9 DNS server seadistamisel probleem, et Bind9 ei toiminud korralikult antud õpetuses toodud chroot lahenduses. Lahenduseks oli, et Bind9 ei seadistatud chroot'na ja muudatust faili „/etc/default/bind9“ sisse ei viidud. Tulemus Bind9 töötab, konfiguratsiooni failid „named.conf“, „named.conf.options“, „named.conf.local“ koos DNS zone'i failidega asuvad kataloogis „/etc/bind“.

Järgmine õpetuse järgne tõrge oli, et wget http://debian.intergenia.de/debian/pool/main/m/mailscanner/mailscanner_4.68.8-1_all.deb, pakett mailscanner_4.68.8-1_all.deb polnud kättesaadav. Põhjus antud lehel on juba uuem MailScanneri versioon 4.68.8-1 asemel on 4.74.16-1 versioon [40]. Lahenduseks paigalduse hetkel oli Ubuntu 8.04 LTS distributsiooni repositooriumitest saadava MailScanneri paigaldus, milleks oli MailScanner versioon 4.58.9. Antud versioon ei oma näiteks Watermark funktsionaalsust – MailScanneri poolt kontrollitud kirjadele lisatakse vesimärk, millealusel sama ettevõtte (sama salasõna sisaldav) MailScanner antud sõnumit uuesti ei kontrolli, nii hoiab serveri ressurssi kokku ja kirjade liikumisel on väiksem viide. Seega on plaanis MailScanner versioon 4.58.9 asendada versiooniga 4.74.16.

MailScanneri konfiguratsiooni failis „MailScanner.conf“ tehti DNSBL kontrolli parameetris täiendus „Spam List = spamcop.net SBL+XBL“ asemel kirjutati „Spam List = spamhaus-ZEN spamcop.net SBL+XBL“. Mida antud sõnad tähendavad on toodud punktis 4.2.2 MailScanneri poolt teostatava filtreerimise analüüsi peatükis.

Õpetuse The Perfect SpamSnake - Ubuntu 8.04 LTS leheküljel 5 punktis 9.25 [41], tuli koodi lisamisel etteantud kood korralikult treppida, et oleks arusaadavam, kust konstruktor lõpeb ja kus algab järgmine.

Õpetuse The Perfect SpamSnake - Ubuntu 8.04 LTS leheküljel 6 punktis 12.4 [42] tehti failis „/usr/bin/update-relay-recipients.sh“ järgmine muutus:

```
#!/bin/sh
#/usr/bin/getadsmtp.pl
postmap /etc/postfix/relay_recipients
```

Joonis 3 Autori muudatus failis „/usr/bin/update-relay-recipients.sh“

Joonis kolmelt on näha, et Perl skripti käivitamine on väljakommenteeritud. Põhjus selles, et AD-ga kokkutöötamine vajab veel kontrolli. Seega hetkel tuleb käsitsi teha muutused failis „/etc/postfix/relay_recipients“.

5.2. E-postilahenduse lõpp e-postiserver teostus

Antud e-postilahenduse e-postiserveri teostusel järgiti „Virtual Users With Postfix, PostfixAdmin, Courier, Mailscanner, ClamAV On CentOS“ [43] õpetust. Autor kasutas Linux operatsioonisüsteemiks CentOS 5.3 distributsiooni [44]. Järgnevalt on ära toodud antud õpetuse järgi paigaldades õpetuses olnud vead ja autoripoolsed lahendused.

CentOS 5.3 distributsioon baseerub Red Hat Enterprise Linux 5 lähtekoodil [45]. Baas konfiguratsioonis paigaldati vaid OpenSSH, server. Lisaks süsteemi ketas 8 GB jagati 3 primaarseks jaoks:

5. /boot – maht 47 MB, vormindati ext3 failisüsteemi. „/boot“ kettajaol hoitakse süsteemi käivitamiseks vajalikke faile.

6. swap – maht 510 MB, vormindati Linux swap failisüsteemi. Saale ala näol on tegemist operatiivmälu laiendusega kõvakettal.

