Tallinna Ülikool

Digitehnoloogiate Instituut

Tasuta viirusetõrjete võrdlus Microsoft Windows 8.1 näitel

Seminaritöö

Autor: Talis Dreifeldt

Juhendaja: Edmund Laugasson

Autor:……“…….……”2015

Juhendaja:……...……..“..……...……”2015

Instituudi direktor:..……...……“…….……”2015

Tallinn 2015

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

Viirusetõrjed, sealhulgas just tasuta viirusetõrjed, on laialt levinud tänapäeval. Inimesed kasutavad üha rohkem priivaralisi tooteid ja mõistavad, et nad ei jää palju alla tasulistele versioonidele. Kiputakse ekslikult arvama, et tasuta saadud programm ei kõlba kuhugi. Tegelikkus on aga see, et kui kasutada arvutis õigeid võtteid ja tasuta turvavarustust, ei ole nendel programmidel häda midagi.

Viirusetõrjeid on palju: on olemas kalleid viirusetõrjeid paljude funktsioonidega. Samas leidub ka odavamaid mitmete funktsioonidega ning on ka tasuta erinevate funktsioonidega. Valik on ühesõnaga suur ja autorina leian, et miks mitte proovida priivaralisi viirusetõrjeid. Kui nad juba on valmis tehtud ja neid kasutatakse ülemaailmselt, siis miks ma peaksin sellest võimalusest loobuma.

Antud seminaritöö eesmärgiks ongi välja selgitada, kas tasuta viirusetõrjed sisaldavad vajalikke funktsioone ja oskusi, et kaitsta minu arvutit erinevate ohtude eest. Seejärel võrrelda nende funktsioone omavahel ning koostada loend sammudest, millest kinni pidades võiks arvutis kasutada priivaralist viirusetõrjet. Samuti seletada mõningaid mõisteid, mis arusaamatuks võivad jääda.

Selle eesmärgi saavutamiseks koostab töö autor artiklite põhjal loendi populaarsetest tasuta viirusetõrjetest. Andes nendest programmidest ülevaate, kus toob välja head ja halvad küljed. Käib läbi nii paigaldusprotsessi kui ka kasutajaliidese. Peale kõikide programmide testimist on plaanis koostada kokkuvõttev funktsioonide tabel ning kõike eelnevat silmas pidades ja juurde lugedes, koostada loend turvalisest arvutikasutusest.

1. Tuntumad tasuta viirusetõrjed

Arvuti kaitsmiseks mõeldud priivaralisi viirusetõrjeid on nii erineva välimuse kui oskustega. Autor tutvustab siinkohal populaarsemaid priivaralisi viirusetõrjeid, mida soovitatakse kasutada spetsialistide arvamuse kohaselt oma arvuti turvamiseks mittevajalike programmide eest. (PCMag).

Kõik need viirusetõrjed võivad olla sobivad turvamaks ükskõik millist arvutit ükskõik milliste ohtude eest. See nimistu peaks aitama arvuti kasutajal otsustada, millist priivaralist viirusetõrjet ta tulevikus kasutab enda arvuti failide kaitsmiseks. Samuti andma ülevaate kõigist maailmas enim kasutavatest tasuta viirusetõrjetest. Autor katsetas antud seminaritöö käigus seitset erinevat tasuta viirusetõrjet.

1.1 Tasuta programmid

Priivaralised viirusetõrjed on neile, kel puudub võimalus ja vajadus soetada midagi kallist. Samuti teadmatus, kas just see tasuline versioon on seda raha väärt või mitte. Võrreldes tasuliste viirusetõrjetega on priivaralisel vähem funktsioone, aga see ei tähenda seda, et samade funtsioonide töö tase oleks halvem. Autori arvates on tasuta viirusetõrjete puhul just eeliseks lihtsus, mis tasuliste puhul on kaduv nähtus.

1.1.1 360 Total Security

Nõuded arvutile

Koduleht: http://www.360totalsecurity.com

Operatsioonisüsteem: MS Windows 10/8.1/8/7/Vista/XP

Mälu: 512 MB RAM

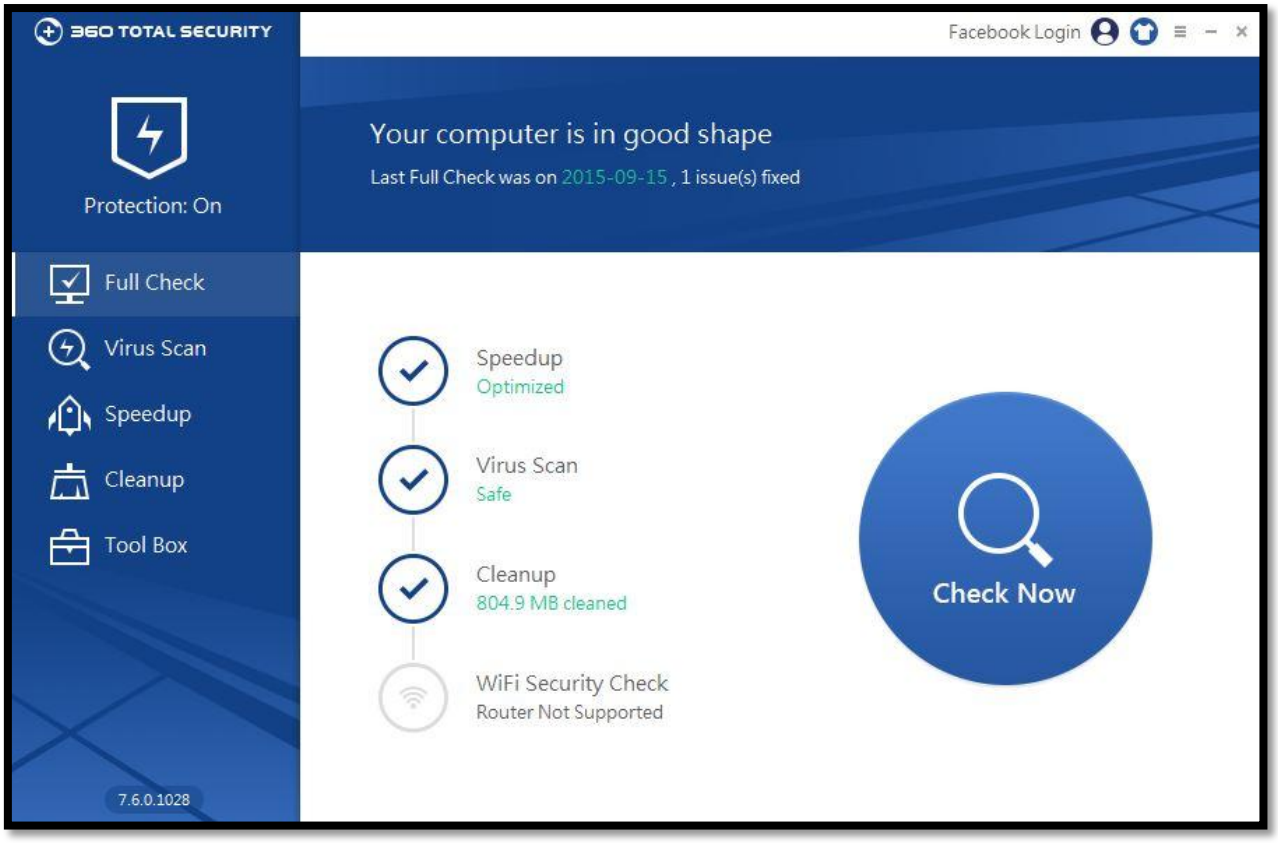
Protsessor: 1,6 GHz

Vaba ruumi vajadus kettal: 1 GB (360totalsecurity).

