Tallinna Ülikool

Digitehnoloogiate instituut

GNU/Linuxi pahavara ja sellest hoidumine

Seminaritöö

Autor: Sten-Aron Ulp

Juhendaja: Edmund Laugasson

Autor: ..... ,, ... ,, 2016

Juhendaja:..... ,, ... ,, 2016

Instituudi direktor:..... ,, ... ,, 2016

Tallinn 2016

Autorideklaratsioon

Deklareerin, et käesolev seminaritöö on minu töö tulemus ja seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

....

(kuupäev) (autor)

Sisukord

Sissejuhatus

Tihtipeale arvatakse, et mida levinum on GNU/Linux operatsioonisüsteem, seda rohkem ka pahavara leitakse ja levib. Samuti on sagedane arvamus, et GNU/Linux'i operatsioonisüsteemid on viirusevabad. Töö autor soovis seda teemat uurida ja saada teada kuidas tegelikult on lood GNU/Linuxi pahavara ja viiruste levikuga ning kuidas on võimalik oma arvutit nende eest kaitsta.

Küberturvalisus on tänapäeval tõsine teema - aina rohkem sõltutakse arvutitest ja nende abil töötavatest süsteemidest, kuna need on peamiseks tähtsate dokumentide ja failide hoiustamise kohaks, mis vajavad erilist kaitset. See ongi peamine põhjus, miks on äärmiselt oluline hoida arvutid turvatud ja pahavaravabad.

Käesoleva töö eesmärgiks on uurida, kas ja miks GNU/Linux on vähem või rohkem haavatavam kui teised operatsioonisüsteemid. Samuti soovitakse töös uurida kuidas kaitsta ennast viiruste ja pahavara eest ning millised on kõige levinumad pahavarad ja selgitada välja GNU/Linuxile parimad viirusekaitse tarkvarad.

Töö eesmärgi saavutamiseks kasutatakse erinevaid otsingumootoreid, meediat, foorumeid ja muid netiväljaandeid, kust otsitakse antud teema kohta aktuaalset ja tarvilikku informatsiooni.

1 Ülevaade GNU/Linuxist

Linux on operatsioonisüsteem - programmide kogum, mis juhib arvuti tööd. Linux on sarnane Microsoft Windowsiga, erinevuseks, et ta on täienisti tasuta. Korrektsem nimi sellel on GNU/Linux, kuid lihtsalt „Linuxit“ kasutatakse rohkem. (Pereira, 2012)

Linux ei ole ühe ettevõtte toode, kuid paljud ettevõtted ja erinevad inimrühmad aitavad seda arendada. Linuxi kerneli ümber loodud tarkvara, dokumentatsiooni ja tugiteenuste kogumit kutsutakse distributsiooniks. Distributsioonid muudavad Linuxi välimust ja funktsioone täielikult. Need ulatuvad suurtest, hästi toetatud täielikest süsteemidest (firmade poolt heaks kiidetud) kuni vähesema arengu ja toetusega süsteemideni. (Pereira, 2012)

1.1 GNU/Linuxi kasutamine

1.1.1 Tutvumine

GNU/Linuxi kasutamine pole Windowsi kasutamisest keerulisem ja sellel on rohkem võimalusi. On tarvis kõigest mõni minut, et teha tutvust erinevate distributsioonidega nagu Ubuntu või Fedora, mis kaasnevad erinevate juba paigaldatud programmidega. Linuxiga saab kaasa ka tuhandeid erinevaid tasuta programme, mis toetavad erinevaid dokumente ja faile, mida ka Windowsit kasutades avada saab. (Pereira, 2012)

1.1.2 Eelistused

Linuxil on mitut erinevat tüüpi kasutajaid. Ühed on need kes eelistavad käsurida ja teised kes eelistavad graafilist liidest. Graafiline liides on siiski ressursinõudlikum, seega leidubki kasutajad, kes kasutavad graafilist liidest ainult mitme terminali

emulaatori akna üheaegseks käivitamiseks, kuna saadakse hakkama programmeerimise ja muude tegevustega ka väikse ja kiire aknahalduriga.

Linuxil on palju erinevaid aknahaldureid ja töölaua keskkondi, mida kasutaja saab vastavalt maitsele ja teatud ülesande lahendamiseks omale sobiliku valida. Ühed populaarsemad töölaua keskkonnad on GNOME, KDE ja XFCE. (Vananurm, 2002)

1.2 GNU/Linuxi distributsioonid

Iga Linuxi distributsiooni tuumas on operatsioonisüsteem Linux Kernel, kuid igat ühte on ehitatud üles oma valikul teistest komponentidest põhinedes valitud sihtgrupile. Enamik Linuxi kasutajaid valib omale Linuxit vahetades erinevaid distributsioone kuni leiab ühe enda vajadustele sobiliku. Kuid uutel ja kogemusteta kasutajatel valik sadade erinevate distributsioonidel, millel erinevusi võib raske leida võib olla keeruline.