7. lvm – maht 7,48 GB, vormindati Linux LVM pinnaks

8. / - maht 7,41 GB, vormindati ext3 failisüsteemi. „/“ kettajaol hoitakse süsteemi faile. / kettajagu kasutab kasutajate ja kasutaja gruppide põhist kettakasutuse limiidi arvestust – Quotas.

Võrk seadistatid paigalduse käigus järgnevalt:

6. IP 192.168.5.11,
7. mask 24 biti,
8. võrgu lüüs 192.168.5.254,
9. nimeserver 192.168.5.254
10. serveri nimeks pandi mail.testhost.ee (tegemist on pilootprojektiga).

Juhendijärgi tehes jäeti vahele courier-authlib, courier-authlib-devel, courier-authlib-mysql, courier-imap ja maildrop rpm pakkide kompileerimine lähtekoodist, sest õpetuses „Virtual Users And Domains With Postfix, Courier And MySQL (CentOS 5.1)“ [46], on vastavate eelkompileeritud rpm pakkide allalaadimise võimalus juba äratoodud.

PostfixAdmin paigutati „/usr/share/postfixadmin“ kasuta ja Apache seadistus kataloogi „/etc/httpd/conf.d/“ lisati fail postfixadmin.conf, mis suunab http://host/postfixadmin päringud kataloogi „/usr/share/postfixadmin“.

Lisaks kasutati SquirrelMaili seadistamisel õpetust „Virtual Users And Domains With Postfix, Courier, MySQL And SquirrelMail (CentOS 5.3 x86_64) - Page 5” [47].

E-postilahendus töötab saates kirja välja mail.adamson.cc serverist jõuab kiri mailgw.testhost.ee serverisse ja sealt edasi mail.testhost.ee serverisse. E-postiserverist mail.testhost.ee saab kirja lugeda SquirrelMaili abil. Postfixi saab veebipõhiselt seadistada PostfixAdmin abil. Samas antud lahenduses tuleb Maildir postkastid tekitada käsitsi, sest vastav skript „/usr/sbin/maildirmake.sh”, ei käivitu Apache kasutaja õigustes.

```
#!/bin/bash
set -e
mail_home="/srv/vmail"
if [ ! -d $mail_home/$1 ] ; then
        mkdir $mail_home/$1
        chown -R vmail:vmail $mail_home/$1
        chmod -R 700 $mail_home/$1
        #echo "$mail_home/$1 CREATED"
fi
if [ -d $mail_home/$1 ] ; then
        cd "$mail_home/$1"
        maildirmake $2
        #echo "$mail_home/$1/$2 CREATED"
        maildirmake -q "$3S" $2
        #echo "$3S $2 QUOTA CREATED"
        chown -R vmail:vmail $mail_home/$1/$2
        chmod -R 700 $mail_home/$1/$2
fi
```

Joonis 4 Maildir postkastide tekitamise skript „/usr/sbin/maildirmake.sh" [48]

Analüüsis toodud reaalse lahenduse korral kasutatakse mailgateway'de puhul serverinimesid mailgw.emara.ee ja mailgw.merekool.ee. Et süsteemid on virtualiseeritud jäävad seadistused samaks väljaarvatud serverinimi, IP-aadress ja MailScanneri seadistust sisaldab MySQL baas. Erinevused tulevad siis domeeni ja kasutajate definitsioonides. Lisaks on erinevused ka Postfix konfiguratsiooni failides, mis käsitlevad e-posti transporti filtreerimise järgselt (@emara.ee suunatakae mail.emara.ee serverisse ja @merekool.ee suunatakse mail.merekool.ee serverisse).

E-postiserverid on ka virtualiseeritud, seega mail.emara.ee ja mail.merekool.ee hakkavad mõlemad baseeruma CentoOS 5.3 Linuxil ja sarnaselt mailgateway'dega muutuvad IP-aadressid ja serverinimed, ning MySQL baasis on erinevalt defineeritud Postfixi seadistuses e-postiaadressid ja domeenid.

6. Hinnang teostusele ning arengukava järgnevaks 5 aastaks

Antud peatükis annab autor hinnangu teostusele ja loetleb tööd, mida tulevikus võiks teha, et e-postilahendust muuta mugavamaks haldamise seisukohast, ning töökindlamaks käideldavuse seisukohast.