Paigaldamine

Paigaldamist alustades küsitakse nõusolekut info saatmise kohta tootjale. Samuti tuleb nõustuda litsentsitingimustega. Linnukese eemaldamisega loobume info saatmisest. Litsentsiga peab olema päri, muidu paigaldada ei lasta. Samuti saab valida 11 keele seast endale sobiva, eesti keel valikusse ei kuulu. Paigaldamine käib kiirelt ja kohe teostatakse esmane kontroll. Esimene viirusetõrje, mis uurib kas arvutis on lehitsejate juures midagi üleliigset ja vajadusel eemaldab ka selle. Samuti saab kontrollida, ega sinu operatsioonisüsteemile uuendusi vahepeal välja ei ole tulnud. Lisaks saab viirusetõrjele juurde paigaldada nii avira kui ka bitdefenderi mootori. Üks väheseid viirusetõrjeid, millel puudub hetkel tasuline versioon.

Facebooki sisselogimise võimalus läbi viirusetõrje. Ka USB pulga ühendades arvutiga, kontrollib antud viirusetõrje selle kohe läbi. Üldse ei meeldi failid faililaiendiga .exe ja tahab nad kohe eemaldada. Ükskõik, kas nad on reaalselt ohtlikud või mitte. Veel jäi silma suutmatus administraatori õigustega koostööd teha. Käivitasin viirusetõrje administraatori õigustes ja pannes ta faile kontrollima, ei suuda ta endiselt neid funktsioone käivitada, mis vajavad administraatori õigusi. Viiruse üldine välimus on silmasõbralik (vt Pilt1).



Pilt1: 360 Total Security

Kasutajaliides

Alustame esimesest reast, kust leiame *Full Check* ehk täis kontroll. Antud kontroll on jagatud nelja ossa. Esimene kontrollib seda, kui kiiresti arvuti käivitub ehk *Speedup*. Teises osas viskab ta pilgu arvutis olevatele failidele ehk *Virus Scan*. Kolmandas puhastab ta lehitsejat, kui seal peaks olema midagi üleliigset ehk *Cleanup*. Viimaseks on Traadita võrgu turvalisuse kontroll ehk *WiFi Security Check*. Pean mainima kahjuks, et minu traadita võrku ta kordagi kontrollida ei suutnud. Seda sel lihtsal põhjusel, et minu ruuter ei toeta seda funktsiooni.

Teises reas asub Virus Scan ehk viiruse kontrollimine. See jaguneb kolmeks. Esimene neist teeb failidest kiire ülevaate ehk *Quick Scan*. Teine vaatab läbi kõik arvutis olevad failid ehk *Full Scan*. Viimases saab kasutaja ise valida, mida ta tahab, et viirusetõrje üle vaataks ehk *Custom Scan*. Samuti on seal näha, kui palju faile on hetkel karantiinis (*Quarantine*) ja kasutaja poolt lisatud usaldusväärseid lehekülgi (*Trust List*). Kas siin esineb kadusid administraatori õigustega tavakasutajal.

Kolmandas reas asetseb juba kord mainitud *SpeedUp*, mis on jaotatud viieks. Esimene rida annab teada, kas arvuti käivitus protsess on korras ja midagi üleliigset ei käivitu. Järgmised neli toimivad ainult administraatori õigustes. Isegi kui ma käivitan viirusetõrje administraatori õigustes (Run as administrator), siis endiselt ma neid kasutada ei saa. Töötavad ainult siis, kui viirusetõrje avada administraatori kasutaja alla. Tavakasutaja kontos midagi neist kasutada ei saa kahjuks. See on väga ebameeldiv.

Eelviimases reas on ka teistkordselt mainitud *Cleanup* ehk ebavajalike failide kontroll lehitsejates. Kontrollib lehitsejate vahemälu ja tühjendab need vajaduse korral. Ka siin saab karantiini (*Quarantine*) kontrollida. Kas siin kõik funktsioonid ei toimi tavakasutajal.

Viimaseks on *Tool Box*. Esimene funktsioonidest on *Patch Up*, mis kontrollib operatsioonisüsteemi uuendusi ehk tagab selle, et süsteemi kõik turvaaugud on maksimaalselt kaitstud. Teine on *SandBox*, kus saab käivitada programme, mille puhtuses viirustest kasutaja kindel pole. Kolmandaks on *System Backup Cleaner*, mis puhastab kasutamata varukoopia failidest, mida enam kasutataval kettal pole, et kettale rohkem ruumi saada. Uutest funktsioonidest on siin veel *Browser Protection* ehk brasuseri kaitse, kus on võimalik lukustada lehitsejate seaded. Veel on *Firewall* ehk tulemüür, mis tuleb eraldi programmina alla laadida. Samuti saab ruuterisse sisse logida läbi viimase lisa, milleks on *Router Manager*. Need samuti ei toimi tavakasutajas. (vt Pilt1)

Kasutajamugavus

Esmane tutvus antud viirusetõrjega oli igati positiivne, kuna leidis palju uut ja huvitavat, mida mujal kohanud pole. Kasutada oli viirusetõrjet väga lihtne, kõik oli viirusetõrjet avades nähtav ja väga mugavalt seadistav. Sinna hulka kuulub ka töölaualt failide kontroll hiire parema klahvi alt. Ainuke asi, mis tõsiselt häiris on see varem mainitud administraatori õigustega koostöö, mis tavakasutaja puhul üldse ei toimi.

Eripärad

Mainis siin ära, et nagu mobiilil saab taustapilti vahetada, sai antud viirusetõrje puhul sama teha. Esialgu küll pilt kaua ei püsinud ja viskas peale uuendust algseadistuse peale tagasi, siis uuesti muutmine polnud väga keeruline. Lehitsejate vahemälu tühjendamine. USB seadme läbivaatus ning MS Windowsi uuenduste kontroll. Lisaks saab lehitsejate seadeid lukustada ja oma ruuterisse sisse logida läbi viirusetõrje. Palju puudusi seoses administraatori õigustega. Automaatse kontrolli saab seada, aga ainult ühe.