1.2.1 Tuntud GNU/Linuxi distributsioonid

Ubuntu

Ubuntu on arvatavasti kõige tuntum Linuxi distributsioon. Ubuntu omab Unity’t, mis on üheks kõige poleeritumaks graafiliseks kestprogrammiks Linuxi ökosüsteemis. (Sharma, 2015)

Ubuntu omab väga lihtsat paigaldajat. Ubuntu ei oma eelnevalt koodekeid, kuid neid saab lihtsalt märkeruuduga endale paigaldamisel kaasata. (Sharma, 2015)

Samuti omab Ubuntu tööriistu veebi ja e-posti sirvimiseks, multimeedia failide mängimiseks ja dokumentidega töötamiseks. Ubuntul on üks ühest suurematest tarkvara-hoidlatest, kust võib leida juurde erinevaid huvitavaid rakendusi. (Sharma, 2015)

Linux Mint

Linux Mint on järsku tõusnud teiste populaarsete Linuxi distributsioonide sekka, selle peamisteks põhjusteks on Ubuntul põhinemine ja traditsioonilisem töölaud kui Ubuntu vastuoluline Unity liides. (Sharma, 2015)

Nagu Ubuntu, selle distributsiooniga on samuti kaasas palju erinevaid rakendusi tööks ja meelelahutuseks. Mint kaasab audio ja video koodekid koheselt distributsiooniga. (Sharma, 2015)

Fedora

Üheks vanimaks Linuxi distributsiooniks on Fedora. Fedora on alguse saanud 1990. aastatel ning tekkis kui Red Hat Linux otsustas hargneda oma distributsiooni Red Hat Enterprise Linux'iks ja Fedora Projektiks aastal 2003.

Selle distributsiooni eesmärgiks on pakkuda täiesti tasuta tarkvara kõigile ning on loodud alternatiiviks Ubuntule. Tänu oma pühendatud tarkvarale ja serveri-kesksete funktsioonidele, see RPM-põhine distributsioon on sageli kirjeldatud sobilikuks teadlikule kasutajatele. (Sharma, 2015)

Gentoo

Gentoo distributsioon on mõeldud rohkem teadlikule kasutajale. Kasutajad saavad üles seadistada oma operatsiooni-süsteemi peaaegu nullist. See on üheks kõige rohkem seadistatavaks distributsiooniks, mille paigaldamine võib võtta tundidest päevadeni. (Sharma, 2015)

1.2.2 Erinevad Linuxi turvatestimise distributsioonid

Linuxi distributsioonid saab jagada erinevateks kategooriateks põhinedes sihtgruppidele ja kasutaja vajadustele.

Kasutajad, kes soovivad olla rohkem turvatud on saadaval ka erinev valik distributsioone, mis põhineb just privaatsuse kaitsmisel. Need distributsioonid aitavad hoiduda digitaalse jalajälje mahajätmist veebis liikumisel.

Kuid tõsiselt paranoilistele, privaatsus distributsioonid on ainult üks osa võrrandist – ja suurem osa sellest võrrandist hõlmavad turvatestimise (*penetration testing)* distributsioonid. Need distributsioonid on mõeldud võrgu süsteemide turvalisuse hindamiseks ja analüüsimiseks. (Sharma, 2015)

Blackbox

Ubuntul põhinev distributsioon, mis on mõeldud turvatestimiseks. Blackboxil on vaikimisi lihtne XFCE töölauakeskkond, millel on xfwm aknahaldur, mis teeb ta väga kiireks süsteemiks.

Erinevalt enamikust teistest distributsioonidest mis omab kirevat rakenduste valikut, Blackbox teeb teadlikke jõupingutusi, et vältida rakenduste ülearususi. Otsides rakendusi leiab ainult kõige paremad tööriistad vajaliku ülesande jaoks. Tööriistad on sorteeritud kategooriatesse, mis muudavad need kergesti märgatavaks.

Blackbox omab ka Tor veebilehitsejat, mis tavaliselt leidub privaatsust hindavatel distributsioonidel, mis on mõeldud oma digitaalse kohaloleku varjamiseks. (Sharma, 2015)

Kali

Vaieldavalt kõige populaarsem turvatestimise distributsioon, mis sisaldab sadu vahendeid selle teostamiseks. Kalit on võimalik jooksutada läbi CD, USB pulga või installida kettale. Kali on ulatuslikult kohandatav distributsioon, mis võimaldab

kasutajatel muuta ja kompileerida Linux Kernelit oma täpsetele nõuetele. (Sharma, 2015)

Security Onion

Baseerunud Ubuntul, see distributsioon on mõeldud sissetungimise avastamisele ja võrgu turvalisuse järelvalvele. Erinevalt *penetration testing* distributsioonidele, mida mõeldakse ründava turvalisuse distributsiooni all, Security Onion on pigem kaitsev distributsioon. (Sharma, 2015)

1.3 GNU/Linuxi levik

Kuigi Linux on hakanud viimastel aastatel levima rohkem, on selle osakaal tavakasutajate seas ikka veel väga väike. Kindlasti on haridussüsteem ja harjumuspärasus selle suur mõjutaja. Enamus tavakasutajaid on käsitlenud ainult Microsofti Windows operatsioonisüsteeme seega kardetakse, et üleminek teisele operatsioonile võib olla liialt keeruline ja tülikas ning võtab kaua aega ümberõppimiseks. Samuti õpetakse ka koolides siiani kahjuks „Excelit“ ja „Wordi“, mitte tabeli- ja tekstitöötlust. Teadmatus ja hirm uue ees on rahvasuus loonud müüte ja hirmulugusid Linuxist, mis enamasti ei vasta tõele. (Vananurm, 2002)

1.4 GNU/Linuxi kasutamise põhjused

Linuxit valitakse operatsioonisüsteemiks järjest rohkem kasutajaid. Nendeks on professionaalid, arvutihuvilised, teadlased ja isegi kodukasutajad. (Vananurm, 2002)