Antud e-postilahenduse välja töötamine oli huvitav, arendav. Näiteks ettevalmistus eeldas Microsoft Windows Server 2003 AD tööpõhimõtte selgeks tegemist. Antud probleemi lahendamine oli oluline praktiliste oskuste täiendus, mida autor läbides IT kolledži õppeaine „Windows 2003 serveri administreerimine“ ei saanud.

Pilootprojekti eemalt haldamiseks tuli endale selgeks teha VPN lahendus. Baseerub OpenVPN lahendusel ja kasutab udp protokolli. Põhjus selles, et TCP protokolli kapseldada veelkord TCP protokolli tekitaks liigse SYN, ACT pakettide vahetuse, mis on koormav.

Kindlasti tuleb ära mainida, et antud uurimus arendas autorit ka Linux serveite administreerimise vallas. Autori ja juhendaja vaheline koostöö seisnes vormistuse alastes konsultatsioonides. Ja juhendaja vaatas töö kriitilise pilguga üle, et kuis on vaja veel põhjendada ja milliste punktide kalla võidakse komisjonis lisaküsimusi esitada. Antud töö teema on autor ise välja mõelnud ja ka realiseerinud iseseisvalt. Autoril oli varem kogemus e-postilahendustega, kus autentimisega tegeles Dovecot, postkastid on mailbox formaadis ja kasutajad on süsteemsed Linux kasutajad. Seega autor peab oluliseks, et lõputöö ei korranud varasemaid teadmisi, vaid selle käigus sai autor laiendada silmaringi valdkonnas, mida ta polnud varem realiseerud.

Antud töötulemus on reaalselt toimiv e-postilahendus, mis on arhitektuuriliselt kergesti skaleeruv (rämpspostifilter on eraldi, vajadusel võib nende arvu suurendada tehes DNS kirjetes vajalikud täiendused), eraldi on e-postiserverid eridomeenidel, mis võimaldab koormuse jaotamist. Mailgateway’sid on kaks seega ühe mailgateway

mittetöötamisel lähevad kirjad teise mailgateway kaudu (selline liias arhitektuur tõstab töökindlust ja võimaldab katkestusteta hooldustöid).

6.1. E-postilahenduse komponentidele lisatavad täiendused

Antud e-postilahendusele tuleks kindlasti lisada monitooring, seda ei käsitletud antud lahenduse analüüsis. Autoril on tulevikus plaanis teha monitooring kasutada Nagios seiretarkvara.

Teine oluline komponent on varundamine, millepuhul antud juhul kasutatakse Linux keskkonnas bash skripte (tar töövahendi) ja üle samba teenuse varundatakse e-posti NTbackup töövahenditega Microsoft Windows keskkonda või teine võimalus on varundada Linux keskkonda kasutades vaid bash skripte ja scp võiimalusi.

Kolmandaks tuleb integreerida e-postilahendus Microsoft Windows AD-ga, et muudatused AD kajastuksid automaatselt Postfix konfiguratsioonis, mida hoitakse nii Postfix konfiguratsiooni failides „/etc/postfix“ kataloogis (alias, transport, relay_recepients, releay_domains, virtual), kui MySQL andmebaasis.

Eraldi tuleb välja tuua ka Microsoft Exchange lahenduse kasutuselevõtt. Microsoft Exchange 2000 serverit sain antud töös mainitud, aga selle seadistamist ja analüüsi antud töös ei käsitletud ajapuudusel. Antud lisa funktsionaalsuse kasutuselevõtt on järgmiseks esmaseks tööks pärast e-postilahenduse paigaldamist ja juurutamist sellisel kujul, nagu ta on antud töös ära toodud.

Autor peab oluliseks ka saadud vigade otsimise kogemust. Töökäigus tuli peale iga suuremat muutust uurida logi faile ja veenduda, et erinevad rakendused tõesti teevad seda, mida vaja. Nii Windows kui Linuks serverite haldamisel on kõige vajalikum osata otsida probleemidele lahendust logifailidest. Paljas erinevate variantide proovimine ei too loodetud tulemust.