Katsetused

1. Kolm põhilist kontrollimise tüüpi

Quick scan ehk kiire kontroll - Objekte: 16 831, Aeg: 00:01:11

Custom scan ehk valikuline kontroll(kontrollisin Windowsi kausta) - Objekte: 103 488, Aeg: 00:09:15

Full scan ehk kõikide failide kontroll - Objekte: 231 501, Aeg: 00:56:24

2. Jälgisin ka kontrollide käigus protsessori kasutust(*CPU Usage*) ja protsessori maksimaalset sagedust(*Maximum Frequency*), mõlemaid 5 minutit, mille jooksul kogunes vähemalt 200 näitajat ning kirja läks tulemus, mida esines vähemalt viis korda. Testitaval arvutil on Intel(R) Pentium(R) CPU B960 @ 2.20GHz. Esimesena toon välja samad näitajad, kui viirusetõrje veel ei kontrollinud(*CPU Usage*: 2-6% ja *Maximum Frequency*: 36-43%). Kontrolli käigus esinesid järgnevad näitajad:

CPU Usage: 8-53%

Maximum Frequency: 36-98%

3. Et katsetada viirusetõrje käitumist, kui viirus satub süsteemi, kasutasin EICAR(*European Institute for Computer Anti-virus Research*) faile. Tegemist on failidega, kus esineb ainult üks rida teksti, mis peaks aga äratama iga viirusetõrje tähelepanu. Alla sai tõmmatud neli dokumenti: eicar.com, eicar.com.txt, eicar_com.zip ning eicarcom2.zip. Antud viirusetõrje puhul oli test igati edukas. Alla laaditud failid ei jõudnud kuhugi, vaid liikusid kohe karatiini, kust nad hiljem kustusid. (EICAR).

1.1.2 Avast Free Antivirus 2015

Nõuded arvutile

Koduleht: https://www.avast.com/

Operatsioonisüsteem: MS Windows 10/8.1/8/7/Vista/XP, Linux CentOS 6 ja uuem/Debian 7 ja uuem/Red Hat Enterprise Linux 6/Ubuntu LTS 12.4

Mälu: 128 MB RAM

Protsessor: Intel Pentium III või kõrgem

Vaba ruumi vajadus kettal: 2 GB (Avast).

Paigaldamine

Paigaldamise protsess alguses tuleb valida kahe erineva variandi vahel. Esimene valik on *Regular Installation* ehk regulaarne paigaldus. See võimalus on ka esitletud suurema kirjaga. Selle variandi puhul valitakse kõik kasutaja eest ära ja tulebki ainult nõustuda litsentsiga ja informatsiooni saatmisega tootjale, et muuta viirusetõrjet paremaks. Samuti annab teada, et kui ei soovita infot saata, saab selle hiljem seadetest maha võtta. Peale paigaldamist käivitub *quick scan* ehk kiire kontroll.

Teiseks võimaluseks on *Custom Installation* ehk kohandatud paigaldus, mille esimese sammuna saame valida asukoha, kuhu me paigaldame. Seejärel saame valida komponendid ja keele. Edasi on litsentsi ja andmete saatmisega nõustumine ning järgnebki paigaldamise protsess. Peale mida käivitub taaskord juba mainitud kiirkontroll.

Keelte kohta tuleks veel nii palju rääkida, et seadete alt saab seda muuta. Esialgu on seal ainult inglise keel, aga erinevate keelte pakette on kokku 45, mida saab alla laadida. Mainin siinkohal ära, et peab olema administraatori kasutajas, et alla laadida uusi pakette. Keelte hulka kuulub ka eesti keel. Samuti saab seadete alt tõesti loobuda linnukese eemaldamisega andmete saatmisest tootjale. Lisaks annab viirusetõrje häälega teada, kui mingi toiming on toimunud. Esmaspilgul autorit selline asi ehmatas ja õnneks saab ka seda seadete alt linnukese eemaldamisega keelata. Kahjuks ei saa reklaame alumisest osast linnukese kaotamisega eemaldada. Selleks peab tasulise versiooni juba kasutusele võtma.

Tegu on küll tasuta viirusetõrjega, aga ilma kasutaja registreerimiseta, saab antud toodet kasutada ainult 30 päeva. Registreerides pakutakse ka tasulist versiooni, aga valides tasuta versiooni, saate ühe aastase litsentsi. Mainitakse ka ära, et tasuta versiooni litsentsi saab uuendada nii palju kui kasutaja seda soovib. Registreerimisel küsitakse e-posti aadressi ja nüüd pakutakse tasulist versiooni 20 päevaks, millest saab keelduda. Kõige selle tulemusel saab nüüd antud viirusetõrjet kasutada 365 päeva. Meilile mitte mingit teadet selle kohta ei saabunud.

Pilt2: Avast Free Antivirus 2015

Kasutajaliides

Alustame vasakust reast kõige kõrgemalt, milleks on *Overview* ehk ülevaade. Siit näeb kas kõik kaitsekilbid on tööseisukorras ja kas viirusetõrje on ajakohane. Lisaks saab käivitada *Smart scan* ehk nutikat kontrolli. Antud kontroll otsib esmalt pahavara ja viiruseid. Järgneb uuenduste kontroll tarkvarale ning lehitsejate lisade kontroll. Viimastena kontrollitakse koduvõrku, ühilduvust ja kas jõudlusega on probleeme. Tuleb ära mainida, et kõiki funktsioone ei saa tasuta versioonis kasutada. Järgmisena saab käivitada *Browser cleanup* ehk lehitsejate lisamoodulite kontroll, mida ta tegelikult juba teostas nutika kontrolli käigus. Kolmandaks on *Home network security* ehk koduvõrgu turvalisuse kontroll, mida samuti juba tehti nutika kontrolli käigus. Viimane on *SecureLine VPN* ehk andmete kaitse võõraste eest, mis kuulub tasulise versiooni juurde.