Linux on jäädavalt tasuta

Pole vahet mitmesse arvutisse Linux paigaldatakse, hind jääb ikka nulliks (Bothwick, 2010). Windowsit endale ostes ei saada selle programmi omanikuks, vaid saadakse ainult litsents mis lubab seda kasutada. (Vananurm, 2002)

Linuxi distributsiooni omades on vabadus seda õppida, kopeerida muuta ja edasi jagada seda – mis teebki Linuxist tõeliselt tasuta vabatarkvara. (Pereira, 2012)

Tuhandeid kaasatud programme

Linux distributsioonid tulevad kaasa tasuta tuhandete rakendustega. Kui teised operatsioonisüsteemid peavad töölauda ja veebilehitsejat kõigiks vajalikuks, siis Linuxiga on kaasatud kõik mida sooviksid: interneti-tööriistad, kontori-tarkvara, multimeedia ja mängud. Ja kui midagi jääb pärast paigaldust puudu, on võimalik rakendusi juurde tõmmata. (Bothwick, 2010)

Vabadus valida distributsioone

Kui ei sobi, saab alati uue valida. Enamus distributsioone säilitab kasutaja andmed erineval partitsioonil, et uue distributsiooni valimisel jääksid seaded, emailid ja muud andmed alles. (Bothwick, 2010)

Tarkvara hoidlad

Kogu tarkvara on ühes kohas, mis tähendab, et soovitud programmi leiab hoidlast, mis säästab aega ja vaeva. See samuti tähendab, et tarkvara on iseseisvalt ülevaadatud ja digitaalselt allkirjastatud distributsiooni arendajate poolt, tehes peaaegu võimatuks pahavaraga nakatatud tarkvara saamiseks.

Kontrollitud ja töötava vabatarkvara laod on kohe uuematele Linuxitele sisse ehitatud, neist saab turvaliselt tõmmata kontrollitud tarkvara, mille eest pole vaja maksta ja mis töötab hästi. Ära jääb Windowsi maailmas levinud vabavaralehtedel otsimine, mis võib arvutisse tuua ka ohtlikku tarkvara, reklaamvara või pahavara. Linuxis pole kindlasti tavakasutajal vaja administreerimisõigusi, millega saaks ta arvutisse paigaldada ohtlikke lisasid.Linux on klassikaliste UNIX opsüsteemide vaimus ja põhimõtete järgi loodud süsteem, milles tavakasutaja ja administraatori õigused hoitakse rangelt lahus. (Bothwick, 2010)

Turvalisus

Kasutatakse täielikku mälukaitset, st ükski programm ei saa kirjutada teise programmi poolt kasutatavasse mälualasse, mis on Windows’il põhiline "sinise surmaekraani" tekitaja.

Veelgi enam, kuna Linuxi tuum on avatud lähtekoodiga, on ilmne, et seda vaatavad läbi ja siluvad tuhanded inimesed ja firmad üle maailma. On levinud väärarusaam, et kuna lähtekoodi näevad kõik, siis saab sealt kergemini leida võimalusi, kuidas tuuma vigu kurjalt ära kasutada. Tegelikkuses leiavad enamasti vead üles siiski Linuxi arendajad ja parandused tulevad tavaliselt juba sama päeva jooksul (Microsoftil näiteks on see aeg teatavasti tunduvalt pikem). Linuxi viirused ei saa teha rohkem kahju kui kasutajal on õigusi. (Vananurm, 2002)

Pahavara vähesus

Pahavara on Linuxis üsna vähe levinud. Selle peamiseks põhjuseks on Linuxi avatud lähtekood. Installides oma distributsiooni hoidlatest on teada, et tarkvara on eelnevalt kontrollitud ja pahavaravaba. (Bothwick, 2010)

2 GNU/Linuxi turvalisus

Nagu osad inimesed usuvad, et Mac OS-id on viiruste vastu immuunsed, omavad mõned Linuxi kasutajad ka sama väärarusaama.

Räägitakse, et Linux on viirustevaba, mis kahjuks ei vasta tõele kuna ükski operatsioonisüsteem ei ole 100 protsenti turvatud ja Linux pole ka erandiks. Kuid siiski pole Linuxil olnud nii suurt pahavara puhangut kui Windowsi operatsioonisüsteemidega. Kuigi Linuxil viiruste levik on väike, võib siiski sattuda süsteem ohtu kui Linuxit ei hooldata turvaliselt. (Kumar 2013)

Linuxi turvalisus

Linux on iseenesest arhitektuuriliselt tugev, ning pakub väga head turvalisust tema kasutajatele. Regulaarsetest kerneli uuendustest kuni peaaegu igapäevastele turvalisuse uuendustele, Linuxi arendajad hoiavad Linuxit väga turvatuna. Ettevõtete omanikud kes tuginevad kaubanduslikult toetatud Linux distributsioonidele saavad juurdepääsu igale turvalisuse uuendusele. Linuxil on ülemaailmne kogukond, kes pakuvad parandusi turvaaukudele ja muudele probleemidele, kus ühelgi ettevõttel pole suletud lähtekoodi. (Hess, 2010)

On levinud väärarusaam, et kuna lähtekoodi näevad kõik, siis saab sealt kergemini leida võimalusi, kuidas tuuma vigu kurjalt ära kasutada. Tegelikkuses leiavad enamasti vead üles siiski Linuxi arendajad ja parandused tulevad tavaliselt juba sama päeva jooksul. (Vananurm, 2002)

Otsides endale sobilikku Linuxit, tuleks olla kindel mis leheküljelt distributsioon endale tõmmatakse. Tuleb veenduda, et leht oleks sama distributsiooni arendajate poolt loodud, kuna võõrastelt lehtedelt võib saada juba pahavaraga nakatunud distributsiooni.