Lisaks teadmised Linux serveri seadistamisest aitavad oluliselt kaasa Microsoft Windows serverite seadistamisel, sest Linux lahendustes on asjad vähem „munapraadijasse“ peidetud ja tuleb rohkem tutvuda erinevate RFC dokumentidega.

6.2. E-postilahenduse arengukava järgnevaks 5 aastaks

Antud alapeatükis on punktide kaupa ära toodud autori arvates olulised punktid antud e-postilahenduse arengus järgneva 5 aasta jooksul.

1. Tulevikus tuleb MySQL andmebaasi teenus viia eraldi serverisse nii mailgateway'de puhul kui lõpp e-postiserverite korral. Võimaliku lahendusena toob autor ära lahenduse, kus mailgatewayde arv kasvad 2-lt 4-ni, sama mahu muutus toimub ka e-postiserveritega, seega 6 serveri peale on mõistlik panna kahest noodist koosnev MySQL klasterserver.
2. Kindlasti tuleb tulevikus viia Maildir formaadis postkastid võrgus paiknevale kettamassiivile (storage'le).
3. Lisaks tuleb monitooring teostada vähemalt 2 iseseisva monitooringu süsteemi abil.

Samas autor möönab rahastamise võimalustele viidates, et eelnev on ideaalplaan. Reaalplaan on et, kui saab vähemalt teise kaasaegse serveri juurde on see arvestades antud ettevõtte profiili oluline muutus, millega kaasneb võimalus muuta e-postiteenuse käideldavuse taset.

Kokkuvõte

Käesolev diplomitöö on kirjutatud soovist lahendada Eesti Mereakadeemia e-postiteenusega seotud probleemid. Teema kerkis päevakorda praktikakäigus, kus selgus, et asustuse sisese ja asutuse välise informatsiooniliikumise seisukohalt kõigeolulisem teenus ostetakse sisse.

Lisaks oli autoril endal ka huvi õppida korralikult seadistama e-postilahendust, mis paikneb enam, kui ühes serveris.

On olemas nii tasulisi, kui vabavaralisi vahendid saavutamaks etteseatud eesmärki. Mõistlik on kasutada vabavaralisi lahendusi seal, kui nad oma töö ära teevad (pole vajalikud spetsiifilised lisafunktsioonid).

Internetis on kättesaadav tervehulk asjalikke materjale, kui autor leiab, et pelgalt „copy paste“ stiilis ikka korralikku lahendust püsti ei pane. Töökäigus tekib tõrkeid, mille lahendamine eeldab, et saadakse aru:

1. kogulahenduse tegelikust tööpõhimõttest (kuidas komponentide vahel andmevahetus toimib,
2. saadakse ka aru iga komponendi ülesannetest ja tööpõhimõttest.
3. Linux serverite seadistamine eeldab rohkem asjasisust arusaamist ja RFC dokumentidega tutvumist, kui Microsoft Windows serverite puhul.

Postfix on väga paindlik MTA, millele on paljurohkem võimalusi, kui IT kolledži õppeaines „Infrastruktuuri teenused“ või „Linux serveri administreerimine“ käsitleda jõuti.

Töö tulemus on töötav kaasaegne e-postilahendus. Ära on realiseeritud analüüsi käigus toodus nõuded funktsionaalsusele järgnevalt:

1. Ühele kindlale MUA-le, Outlookile, üleminekuga on alustatud.

2. Sisufiltreerimine on teostatud MailScanneri abil, nii asutuste vahelisel tasemel mailgateway'des, kui asutuse siseselt e-postiserverites.
3. E-postiliikluse mahasalvestamine on teostatud MailScanneri abil, nii asutuste vahelisel tasemel mailgateway'des, kui asutuse siseselt e-postiserverites.
4. Varundamine on teostatud Unix/Linux skriptide abil.
5. E-postiteenuse lihtne haldamine on realiseeritud PostfixAdmin veebiliideseabil.
6. Rämpspostifiltri lihtne haldamine on realiseeritud MailWatch veebiliidese abil.
7. E-postiteenuse kerget laiendatavust tagab lahenduse hierarhiline arhitektuur, mis võimaldab vajadusel alamkomponentide hulka suurendada.