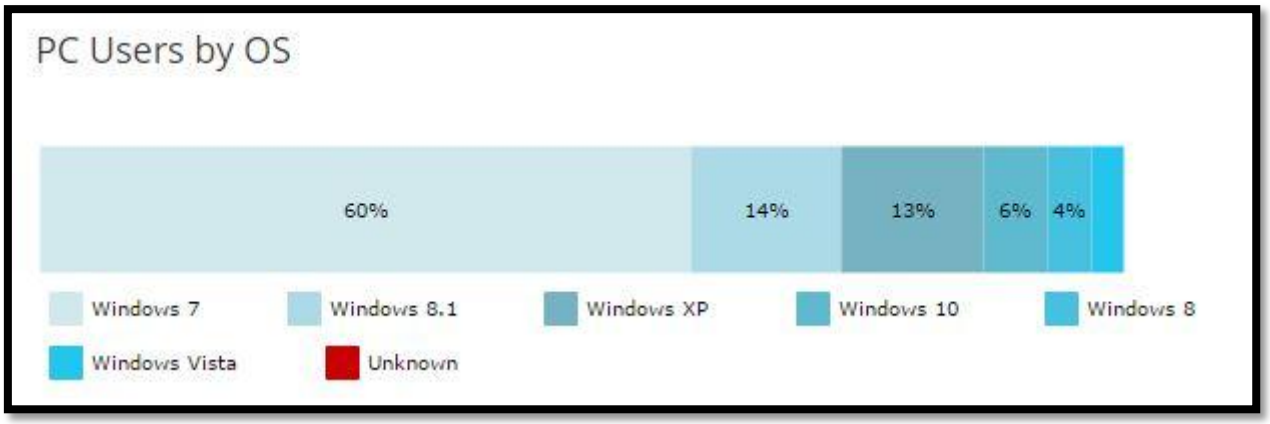
Järgmiseks on *Scan* ehk kontroll. See jaguneb kuueks. Esimene neist on juba tuttav *Smart scan* ehk nutikas kontroll. Teiseks on *Scan for viruses* ehk viiruste kontroll arvutis. Kolmandaks *Scan for browser add-ons* ehk lehitsejate lisamoodulite kontroll. Neljandaks *Scan for outdated software* ehk kontrollib, kas arvutis olev tarkvara on uuendatud viimasele versioonile. Eelviimasena on *Scan fot network threats* ehk võrgu ohtude kontroll. Viimaseks *Scan for performance issues* ehk jõudluse probleemide kontroll. Siingi pean hoiatama, et kõik funktsioonid ei tööta tasuta versioonil.

Kolmas ülevalt vasakust reast on *Tools* ehk tööriistad. Seegi on sarnaselt eelmisele jagunenud kuueks. Esimeseks on *SecureLine VPN* ehk oma andmete kaitse võõraste eest, mida saab proovida 7 päeva, aga muidu on tasuline. Järgmiseks on *Remote Assistance* ehk kaugabi. Selle abil saab minna teise Avastit kasutava kasutaja töölaule ja teda aidata, kui ta peaks millegiga abi vajama. Probleem ei pea ainult antud toodet puudutama. Kolmandaks on *Rescue Disk* ehk päästeketas, kus saab luua koopia enda arvuti kaustadest ja failidest. Seda saab kas teha USB pulgale või CD plaadile. Kolm järgmist funktsiooni kuuluvad tasulise versiooni alla.

Neljandaks on *Store* ehk pood, kus saab soetada nii erinevaid lisasi kui ka tasulisi täispakette.

Viiendaks on *Account* ehk kasutaja. Imelik on see, et e-post, mille autor alguses registreeris, et antud toode kestaks kauem kui 30 päeva, ei saa kasutada kasutaja tegemisel, sest see on juba kasutuses. Samas saab sisse logida läbi facebooki ja google konto. Kasutaja loomine suurt midagi juurde ei anna, lihtsalt veel üks koht, kus saab tasulist versiooni osta. Lisaks saab tegevuste eest punkte, mille alusel pannakse viirusetõrje kasutaja tootja edetabelisse.

Eelviimaseks on *Statistics* ehk statistika. Siin all kohtab nii kasutaja andmed kui ka ülemaailmsed andmed. Kasutaja andmete all näeb näiteks üldist statistikat sellest, kui palju kontrolle on teostatud ja mitu viirust on blokeeritud. Samas ülemaailmsete juures kohtame liigitust turvalisuse statistika ja kasutajate statistika. Turvalisuse statistika all näeme kui palju erinevaid viiruse definitsioone on lisatud viimase 12 kuu jooksul. Kasutajate statistikast näeme aga millise MS Windowsi versiooniga jookseb kõige rohkem antud viirusetõrjeid. Populaarseim on ülekaalukalt MS Windows 7 (vt Pilt3).



Pilt3: Populaarseim MS Windows

Viimaseks on *Settings* ehk seaded. Koosneb seitsmest erinevast osast. Esimene neist on *General* ehk üldised seaded. Nende alla kuuluvad näiteks keele valik, nutika kontrolli seadistamine ja andmete jagamisest keeldumise võimalus. Teiseks on *Active Protection* ehk püsikaitse. Siia alla kuuluvad *File System Shield* ehk failisüsteemi kilp, *Mail Shield* ehk e-kirja kilp *ja Web Shield* ehk veebi kilp. Kolmandaks *Update* ehk uuendamine, kus näeb, mis versioonid jooksevad hetkel ja millal viimati uuendati. Neljandaks on *Registration* ehk registratuur, millest on juba varem juttu tehtud, kui 30 päevasest litsentsist sai 365 päeva. Viies on *Tools* ehk tööriistad. Seal saab osasid funktsioone välja või sisse lülitada. Järgmiseks on *Troubleshooting* ehk vea selgitamine ehk valikud mis võivad aidata lahendada erinevaid probleeme. Viimaseks on *About Avast* ehk teave antud viirusetõrje kohta. (vt Pilt2)

Kasutajamugavus

Kasutamine on mugav, kuna kõik valikud on nähtavad avades viirusetõrjet. Samuti saab faile mugavalt kontrollida töölaualt. Häiriva tegurina jäi silma keele pakettide paigaldamine. Et vahetada viirusetõrje keelt, peab alla laadima antud keele paketti ja see toimib ainult administraatori kasutajas. Käivitades toote administraatori õigustes (*Run as administrator*), ei saa ma endiselt alla laadida pakette, sest ta endiselt nõuab administraatori õigusi.

Eripärad

Esimesena meenub nutikas kontroll. Kahjuks ei saa viirusetõrjet täisekraani suuruseks panna. Lisaks veel statistika ja pood viirusetõrjes. Keelte vahetamiseks pead antud keele paketti alla laadima. Viirusetõrje helid ütlevad, kui midagi sai viirusetõrje poolt tehtud. Viirusetõrjele saab seada salasõna, et keegi võõras ei saaks seadeid muuta. Saab seada automaatseid kontrolle

kindlale kellaajale. Lehitsejate lisade ja tarkvara ajakohasuse kontroll. Kaugabi võimalus teise Avasti viirusetõrje kasutajaga. Viimasena mainiks veel päästeketta loomise võimalust.

Katsetused

1. Kolm põhilist kontrollimise tüüpi

Quick scan ehk kiire kontroll - Objekte: 216 215, Aeg: 00:37:57

Custom scan ehk valikuline kontroll(kontrollisin Windowsi kausta) - Objekte: 125 936, Aeg: 00:22:26

Full scan ehk kõikide failide kontroll - Objekte: 362 764, Aeg: 01:11:12

2. Jälgisin ka kontrollide käigus protsessori kasutust(*CPU Usage*) ja protsessori maksimaalset sagedust(*Maximum Frequency*), mõlemaid 5 minutit, mille jooksul kogunes vähemalt 200 näitajat ning kirja läks tulemus, mida esines vähemalt viis korda. Testitaval arvutil on Intel(R) Pentium(R) CPU B960 @ 2.20GHz. Esimesena toon välja samad näitajad, kui viirusetõrje veel ei kontrollinud(*CPU Usage*: 2-6% ja *Maximum Frequency*: 36-43%). Kontrolli käigus esinesid järgnevad näitajad:

CPU Usage: 12-26%

Maximum Frequency: 36-84%

3. Et katsetada viirusetõrje käitumist, kui viirus satub süsteemi, kasutasin EICAR(*European Institute for Computer Anti-virus Research*) faile. Tegemist on failidega, kus esineb ainult üks rida teksti, mis peaks aga äratama iga viirusetõrje tähelepanu. Alla sai tõmmatud neli dokumenti: eicar.com, eicar.com.txt, eicar_com.zip ning eicarcom2.zip. Antud viirusetõrje puhul saab testi pidada igati edukaks. Alla laadima minnes, blokeeriti leht ja allalaadimist ei olnud võimalik sooritada. (EICAR).