Programmid jooksevad tava-, mitte juur-kasutajal

Et Linuxil viirus nakatada käivitava failiga, need failid peavad olema kirjutavad kasutaja poolt, kes seda viirust aktiveerib. Võimalik, et programmid kuuluvad juur kasutajale ja kasutatakse tavakasutaja kontot. Seega mida vähem kogenenud kasutaja, seda väiksem on tõenäosus, et ta üldse omabki mingit käivitavad programmi. Seega kasutajad, kes on vähemteadlikud on need kellel on vähem viljakad kodukataloogid viiruste jaoks. (Ray, 2015)

Tarkvara paigaldada usaldusväärsetest hoidlatest

Linuxi distributsiooniga saab kaasa palju erinevaid rakendusi, mis on arendajate poolt eelnevalt kinnitatud ja allkirjastatud, tõestamaks, et neid on ohutu paigaldada. (help.ubuntu, 2015)

Hoida eemale imelikest käskudest

Ei tohiks terminalis jooksutada käske, mida ei usalda. Näiteks käsk rm -rf / kustutab kõik mis vähegi võimalik, kaasa arvatud failid kõvakettal ja failid ühendatud irdkandjad. (Hoffman, 2012)

Teha varukoopiaid

Arvutis olevad andmed võivad kahjustada saada mitte ainult pahavara tagajärjel, samuti pole riistvara ka igavene ning näiteks tugev voolukõikumine või telefoniliini sisselöönud pikne võivad hävitada teie fotod, videod, muusika, dokumendid ja palju muud hädavajalikku. Kõige selle uuesti loomine võtaks tohutult palju aega ning pahatihti pole see ka võimalik. Tehes varukoopiaid võib pärast süsteemi taastamist jätkata oma tegemist samast seisust, millal viimase varukoopia tegid. Praegusel ajastul on väga levinud ka erinevad pilveteenused, mis võivad samuti hoiustada teie tähtsaid faile ja meedia faile. (Marek, 2013)

3 GNU/Linuxi pahavara

Pahavara on igasugune programm või fail, mida kasutatakse ilma omaniku teadmata tema arvutisse tungimiseks ja/või selle kahjustamiseks. Pahavara arvutis on mitut liiki: viirused, ussid, troojalased, reklaamvara, nuhkvara ja palju teisi. Pahavara ei teki iseenesest, see on loodud mingi inimese või inimesegrupi poolt uudishimust või soovist kellelegi liiga teha varaliselt. (Rouse, 2008)

3.1 GNU/Linuxi pahavara levik

Suurem sihtmärk ei võrdu suurema haavatavusega

Usutakse, et kui Linux oleks sama levinud kui Windows oleks Linuxil sama palju viiruseid ja pahavara kui praegu Windowsil. Mida võib vähesel määral tõeks pidada desktopi kasutajate seas. (Trent, 2013)

Argumendiks on öeldud, et „Linux on viiruse ja pahavara vaba ainult sellepärast, et sellel on nii väike turuosa“, mis on tegelikult vale, kuna mainitakse ainult desktopi maastikul põhinevaid Linuxi andmeid. Netcrafti andmetel on Windowsi osakaal veebi serverites on ainult viiendik ning ülejäänud on põhiliselt Unix/Linux serverid, kus üle 75% maailma veebiserverite jooksevad Unixil ja Linuxil, tuua esile argumendi „mida rohkem GNU/Linux operatsioonisüsteemis esineb seda rohkem ka pahavara leitakse ja levib“, võib öelda, et Linuxi serverid on kõige suurema sihtmärgiga. Kuid nii see pole, kuna tavaliselt rünnatakse servereid, mida on lihtsam ära kasutada, milleks on pigem Windowsi serverid kui Linuxi omad.

Siiski Windowsi populaarsus desktopi maastikul on ikkagi faktor, kuna rünnatakse palju tavakasutajaid. (Trent, 2013)

Kust võib saada endale pahavara?

Pahavara võib arvutisse sattuda mälupulgal, CD- plaadil või mingil muul andmekandjal, peidetud mõnda rakendusse või dokumenti, kaasatud e-kirjale või tulla ise läbi puuduva või aukliku tulemüüri. Nakatunud arvutil võib kahjustada saada

kõvaketas, emaplaat või mõni muu seade, pahavara võib arvutist kustutada olulisi andmeid või vajaminevaid programme.

Uusim pahavara üritab siiski toimetada teie arvutis võimalikult vaikselt ja tagasihoidlikult, et te midagi kahtlustama ei hakkaks ning oma igapäevaseid toimetusi julgelt edasi teeksite – kasutaksite internetipanka, vahetaksite konfidentsiaalseid sõnumeid, sisestaksite oma kasutajatunnuseid ja salasõnu. (Kirna, Aasmäe).