On koostatud arengukava e-postilahendusele järgnevaks 5 aastaks.

Töö käigus jäi lahedamata Maildir postkastide automaatne tekitamine ja kustutamine. Vastavad skriptid on olemas, lahendamist vajab veel meetod, kuidas veebipõhiselt antud skriptid käivitada saab. Lahenduse on seotud ka turvalisuse küsimustega, sest veebiliidese kaudu on juurdepääs süsteemile avatud ka kräkkeritele ja seega lubades Apache'il käivitada käsurea skripte on selge turvaaugu tekitamine.

Antud töö käigus tekkis ka mõtteid, mida võiks tulevikus teha. Järgmisena on äratoodud mõned punktid:

1. E-postilahendusele on vaja teha seire,
2. Oluline on teha e-postilahendusele keskse haldusega varundus,
3. Andmebaasi server on vaja viia eraldi füüsilisse serverisse,
4. Microsoft Exchange serveri on vaja integreerida antud lahendusse,
5. Tuleb automatiseerida Microsoft AD tehtavad muutused kajastuks Postfix konfiguratsioonifailides ja kasutatavates MySQL andmebaasides.

Estonian Maritime Academy e-mail services infrastructure upgrade

Siim Adamson

Summary

This diploma thesis describes the e-mail system for Estonian Maritime Academy. To have good e-mail system ones need good analysis of requirements. Outsourcing was not a viable option for the Estonian Maritime Academy. Using open software is reasonable to met cost effectiveness.

Good e-mail system includes SPAM and virus detection ability. Also it is wise to delegate everyday administrative work to ordinary end-user. To build e-mail system with good redundancy and scalability the system should consist of two levels. Each level consist at least two components. First level is for SPAM and virus detection and second level storage e-mails. Such hierarchical structure makes the whole system well scalable. In each level all functionality has to by mirrored to give good redundancy to e-mail system.

There are many user guides in the Internet nowadays, but using them with out understanding the key issues of e-mail system are not an option. Only understanding how the e-mail system actually works makes it possible to setup solution in practice.

The diploma work describes future plans and results as well.

7. Viiteloetelu

1. IMAP Security - encryption and authentication http://www.coruscant.demon.co.uk/mike/imap/security.html, vaadatud 14.05.2009
2. Kodulehe majutus ja e-post http://lahendus.elion.ee/?event=Show_hosting#anchor01, vaadatud 13.05.2009
3. Exchange Server Version Comparison http://www.microsoft.com/exchange/2007/evaluation/features/ex_compare.mspx , vaadatud 14.05.2009
4. Re: sendmail vs. postfix question http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2001-02/0676.html, vaadatud 19.05.2009
5. Sendmail Versus Postfix Versus Exim http://www.bobhoffman.com/forums/viewtopic.php?f=4&t=14, vaadatud 19.05.2009
6. Fedorafoorum.org postfix vs sendmail http://fedoraforum.org/forum/showthread.php?t=124640, vaadatud 13.05.2009
7. Postfix vs. qmail – Performance http://www.dt.e-technik.uni-dortmund.de/~ma/postfix/vsqmail.html, vaadatud 13.05.2009
8. PostfixCompleteVirtualMailSystemHowto http://www.dt.e-technik.uni-dortmund.de/~ma/postfix/vsqmail.html, vaadatud 13.05.2009
9. OSnews What to select for Servers: Windows 2003 or UNIX? http://www.osnews.com/story/8626/What_to_select_for_Servers_Windows_2003_or_UNIX_, vaadatud 13.05.2009
10. SquirrelMail https://mailhost.ut.ee/src/login.php, vaadatud 14.05.2009,

11. http://en.wikipedia.org/wiki/Squirrelmail

12. The Big Picture https://help.ubuntu.com/community/PostfixCompleteVirtualMailSystemHowto, vaadatud 13.05.2009

13. The Perfect SpamSnake - Ubuntu 8.04 LTS http://www.howtoforge.com/the-perfect-spamsnake-ubuntu-8.04, vaadatud 05.05.2009