1.1.3 AVG AntiVirus Free

Nõuded arvutile

Koduleht: http://www.avg.com/

1. Operatsioonisüsteem: MS Windows 10/8.1/8/7/Vista/XP

Mälu: 512 MB RAM

Protsessor: Intel Pentium 1.5 GHz

Vaba ruumi vajadus kettal: 950 MB

2. Operatsioonisüsteem: Mac OS X Mountain Lion või hilisem

Mälu: 2 GB RAM

Protsessor: Intel 64bit

Vaba ruumi vajadus kettal: 500 MB

3. Operatsioonisüsteem: Android 2.2 või uuem (AVG).

Paigaldamine

Paigaldamine algab laadimisega, millele järgneb valik, kas *Continue* ehk jätka või *Custom installation* ehk kohandatud paigaldus. Samuti saab siin valida endale sobiliku keele 23 variandi seast, kuhu eesti keel ei kuulu. Valides valikuks *Continue* nõustute antud toote litsentsiga ja teie eest tehakse kõik ülejäänud valikud automaatselt. Kuid enne paigaldamisprotsessi algust, pakutakse veel tasulist versiooni 30 päevaks, mis on automaatselt valitud teie eest või saate valida tasuta versiooni. Järgmiseks peatub paigaldamine 86. protsendi juures. Soovitakse kasutaja registreerimist ja seda selleks, et tasulise versiooni kõik funktsioonid aktiveeruks. Õnneks on kasutaja loomist võimalik edasi lükata, sest autori huvi on ainult tasuta toote vastu hetkel. Paigaldamise lõpuks teeme arvutile taaskäivituse antud viirusetõrje nõudmisel. Peale taaskäivitust toimub pikemat sorti uuendus, enne kui viirusetõrje tööle sai.

Valides aga *Custom installation*, pakutakse samamoodi 30 päeva tasulist versiooni. Valides tasuta versiooni jõuame järgmiste küsimusteni. Nimelt, kuhu kohta paigaldame ja millised komponendid. Järgneb paigaldamise protsess, mis peatub sarnaselt 86. protsendi juures, tahtes kasutaja registreerimist, millest loobume ning seejärel taaskäivitust arvutile. Peale taaskäivitust toimus esimene uuendus, mis kestib päris pikalt, enne kui viirusetõrjet kasutama sai hakata.

Esimene kontroll toimus läbi programmi *PC Analyzer* ehk arvuti analüüsija. Peale analüüsimise lõppu sooviti paigaldada teine programm nimega *AVG PC TuneUp* ehk AVG arvuti häälestaja, mis kirjade järgi oli tasuta. Paigaldades, aga pole kasutaja arvuti ühegi teise viirusetõrjega nii palju jahutust otsinud. Peale paigaldamist sai selgeks tõsiasi, et kogu värk on tasuta ainult üheks päevaks ja edasi kasutamiseks peab maksa. Ei tasu ikka alati kõike uskuda, mida kirjutatakse.

Pilt4: AVG AntiVirus Free

Kasutajaliides

Nagu pildilt on näha, jaguneb viirusetõrje avaleht viieks kastiks, millest esimese nelja juures saab midagi muuta. Viimane viies on juba tasulise versiooni osa. Esimene neist on *Computer* ehk arvuti. Sealt saab viirusetõrje välja lülitada vajadusel. Samuti saab sealt avada seaded, kust saab näiteks muuta seda kui põhjalikult faile kontrollitakse ja üldisi seaded viirusetõrje toimimise kohta. Samuti saab seadeid avada viirusetõrje ülevalt paremast nurgast *Options* ehk valikute alt. Seal asub ka *Reports* ehk aruanded, kus on kirjas kõik, millega viirusetõrje hakkama on saanud.

Järgmiseks on üldnimetus *Web* ehk võrk. Tema alla kuulub *LinkScanner* ehk veebilehekülgede kontroll. Ülessandeks on kontrollida veebilehekülgi, mida kasutaja külastab ja anda teada, kui satutakse kuhugi, mis võib sisaldada ohte. Lisaks saab seadete alt seda välja lülitada, kui ta peaks hakkama rohkem segama, kui aitama kasutajat.

Kolmandaks on *Identity* ehk identiteet, mis tegeleb identiteedi kaitse ja eraelu puutumatusega võõraste eest. Seda aitab teha *Identity Protection* ehk identiteedi kaitse, mis analüüsib tarkvara käitumist, et teha kindlaks, ega temas mingit ohtu ei pesitse. Seadete alt saab muuta seda, mida tehakse ohuga, kui see leitakse.

Viimaseks toimivaks osaks on *Email* ehk elektronpost, mis kontrollib sissetulevaid ja väljaminevad kirju ja ohu leidmisel suunab nad rämpsposti. Tema alla kuulub *Email Scanner* ehk elektronposti kontroll. Ta otsib kirjade juures kahjulikke lisasid. Seadete alt saab seada, kas kontrollitakse ainult sissetulevaid või ka väljaminevaid kirju ja näiteks missugune kirjutis ilmub ohtliku kirja pealkirjana.

Lisaks on nende all rida kust saab käivitada kiirelt kontrolli ehk *Scan now*. Tema alt saab algatada nii kõikide failide kui ka valitud failide ja kaustade kontrolle ning seada automaatseid kontrolle. Samast reast saab kontrollida ka viirusetõrje uuendusi, mis asuvad nupu all *Protection is up-to-date*. Nupp *Fix performance* ehk paranda jõudlust. Sellega käivitad *PC Analyzeri*, millest oli juba varem juttu. (vt Pilt4)

Kasutajamugavus

Kasutamise kohta mainiksin kohe ära, et kõik tasuta funktsioonid toimivad tavakasutajas, samas tähendab see seda, et iga muudatuse pealt küsitakse administraatori õigusi. Siiski on see variant parem, kui et osaliselt funktsioonid toimiks ning lisaks muudab see viirusetõrje turvalisemaks. Üldjoontes on viirusetõrje kasutamine mugav, kuna nii kontrolli kui uuendusi saan alustada ühe nupu vajutusega. Sama toimib ka töölaual, kus saan faile kontrollida hiire parema klahvi vajutuse alt. Kõikidele seadetele ligisaamine ei ole samuti raske, sest kõik seaded on ühes kohas. Samuti saab mugavalt seada automaatseid kontrolle kindlale kellaajale.