Linuxi tarkvara paigaldamine

Linux võib sattuda ohtu kui otsides internetist mingi programmi paigaldamise kohta, soovitatakse sul lisada mingi PPA (*Personal Package Archive*) hoidla, mis tähendab mittestandardset tarkvara/uuendust, mis on mõeldud neile, kes soovivad kõige uuemat ja paremat. PPA hoidlad on tavaliselt tavainimese poolt loodud, mis tähendab, et alati ei pruugi teada kas see on legitiimne või pahatahtlik hoidla. Samuti võidakse soovitada installida ka kuritahtlik .deb fail, mis on Debian distributsiooni laiendus failitüüp, et lisada mingit põnevat funktsionaalsust, mis Ubuntul puudub. (Rovelli 2015)

Seetõttu soovitatakse ikka kõik vajaminev tarkvara ametlikest hoidlatest installeerida, mis on palju turvalisem kui ise internetist midagi otsima minna.

Enamasti viirused ja pahavara on probleemiks mitte süsteemi pärast vaid kasutaja tõttu (kelleks enamusajast on süütu ohver).

Samuti ei aita sellele kaasa see ütlus - „Linux on immuunne viiruste vastu“, mis võib mõned kasutajad ära petta, seejärel julgelt internetiavarustes ringi liikuda ning faile avada ja tõmmata. (askubuntu, 2011)

Kuigi võib olla, et kasutaja on ise teadlik oma turvavigadest, ning eelistabki olla vähe turvatud või siis ei osata või pole aega. Ohtlik võib olla süsteemi ja tarkvara mitte uuendamine, viiruse- ja pahavaratõrje programmide puudus. Tulemüüri mittekasutamine, igasuguse mittevajaliku allalaadimine ja rämpspostiga saadetud failide avamine. (landfield, 2008)

E-kirjaga saadetavad failid - Tavaliselt on saadetavad failid .exe või .zip faili-tüübiga, mis Linuxi masinas niisama tööle ei hakka. Kui saadud fail oleks suunatud Linux masinatele oleks failitüübiks .deb, .rpm või .bin.

Kui kasutatakse RPM-põhist süsteemi ja saadetud manuse failitüübiks oleks .rpm, avaneks see peale vajutades. Seejärel, pärast pealevajutamist küsitaks juurkasutaja õigustes kasutaja salasõna ning selle sisestamisel on süsteem sattunud ohtu kui on tegemist pahavaralise failiga. (Wallen, 2010; landfield, 2008)

Pahatahtlikud veebilingid - Üheks pahatahtlikuks veebilingiks on võltsitud aadress. Aadress, mis on pahatahtlik aga kujutab ennast turvalisena. Need võivad olla võltsitud panga konto sisselogimise ekraanid, Paypali sisselogimise leht või mingi muu leht, mis üritab kasutajalt kasutajanime ja salasõna kätte saada, et seda kurjasti ära kasutada. Need küll ei paku mingit ohtu Linuxi süsteemile, kuid kasutajale võib olla see väga ohtlik. Õnneks on uuematel veebilehitsejatel olemas laiendused, mis kaitsevad sinu veebisirvimist. (Wallen 2010)

Sotsiaalvõrgustikud (Facebook, Twitter, Instagram, Linkedin, Flickr) -

Andmevaraste, rämpspostisaatjate ja pahavaraprogrammide levitajate lemmikkohad. Tavaliselt meelitatakse mingi huvitava videoga, kuid selle vaatamiseks on mingi koodek vaja tõmmata, mis võib sisaldada pahavara. (landfield, 2008)

3.2 GNU/Linuxi pahavara ja viiruste eest kaitsmine

Pahavara tuvastamine

Parimaks pahavara avastamise meetodiks on viirusetõrjeprogrammi kasutamine. Siiski viirustõrjeprogramm ei taga kõikide pahavarade tuvastamist.

Mõnda pahavara saab tuvastada ainult spetsiaalsete, teatud pahavarade jaoks loodud viirusetõrjeprogrammidega ning see pahavara jääb tavapärasele viirusetõrjeprogrammile nähtamatuks. Üheks selliseks pahavaraks on ka eeltoodud rootkit ja lisaks APT (Advanced Persistent Threat) - ebamääraselt jõuline küberoht.

Õnneks on olemas erinevad pahavara skannerid, mis töötavad nagu viirusetõrje ning mis otsivad süsteemist juurkomplekte (*rootkit*), tagauksi (*backdoor*) ja muid teisi varjatud faile ja turvaauke. (landfield, 2008)

Märgid potentsiaalsest pahavarast arvutis

Viirused ja muud pahavarad tihti muudavad veebilehitseja kodulehte. Samuti võib veebilehitsejale äkitselt tekkida uus tööriistariba, mida varem pole näinud. Peale selle iseavanevad aknad veebilehitsejas, mis võivad olla märgiks nuhkvara nakkusest saadud kogemata mingi tarkvara paigaldamisel, mis ei ole ainult tüütu vaid ka pahatahtlik.

Kui ootamatult süsteem, rakendused või interneti kiirus muutub väga aeglaseks võib olla tegemist pahavaraga. Selle põhjuseks võivad olla ka muud asjaolud aga alati tuleks kontrollida, et ei oleks tegu pahavaraga.

Veel üks märk potentsiaalsest pahavara nakkusest on kõvaketta tegevus. Kui on märgata liigset aktiivsust kõvakettal, isegi kui seda hetkel ei kasutata ja pole ühtki programmi või allalaadimist toimumas, tuleks kontrollida süsteemi pahavara osas.