14. Package: pyzor (1:0.4.0+cvs20030201-8) http://packages.debian.org/sid/pyzor, vaadatud 13.05.2009

15. razor-check(1) - Linux man page http://linux.die.net/man/1/razor-check, vaadatud 13.05.2009

16. Distributed Checksum Clearinghouses http://www.rhyolite.com/dcc/, vaadatud 13.05.2009

17. The Rationale: SPF Explained http://old.openspf.org/howworks.html, vaadatud 13.05.2009

18. FuzzyOcrPlugin http://wiki.apache.org/spamassassin/FuzzyOcrPlugin, vaadatud 13.05.2009

19. The Perfect SpamSnake - Ubuntu 8.04 LTS - Page 07 http://www.howtoforge.com/the-perfect-spamsnake-ubuntu-8.04-p7, vaadatud 13.05.2009

20. Greylisting Spams with Postfix + Gld http://hostingfu.com/article/greylisting-spams-with-postfix-gld, vaadanud 13.05.2009

21. Logwatch Statistical Reporting http://www.howtoforge.com/the-perfect-spamsnake-ubuntu-8.04-p7, vaadatud 13.05.2009

22. How To Automatically Add A Disclaimer To Outgoing Emails With alterMIME (Postfix On Debian Etch) http://www.howtoforge.com/add-disclaimers-to-outgoing-emails-with-altermime-postfix-debian-etch, vaadanud 13.05.2009

23. SpamLinks Backscatter http://spamlinks.net/prevent-secure-backscatter.htm, vaadatud 13.05.2009

24. Re: [Clamav-users] ClamAV vs Commercial Products http://www.mail-archive.com/clamav-users@lists.clamav.net/msg03578.html, vaadatud 15.05.2009

25. The Perfect SpamSnake - Ubuntu 8.04 LTS - Page 06 http://www.howtoforge.com/the-perfect-spamsnake-ubuntu-8.04-p6, vaadatud 13.05.2009
26. zen.spamhaus.org http://www.spamhaus.org/ZEN/, vaadatud 15.05.2009
27. SpamCop http://www.spamcop.net/, vaadatud 15.05.2009
28. The Spamhaus Block List http://www.spamhaus.org/sbl/index.lasso, vaadanud 15.05.2009
29. Exploits Block List http://www.spamhaus.org/xbl/index.lasso, vaadanud 15.05.2009
30. Bayesian spam filtering http://en.wikipedia.org/wiki/Bayesian_spam_filtering, vaatadud 15.05.2009
31. transport - Postfix transport table format http://www.postfix.org/transport.5.html, vaadatud 15.05.2009
32. Virtual Users With Postfix, PostfixAdmin, Courier, Mailscanner, ClamAV On CentOS http://www.howtoforge.com/virtual_users_postfix_courier_mailscanner_clamav_centos, vaadatud 10.05.2009
33. PostfixCompleteVirtualMailSystemHowto https://help.ubuntu.com/community/PostfixCompleteVirtualMailSystemHowto, vaadatud 15.05.2009
34. Postfix Configuration Parameters http://www.postfix.org/postconf.5.html, vaadanud 15.05.2009
35. Postfix + Maildrop Howto http://www.postfix.org/MAILDROP_README.html, vaadatud 15.05.2009
36. Postfix Configuration - UCE Controls http://www.postfix.org/uce.html, vaadanud 15.05.2009
37. SMTP Service Extension for Authentication http://tools.ietf.org/html/rfc4954, vaadatud 15.05.2009
38. SMTP Service Extension for Command Pipelining http://www.ietf.org/rfc/rfc1854.txt, vaadatud 15.05.2009

39. „Windows Server Inside Out“ William R. Stanek Microsoft Press 2008, vaadanud 10.05.2008

40. Index of /debian/pool/main/m/mailscanner, http://debian.intergenia.de/debian/pool/main/m/mailscanner/, vaadanud 16.05.2009

41. The Perfect SpamSnake - Ubuntu 8.04 LTS - Page 05, http://www.howtoforge.com/the-perfect-spamsnake-ubuntu-8.04-p5, vaatatud 16.05.2009