Eripärad

Alustan sellest, et viirusetõrjet ei saa muuta täisekraanisuuruseks. Kontrollimise juures saab muuta kiirust. Mida kiiremaks muuta, seda rohkem kasutab viirusetõrje arvuti ressursse ja seda vähem saab kasutaja sama ajal arvutis teha. Viirusetõrje kontrollid tunduvad uskumalt kiired, sest peale esimesi kontrollimisi väheneb aeg märgatavalt. Kui näiteks esimene kontroll kestis 10 minutit, mille jooksul kontrolliti 308 000 objekti, siis kolmandal korral võttis viirusetõrjel 308 000 objekti kontrollimine kõigest 2 minutit.

Katsetused

1. Kaks põhilist kontrollimise tüüpi

Custom scan ehk valikuline kontroll(kontrollisin Windowsi kausta) - Objekte: 67 878, Aeg: 00:00:59

Full scan ehk kõikide failide kontroll - Objekte: 312 545, Aeg: 00:15:12

2. Jälgisin ka kontrollide käigus protsessori kasutust(*CPU Usage*) ja protsessori maksimaalset sagedust(*Maximum Frequency*), mõlemaid 5 minutit, mille jooksul kogunes vähemalt 200 näitajat ning kirja läks tulemus, mida esines vähemalt viis korda. Testitaval arvutil on Intel(R) Pentium(R) CPU B960 @ 2.20GHz. Esimesena toon välja samad näitajad, kui viirusetõrje veel ei kontrollinud(*CPU Usage*: 2-6% ja *Maximum Frequency*: 36-43%). Kontrolli käigus esinesid järgnevad näitajad:

CPU Usage: 21-76%

Maximum Frequency: 59-98%

3. Et katsetada viirusetõrje käitumist, kui viirus satub süsteemi, kasutasin EICAR(*European Institute for Computer Anti-virus Research*) faile. Tegemist on failidega, kus esineb ainult üks rida teksti, mis peaks aga äratama iga viirusetõrje tähelepanu. Alla sai tõmmatud neli dokumenti: eicar.com, eicar.com.txt, eicar_com.zip ning eicarcom2.zip. Antud viirusetõrje puhul sai kõik failid alla laaditud töölauale. Käivitades faile, reageeris viirusetõrje ja eemaldas failid. (EICAR).

1.1.4 Avira Free Antivirus

Nõuded arvutile

Koduleht: http://www.avira.com/

Operatsioonisüsteem: MS Windows 10/8.1/8/7

Mälu: 1024 MB RAM

Protsessor: 1 GHz

Vaba ruumi vajadus kettal: 800 MB

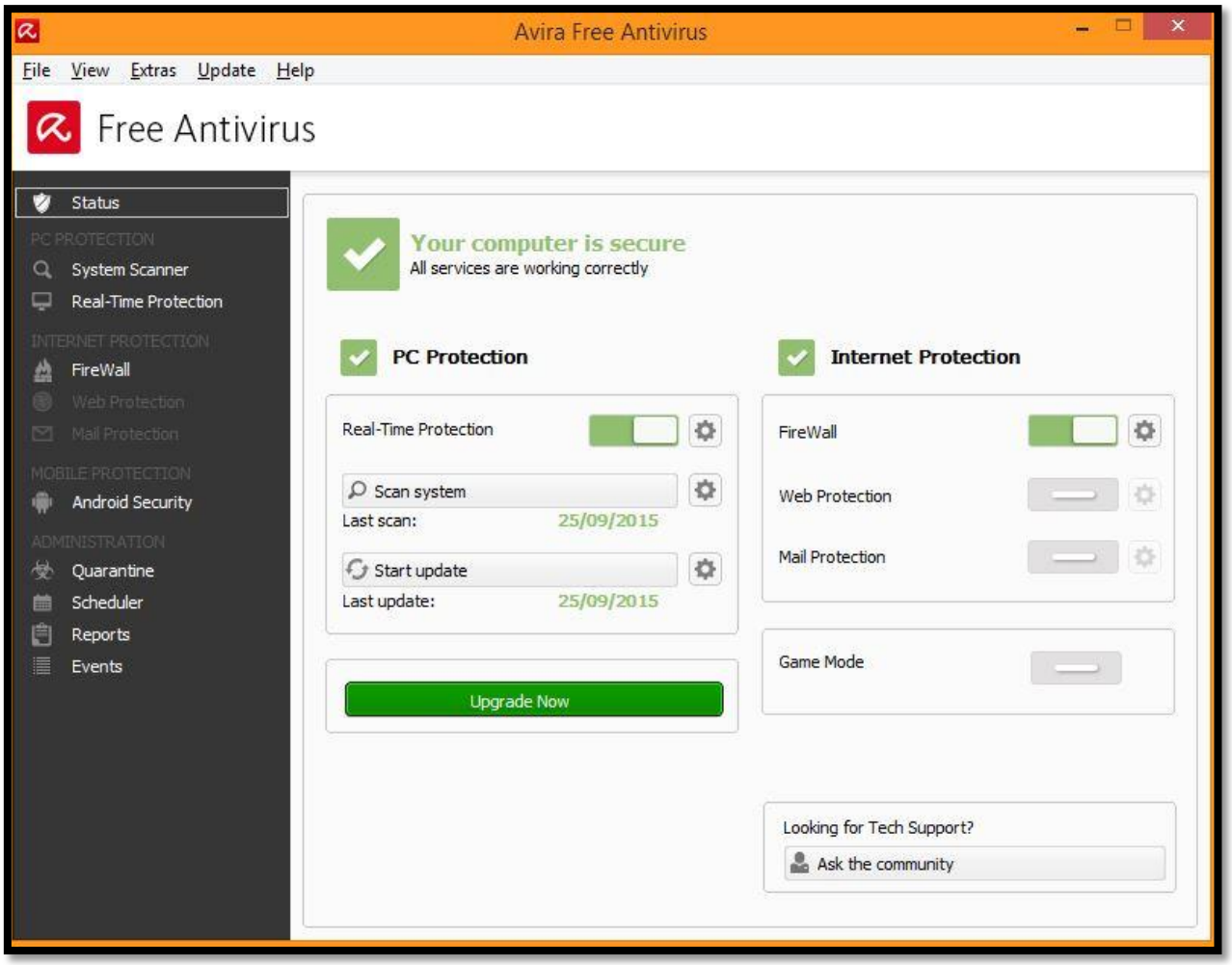
Lehitseja: Internet Explorer 8 või värksem (Avira).