Märk viirusest võib olla ka see kui viirusetõrje on väljalülitatud. Mõned pahavara programmid on spetsiaalselt mõeldud turvaprogrammide väljalülitamisele jättes kasutaja ilma kaitseta. (Neagu, 2014)

Viisid pahavaraga tegelemiseks ning arvuti- ja andmekaitseks

Pahavara eemaldamiseks on kaks meetodit. Esimeseks on viirusetõrjega pahavara eemaldamine. Olenedes viirusetõrje tarkvarast ja pahavara tüübist, mõned viirusetõrjed oskavad parandada nakatunud faili. Seetõttu pole alati vajagi nakatunud faili kustutada. Teine viis pahavara eemaldamiseks on ise käsitsi pahavaraliste failide kustutamine.

Et parandada vigast või nakatunud rakendust, tuleks rakendus uuesti paigaldada. Näiteks kui viirus nakataks Firefoxi, tuleks Firefox uuesti alla laadida ja paigaldada. Pärast seda võiks kasutaja sama teha ka osade süsteemifailidega nagu GRUB ja Linuxi tuum (*kernel*).

Kui kasutaja pole kindel, kas tarkvara on pahavaraga nakatunud või mitte saavad nad skaneerida tarkvara viiruste osas ja eraldada see programm ülejäänud süsteemist (*sandbox*). *Sandbox* on turvalisuse mehhanism, kus ülejäänud süsteemist eraldatud rakendus käivitatakse piiratud ressursidega. See ei luba pahavaral süsteemile liiga teha, kuna piiratud ressursid takistavad rakendusel pahavaraliste ülessannete tööd. Kui süsteem tuvastab, et rakendus on pahavaraga nakatunud, saab kasutaja või süsteem kustutada pahavaralise programmi. *Sandboxing* programmid on osadel viirusetõrjetel toetatud, kui mitte on see allalaaditav..

Hoides programmid ja viirusetõrjed uuendatuna ning tulemüür õigesti seadistatuna aitab pahavara saamise tõenäosust vähendada. Paigaldades veebilehitseja lisandid, mis takistavad kasutajat pahavaralistel lehekülgedel käimist kaitseb samuti pahavara saamise eest. Samuti, ei tohiks kasutada juurkasutaja (*root*) õiguseid kui just väga on vaja. Igapäevaselt juurkasutajana süsteemi kasutamine annab pahavarale samad õigused. See võib juhtuda kui kasutaja käivitab või paigaldab pahavara või nakatunud faili. (Johnson, 2013)

3.2.1 Viirusetõrjetarkvara

Kuigi Linux on üsna turvaline operatsioonisüsteem, peaks seda siiski turvama, kuna üksi süsteem pole veatu, mida keegi võib kurjasti ära kasutada. Turvalisus pole seisund vaid protsess, mille eest peab pidevalt hea seisma sõltumata kasutatavast tarkvarast. See on kasutaja enda otsustada, kas ta soovib viirusetõrjet või mitte, siiski peaks viirusetõrje-programm olemas olema nii serverite kui tööjaamade jaoks ning samuti ka kui tegeletakse tähtsate firma või kooliasjadega.

Viirusetõrje puudumisel võivad Windowsi arvutid laadida nakatunud failid sinu Linuxi masinasse, lubades neil nakatada teisi Windowsi süsteeme. Antiviirused otsivad Windowsi pahavara ja kustutavad need. Viirusetõrje Linuxi masinal ei ole ainult iseenda kaitseks, see kaitseb ka Windowsi masinaid iseendi eest. (Lutter, 2014)

Erinevad viirusetõrjetarkvarad

ClamAV - Arvatavasti kõige populaarsem vabavaraline Linuxi viirusetõrje. ClamAV on saadaval nii Linuxile kui ka MS Windowsile nime all ClamWin. ClamAV on avatud lähtekoodiga viirusetõrje, mis on oskab leida erinevaid usse ja viiruseid. (Johnson, 2013)

Avast! Linux Home Edition – Tasuta versioon populaarsest Avasti viirusetõrjest. (Lutter, 2014)

AVG Antivirus - AVG on populaarne Windowsis. See on samuti tasuta viirusetõrje Ubuntule, mis nagu teisedki viirusetõrjed tuvastab nakatunud faile aga ei eemalda neid. (Lutter, 2014)

BitDefender - Viirusetõrjetarkvara, mis on saadaval Ubuntule mitteäriliseks kasutamiseks. BitDefender litsentsi saab ainult 30-neks päevaks, kuid seda saab uuesti taotleda, kui tekib vajadus. (Lutter, 2014)

Comodo - Pakub samasugust kaitset viiruste eest, nagu nende turvalahendused Windowsi operatsioonisüsteemidele, kuid lisaks omades täielikult kohandavat rämpsposti filtreerimissüsteemi. (help.ubuntu, 2015)

F-PROT - Viirusetõrjetarkvara, mis on saadaval kõikidele Linuxi tööjaamadele. See pakub täielikku kaitset makro viiruste ja muu pahavara vastu – sealhulgas ka troojalaste. (help.ubuntu, 2015)

3.3 GNU/Linuxi pahavarad ja viirused

Pahavara sisaldab igasugust tarkvara, mis kahjustab süsteemi, andmeid või rakendusi. Paljud pahavara kategooriad kattuvad nagu trooja ja nuhkvara. (Johnson, 2013)