42. The Perfect SpamSnake - Ubuntu 8.04 LTS - Page 06, http://www.howtoforge.com/the-perfect-spamsnake-ubuntu-8.04-p6, vaatatud 16.05.2009

43. Virtual Users With Postfix, PostfixAdmin, Courier, Mailscanner, ClamAV On CentOS, http://www.howtoforge.com/virtual_users_postfix_courier_mailscanner_clamav_centos, vaadatud 11.05.2009

44. CentOS http://www.centos.org/, vaadatud 16.05.2009

45. About CentOS http://www.centos.org/modules/tinycontent/index.php?id=2, vaadatud 16.05.2009

46. Virtual Users And Domains With Postfix, Courier And MySQL (CentOS 5.1) http://www.howtoforge.com/virtual-users-and-domains-postfix-courier-mysql-centos5.1, vaadatud 11.05.2009

47. Virtual Users And Domains With Postfix, Courier, MySQL And SquirrelMail (CentOS 5.3 x86_64) - Page 5, http://www.howtoforge.com/virtual-users-domains-postfix-courier-mysql-squirrelmail-centos-5.3-x86_64-p5, vaadatud 17.05.2009

48. Virtual Users With Postfix, PostfixAdmin, Courier, Mailscanner, ClamAV On CentOS - Page 5 http://www.howtoforge.com/virtual_users_postfix_courier_mailscanner_clamav_centos_p5, vaadatud 17.05.2009

Lisad

Konfiguratsiooni failid on toodud CD-plaadil kataloogides mailgw.testhost.ee ja mail.testhost.ee.

Lisa1 mailgw.testhost.ee konfiguratsioonifailid

header_checks – Postfix kirja päise kontrolli seadistuse fail.

MailScanner.conf – MailScanner filtri põhiseadistuse fail.

main.cf – Postfixi põhiseadistuse fail.

master.cf – Postfix põhiprotsesside seadistuse fail.

named.conf – Bind9 põhiseadistuse fail.

named.conf.options – Bind9 parameetrite seadistuse fail.

relay_domains – Postfixi edastatavate domeenide seadistuse fail.

relay_recipients – Postfixi seadistuse fail, mis määrab, kellele adressaadid, kellele kirju edastatakse.

sender_access – Postfixi seadistuse fail, kus määratakse, kelle kirju võetakse/ei võeta vastu.

transport – Postfixi fail, mis kirjeldab, kuhu edasisuunata mingi domeeni kirjad.

virtual – Postfixi fail, mis kirjeldab, kuhu edastatakse lokaalsete kasutajate kirjad.

aliases – Postfix e-posti aliaste seadistus faili.

config.inc.php – PostfixAdmin seadistus fail.

main.cf – Postfixi põhiseadistuse fail.

master.cf – Postfix põhiprotsesside seadistuse fail.

mynetworks – Postfixi seadistus fail, mis määrab ära usaldusväärsed võrgus, kelle kirju edastatakse.

mysql_relay_domains_maps.cf – Postfixi seadistuse fail, mis sisaldab päringut MySQL baasi, et saada teada domeenid, millele tulnud kirju server edastab (Server on antud domeeni varu MX server).

mysql_virtual_alias_maps.cf – Postfixi seadistuse fail, mis sisaldab päringut MySQL baasi, et saada teada e-postiaadressi aliasaadressid.

mysql_virtual_domains_maps.cf – Postfixi seadistuse fail, mis sisaldab päringut MySQL baasi, et saada teada domeenid, millele tulnud kirju server aktsepteerib (Server on antud domeeni põhi MX server).

mysql_virtual_mailbox_limit_maps.cf – Postfixi seadistuse fail, mis sisaldab päringut MySQL baasi, et saada teada postkasti mahulimiit.

mysql_virtual_mailbox_maps.cf - Postfixi seadistuse fail, mis sisaldab päringut MySQL baasi, et saada teada, kasutaja Maildir formaadis postkasti kaust.

named.conf – Bind9 põhiseadistuse fail

postfixadmin.conf – PostfixAdmin veebiliidese Apache seadistuse fail.

transport – Postfixi fail, mis kirjeldab, kuhu edasisuunata mingi domeeni kirjad.