Paigaldamine

Annab teada, et paigaldamine kestab 6-10 minutit. Saab võtta tasuta lisa oma lehitsejale. Nimeks on *Avira SafeSearch Plus*, mis aitab sildistada välja nakatunud leheküljed interneti otsingutel. See turvab kõiki kasutaja otsinguid ja seadakse ka sinu otsingumootoriks, kui sa otsustad selle paigaldada. Pakuti ka *Avira System Speedupi*, mis on tasuline ja seetõttu paigaldatakse prooviversioonina. Ta peaks aitama muuta arvutit kiiremaks ja suurendada jõudlust kirjade järgi. Veel pakutakse *Avira Mobile Security*. Tegu on nutitelefonide viirusetõrjega androidi ja apple kasutajatele. Kõigist neist mainitud lisadest on võimalik keelduda. Viirusetõrje avatakse läbi teise programmi, mis kannab nime *Avira Launcheri*. Tema alla kuhu kuulub teisigi funktsioone, mis kuuluvad aga tasulise versiooni juurde. (vt Pilt5)

Pilt5: Avira Launcher

Keele valiku kohta nii palju, et keelt kuskilt valida ei saanud paigaldades. Ka viirusetõrje seadetes ei leia kohta, kust saaks keelt valida. Viirusetõrje kodulehel natukene uurides tuleb välja, et viirusetõrjes sees keelt vahetada ei saagi. Et valida keelt, tuled viirusetõrje kodulehe keel muuta vastavalt samaks, mis keeles viirusetõrjet te oma süsteemi soovite paigaldada. Keele vahetamiseks tuleks seega vale keelega versioon eemaldada. Vahetada kodulehe keel, kusjuures võimalusi on 12 ja eesti keel valikusse ei kuulu. Ning sealt samalt kodulehelt viirusetõrje uuesti paigaldada.



Pilt6: Avira Free Antivirus

Kasutajaliides

Tasuta versioonis kasutatavad funktsioonid asuvad avaekraani vasakus ääres ja neid on üheksa. Esimene neist on *Status* ehk seisund, mis avaneb, kui avada viirusetõrje. Sealt on näha, kas kõik funktsioonid on sisse lülitatud, vajadusel saab muuta seadistust ja näha millal viimati nad aktiivsed olid. Samuti on siin nähtaval funktsioonid, mida tasuta versiooni puhul kasutada ei saa ja koht, kus saab uuendada tasulise versiooni peale. Lisaks saab ühe nupuvajutusega alustada nii failide kontrollimist kui ka uuendamise protsessi.

Järgmiseks on *System Scanner* ehk süsteemi kontroll. Siin saab algatada mitmeid erinevaid kontrolli tüüpe. Esimeseks neist on *Scan Local Drives* ehk kohalikud seadmed, mis kontrollib kõiki kõvakettaid, DVD-kettaid ja väliseid andmekandjaid. Teine tüüp on *Scan Local Hard Disks* ehk kohalikud kõvakettad. Kontrollib, kas kõvakettal on pahavara või kahtlaseid programme. Järgmiseks on *Scan Removable Drives* ehk eemaldatavad kettad, mis vaatab läbi

kõik eemaldatavad kettad teie süsteemis. Neljandaks on *Scan Windows System Directory* ehk MS Windowsi süsteemi kataloog ehk kausta *c:\windows\system32* kontroll. Viiendaks on *Full scan* ehk kõikide failide kontroll. Järgmisena *Quick scan* ehk kiire kontroll failidele ja kaustadele. Seitsmendana on mul võimalus kontrollida *Scan My Documents* ehk minu dokumentide kausta. Nüüd on *Scan active processes* kord, mis vaatab üle aktiivsed protsessid. Järgmisena on võimalik otsida peidetud tarkvara pakette, millega võib arvutisse pahavara paigaldada ehk *Scan for rootkits*. Viimaseks variandiks on *Custom scan* ehk kohandatud kontroll, mille abil saab kasutaja valida, mida ta tahab kontrollida ja mida mitte. Paremas üleval nurgas on võimalik seadeid muuta.

Kolmandaks on *Real-Time Protection* ehk reaalaja kaitse, kus kuvatakse viimane ohtlik fail või viirus, mis leitud on. Lisaks on seal nähtaval ka fail, mida viimati kontrolliti ja failide üldsumma, kui palju üldse siiamaani kontrollitud on. Seadete nupp asub endiselt paremas üleval nurgas.

Järjekorras neljas on *FireWall* ehk tulemüür. Siin näeb kinnitust, et MS Windowsi tulemüür toimib hetkel. Vajadusel on ta võimalik seadete alt välja lülitada, mida muidugi ei soovita mitte teha.

Viiendaks on *Android Security* ehk võimalus enda androidi peal töötavale mobiiltelefonile viirusetõrje alla laadida. See on üks tasuta funktsioonidest.

Quarantine ehk karantiin on järgmine. See on koht, kus hoitakse ohtlikke faile, mis võivavad sisaldada viiruseid. Neid puhastatakse võimalusel viirustest, et neid oleks võimalik hiljem taastada ja kasutada.

Järgmiseks on *Scheduler* ehk koht, kus saab automaatseid kontrolle seada.

Viimased kaks on omavahel seotud. Nendeks on *Reports* ehk aruanded ja *Events* ehk sündmused. Nimelt aruannete all näeme kõiki teostatud uuendusi ja kontrolle ainult. Sündmuste juures kohtame kõiki tegevusi, millega viirusetõrje hakkama on saanud, sealhulgas ka viimaseid uuendusi ja kontrolle. (vt Pilt6)

Kasutajamugavus

Tuleb öelda, et natukene häirib viirusetõrje avamise protsess. Kuna ma pean avama programmi, mille seest saan avada viirusetõrje. Kusjuures esimese programmi avamine toimub tunduvalt kiiremini, kui viirusetõrje enda. Kui nüüd rääkida viirusetõrjest, siis põhilised funktsioonid on olemas. Kasutada antud viirusetõrjet on lihtne, kuna tasuta asju saab ainult puutuda ja nende puhul on seadete muutmine tehtud lihtsaks, sest kõik asuvad ühes kohas. Kui avad ühe funtsiooni seaded, saad muuta kõigi funktsioonide seadeid. Ka tavakasutaja puhul toimib kõik, suuremate muudatuse sisse viimiseks küsitakse administraatori salasõna muidugi.

Eripärad

Esimestena meenub viirusetõrje avamisprotsess ja kontrollimise võimaluste paljusus. Samuti on viirusetõrje aknal taaskord kindel suurus. Salasõna seadmise võimalus, et kaitsta võõraid seadeid muutmast.