Troojalased (Trooja hobune) - Rakenduses peidus olev programm, mis kahjustab süsteemi ja kogub kasutaja andmeid. Troojalased levivad tavaliselt e-kirjade teel ning üritavad saada kasutajalt olulisi andmeid ja salasõnu, mis pärast trooja kodeerijale saadetakse. Trooja tavaliselt ennast ei paljunda ja ise-enesest nad arvutisse ei pääse, kasutaja peab seda sisaldava rakenduse ise käivitama. (Johnson, 2013)

Juurkomplekt (*Rootkit*) - Need on teatud tüüpi Trooja hobused, mis toimetavad süsteemis juurkasutaja õigustes, tavaliselt operatsioonisüsteemi tuuma tasandil, hiilides niiviisi mööda operatsioonisüsteemi turvamehhanismidest. Rootkitid hoiavad oma faile, registrivõtmeid ja võrguühendusi niivõrd peidus, et kasutaja ei oleks suuteline neid ise avastama. Rootkitid on ühed kõige ohtlikumad pahavarad, mis võib kasutajal ja turvarakendustel märkamata jääda. (Kirna, 2008)

Nuhkvara - Pahavara, mis kogub kasutaja privaatset infot (finants infot, paroolid, kasutajanimed) ja saadab need nuhkvara loojale või mingile teisele isikule, kes sellel seda infot vaja läheb. Nuhkvarad võivad olla troojalased ja mõned troojalased võivad olla nuhkvarad. (Johnson, 2013)

Reklaamvara - Tarkvara, mis iseenesest kuvab reklaame on reklaamvara. Kuna enamus Linuxi arendajad jätavad distributsioonile avatud lähtekoodi, pole sealt väga palju reklaamvara leitud. (Johnson, 2013)

Ussid - Pahatahtlik arvutiprogramm, ennast paljundab ja levib võrgu kaudu teistesse arvutitesse läbi e-posti, sotsiaalvõrkude ja turvaaukude kaudu. Ussid erinevad viirustest süsteemi pääsemise kaudu. Kui kasutaja toob selle süsteemi on see viirus ja kui pahavara pääses süsteemi ilma kasutaja sekkumiseta on see uss. (Johnson, 2013)

Viirused - Kahjustav arvutiprogramm, mis võib end ise kopeerida ja arvutit nakatada. Viirused leidub tavaliselt rakenduste ja paigaldajate sees. (Johnson, 2013)

Hirmuvara (*Scareware*) - Pahavara, mis meelitab kasutajad paigaldama mingit pahavaralist viirusetõrjeprogrammi, mis võib näidata, et arvuti sisaldab viiruseid ning neist saab lahti juhul kui ostad selle programmi täisversiooni. *Scareware* hirmutab kasutajat maksma raha või paigaldama pahavara, et kaitsta ennast olematu ohu eest. (Johnson, 2013)

Lunavara (*Ransomware*) - Sarnane hirmuvarale, lunavara võib lukustada arvuti ja/või krüpteerida su failid ära ning ainuke viis andmete kättesaamiseks on maksta lunaraha. Lunavara tõesti lukustab süsteemi ja krüpteerib faile, samas kui hirmuvara ainult hirmutab. (Johnson, 2013)

Tagauks (*Backdoor*) - Sissepääs arvutisse läbi nakatunud süsteemi, mis lubab küberkurjategijatel siseneda süsteemi. (landfield, 2008)

Klahvinuhk (*Keylogger*) - Nuhkvara, mis salvestab kõik klahvivajutused ja saadab need üle interneti e-posti või FTP aadressile. Klahvinuhid võivad salvestada ka ekraanipilte ja hiireklõpse. Klahvinuhk installeeritakse ohvri arvutisse nende teadmata, nende tegevuse kontrollimiseks või privaatse info ja pangakonto andmete varguseks. (Malwaretruth)

APT (*Advanced Persistent Threat*) - Võrgurünne, kus volitamata isik saab juurdepääsu võrku ning jääb sinna märkamatult pikemaks ajaks. APT rünnaku põhjuseks on varastada andmeid mitte kahjustada võrku. ATP rünnakute sihtmärgiks on suured organisatsioonid, kus on kõrge väärtusega informatsiooni, nagu riigikaitse, majandus- ja finatssektor. (Veldre, 2011)

Veebilehitseja kaaperdaja (*Browser Hijacker*) - Soovimatu tarkvara, mis muudab veebilehitseja seadeid ilma kasutaja loata. Veebilehitseja kaaperdaja võib asendada olemasoleva kodulehe omaenda otsingu lehega. Need on tavaliselt kasutatud, et sundida külastusi teatud veebilehele, suurendades selle reklaamitulu. (Malwaretruth)

Kokkuvõte

Arvatakse, et mida levinum on GNU/Linux operatsioonisüsteem, seda rohkem ka pahavara levib ja leitakse. See aga ei vasta tõele, kuna mõeldud on ainult tööjaamadel põhinevaid andmeid. Tegelikult on Linux väga levinud - nimelt serverite osas, jooksutades üle 75% maailma veebiserverite kogumahust. Sellegipoolest satuvad Windowsi serverid tihedamini rünnete ohvriteks kui Linuxi serverid, kuna rünnatakse neid, mida on lihtsam ära kasutada.

Linuxi tuum on avatud lähtekoodiga, mis on kõigile alati saadaval vaatamiseks ning muutmiseks, mis tähendab, et isegi kui suudetaks sellele pahavara lisada, leitakse see Linuxi arendajate poolt üles juba samal päeval.

Vaatamata Linuxi turvalisusele pole ta siiski täiesti pahavara- ja viirustevaba, kuna ükski süsteem pole täielikult kaitstud. Enamus pahavara satub arvutisse just kasutaja hooletusena. Internetis ringi liikudes ja faile allalaadides tuleb olla ettevaatlik, kuna kunagi ei tea, kui ette võib juhtuta üks pahatahtlik veebilink, mis võib kellegi isiklikku infot või näiteks pangakonto andmeid kurjasti ära kasutada. Väga ettevaatlik peaks olema just sotsiaalmeedias ja e-posti kasutades, kuna need on andmevaraste, rämpspostisaatjate ja pahavaraprogrammide levitajate lemmikkohad.

Tuleb tõdeda, et alati ei piisa ainult ettevaatlikkusest, sest viirus või muu pahavara võib nakatada arvutit ka ilma kasutaja kaasabita. Seetõttu tuleks arvutit kaitsta viirusetõrje-tarkvaraga ja tulemüüriga. Linuxi kõige enam soovitatumad viirusetõrje tarkvarad on ClamAV, Comodo ja BitDefender.

Kõige levinum pahavara on troojalased, ussid, viirused, hirmuvara, lunavara, nuhkvara, reklaamvara, tagauks, klahvinuhk, juurkomplektid, veebilehitseja kaaperdaja ja APT ning kuigi Linuxit peetakse ohtutumaks olles üldlevinud arvamuse kohaselt vähemlevinud, siis eelnimetatud põhjustel on soovitatav nende eest kaitsmiseks kasutada käesolevas töös väljatoodud kaitsetarkvarasid.

Kasutatud kirjandus

Serrano Pereira. (2012). Linux Frequently Asked Questions. (http://www.getgnulinux.org/en/linux/linux_faq/)

Toomas Vananurm. (2002). Kontoritöö korraldamine LINUX-põhise tarkvara abil. (http://web.zone.ee/zeroconf/materjalid/linux_kontoris.pdf)

Shashank Sharma. (2015). 10 best Linux distros: which one is right for you?

(http://www.techradar.com/news/software/operating-systems/best-linux-distro-five-we-recommend-1090058)

Shshank Sharma. (2015). 10 of the best Linux distros for privacy fiends and security buffs.(http://www.techradar.com/news/software/security-software/10-of-the-best-linux-distros-for-privacy-fiends-and-security-buffs-1292902)

Neil Bothwick. (2010). 20 reasons you should switch to Linux. (http://www.techradar.com/news/software/operating-systems/20-reasons-you-should-switch-to-linux-912294)

Avishek Kumar. (2013). Is Linux Operating System Virus Free? (http://www.tecmint.com/linux-operating-system-is-virus-free/)

Ken Hess. (2010). 10 Reasons to dump windows and use Linux.

(http://www.pcworld.com/article/201731/10_reasons_to_dump_windows_and_use_linux.html)

Chris Hoffman. (2012). 8 Deadly Commands You Should Never Run on Linux

(http://www.howtogeek.com/125157/8-deadly-commands-you-should-never-run-on-linux/)

help.ubuntu. (2015). Why do I need anti-virus software? (https://help.ubuntu.com/community/Antivirus)

Ray. (2015). Why do I need anti-virus software?

(https://help.ubuntu.com/community/Antivirus)

Marek. (2015). Kuidas kaitsta arvutit pahavara/viiruste eest!

(http://ekaitse.ee/uldine/kuidas-kaitsta-arvutit-pahavara/viiruste-eest)

Margaret Rouse. (2008). Malware (malicious software).

(http://searchmidmarketsecurity.techtarget.com/definition/malware)

Trent. (2013). I'M TIRED OF THIS MYTH.

(https://linuxcritic.wordpress.com/2013/09/06/im-tired-of-this-myth/)

Paolo Rovelli. (2015). Don't believe these four myths about Linux security.

(https://blogs.sophos.com/2015/03/26/dont-believe-these-four-myths-about-linux-security/)

Aare Kirna,Priit Aasmäe. (Kuupäev puudub). Pahavara.

(http://www.arvutikaitse.ee/arvutikaitse-algtoed/pahavara/)

Jack Wallen. (2010). Myth Busting: Is Linux Immune to Viruses?

(https://www.linux.com/learn/tutorials/284124-myth-busting-is-linux-immune-to-viruses)

lanfield. (2008). Windows 7 turvalisus - I. Osa.

(http://landfield.pri.ee/Windows_7/Win7_turva_1.html)

Askubuntu. (2011). Why aren't viruses an issue?

(http://askubuntu.com/questions/37198/why-arent-viruses-an-issue)

Aurelian Neagu. (2014). 10 Warning Signs That Your Computer is Malware Infected

(https://heimdalsecurity.com/blog/warning-signs-operating-system-infected-malware/)

Devyn. C. Johnson. (2013). Malware and Antivirus Systems for Linux.
(http://www.linux.org/threads/malware-and-antivirus-systems-for-linux.4455/)

Veronia Lutter. (2014). Linuxi Antiviirused.

(https://wiki.itcollege.ee/index.php/Linuxi_Antiviirused)

Aare Kirna. (2008). Rootkit.

(http://www.arvutikaitse.ee/rootkit)

Anto Veldre. (2011). APT – Jõuliselt ebamäärane küber-oht.
(http://www.arvutikaitse.ee/apt-jouliselt-ebamaarane-kuber-oht/)

Malwaretruth. (Kuupäev puudub). The List of Malware Types.

(http://www.malwaretruth.com/the-list-of-malware-types)