Katsetused

1. Kolm põhilist kontrollimise tüüpi

Quick scan ehk kiire kontroll - Objekte: 2582, Aeg: 00:00:29

Custom scan ehk valikuline kontroll(kontrollisin Windowsi kausta) - Objekte: 213 910, Aeg: 00:21:07

Full scan ehk kõikide failide kontroll - Objekte: 651 600, Aeg: 01:26:27

2. Jälgisin ka kontrollide käigus protsessori kasutust(*CPU Usage*) ja protsessori maksimaalset sagedust(*Maximum Frequency*), mõlemaid 5 minutit, mille jooksul kogunes vähemalt 200 näitajat ning kirja läks tulemus, mida esines vähemalt viis korda. Testitaval arvutil on Intel(R) Pentium(R) CPU B960 @ 2.20GHz. Esimesena toon välja samad näitajad, kui viirusetõrje veel ei kontrollinud(*CPU Usage*: 2-6% ja *Maximum Frequency*: 36-43%). Kontrolli käigus esinesid järgnevad näitajad:

CPU Usage: 11-41%

Maximum Frequency: 59-98%

3. Et katsetada viirusetõrje käitumist, kui viirus satub süsteemi, kasutasin EICAR(*European Institute for Computer Anti-virus Research*) faile. Tegemist on failidega, kus esineb ainult üks rida teksti, mis peaks aga äratama iga viirusetõrje tähelepanu. Alla sai tõmmatud neli dokumenti: eicar.com, eicar.com.txt, eicar_com.zip ning eicarcom2.zip. Esimesed kaks faili eemaldas juba allalaadimise käigus. Kolmanda faili laadis töölauale ära, aga kohe sooviti see ka eemaldada. Neljas fail sai alla laaditud ja lahti pakitud, peale mida avastati lahti pakitud failist viirus, mis seejärel eemaldati, aga algne fail jääb töölauale alles. Peale eemaldamist sooritatakse automaatselt kiire kontroll. (EICAR).

1.1.5 Comodo Antivirus

Nõuded arvutile

Koduleht: https://www.comodo.com

1. Operatsioonisüsteem: MS Windows XP S2 või uuem

Mälu: 152 MB RAM

Vaba ruumi vajadus kettal: 400 MB

2. Operatsioonisüsteem: Linux Ubuntu 12.04/Red Hat Enterprise Linux Server 5.9, 6.3/Fedora 17/SUSE Linux Enterprise Server 11/OpenSUSE Linux 12.1/Debian 6.0/CentOS 5.9, 6.2/Mint 13/CentOS 5.8, 6.2

Protsessor: 2 GHz

Mälu: 2 GB RAM

Vaba ruumi vajadus kettal: 40 GB

3. Operatsioonisüsteem: Mac OS X 10.4/10.5/10.6

Protsessor: Mac Intel i386/x86_64 (Comodo).

Paigaldamine

Kõigepeal peaks ära mainima, et paigaldatav fail on ulmeliselt suur, võrreldes eelmiste viirusetõrjetega. Nimelt tervelt 215 MB suurune. Paigaldamine algab keele valikuga, kus on 25 erineva võimaliku seast tuleb valida endale see õige. Eesti keel on esindatud. Liikudes edasi soovitakse saada e-maili, mis on valikuline. Veel küsitakse nõusolekut info saatmiseks tootjale seoses viirusetõrje kasutamisega ja tundmatute programmide saatmist analüüsimiseks, millest saab samuti loobuda. Järgnevalt andakse teada, et koos viirusetõrjega tuleb uus lehitseja. Antud lehitseja tahetakse seada peamiseks lehitsejaks ning soovitakse seaded ja otseteed üle kanda teie poolt kasutavatest lehitsejatest. Lisaks tahetakse seada veebilehitseja avaleheks *Yahoo*, kui linnukest ei eemalda. Töölauale ongi tekkinud peale paigaldamist lisaks viirusetõrje veel uus lehitseja *Chromodo* ja programm *GeekBuddy*, kuhu saab probleemide tekkimisel pöörduda. Esimesel käivitamisel soovib uuendust, mis võtab päris pikalt aega, seda seetõttu, et failis suurus on 244 MB. Peale seda veel taaskäivitus arvutile. Kui ei soovi peale viirusetõrje mitte midagi muud paigaldada, siis on see võimalus olemas kohandatud paigaldusega. Antud valik asub vasakus all nurgas. Peale komponentide valiku saab valida koha, kuhu kogu programm paigaldatakse.

Pilt7: Comodo Antivirus

Kasutajaliides

Avades viirusetõrje näeme, kas arvuti on hetkel turvaline. Lisaks saame ühe nupuvajutusega sisse lülitada *Game Mode* ehk mängu reziimi, kus viirusetõrje peaks otseses mõttes tagasi tõmbama, et lasta mängul puhtamalt joosta ja kasutada ressursse. See kõik on vasakul. Paremal pool näeb kui palju ohte on eemaldatud, millal viimati uuendati ja mitu sissetungi on peatatud. Avalehe alumises reas asub viis funktsiooni. Esimesega neist saab alustada nelja erinevat tüüpi kontrolle ja lisaks veel seadeid muuta vajadusel. Esimene tüüp on *Quick Scan* ehk kiire kontroll, mis kontrollib sagedasti nakatuvaid piirkondi ja mälu. Järgmiseks tüübiks on *Full Scan* ehk kõikide failide kontroll. Kolmandaks on midagi uut, selleks on *Rating Scan*, mis kujutab endast pilve kõige sagedamini nakatunud piirkondade kontrolli. Viimaseks tüübiks on *Custom Scan* ehk kohandatud kontroll, millega kasutaja saab ise valida millist faili või kausta kontrollida tahetakse. All reas edasi liikudes on järgmiseks *Update*, millega saab alustada uuendamis protsessi viirusetõrjes või vähemalt kontrollida, kas ta jookseb uusima versiooni peal. Järgmiseks on uus ja huvitav funktsioon, mida siiani pole teiste viirusetõrjetes kohanud. Selleks on *Virtual*

Desktop ehk virtuaalne töölaud, mis loob turvalisema töölaua kasutaja arvutist. Neljandaks on *View Qurantine*, millega saab pilgu heita sellele, mis karantiinis hetkel toimub. Viimaseks reas on *Get Live Support* ehk koht, kus saada abi probleemide lahendamisel. Vajutades üleval paremalt nuppu *Tasks* ehk ülesanded, näeme funktsioone, mis avalehel kuvatud pole. Näiteks *Sandbox* ehk liivakast, kus saab käivitada programme, mille puhtuses kindlad väga pole. Kui käivitada eeldatavalt viirustega nakatunud programm liivakastis, siis käivitatakse antud programm lavastatud keskkonnas. See tähendab, et kui sealt leidakse viiruseid, siis teie arvuti süsteemi nad ei pääse ning lavastatud keskkonna sulgemisega kaovad ka viirused. Samuti saab luua päästeketta. Avalehe kompaktsest vaatest saab luua täpsema vaate, selleks tuleb vajutada ülevalt vasakult väikest kastikest. Selle tulemusel näeme rohkemate funktsioonide toimimist ja saame siia faile tõsta, et neid kontrollida. (vt Pilt7)

Kasutajamugavus

Mugavuse kohapealt tundub olevalt igati hästi ja loogiliselt üles ehitatud viirusetõrje, kus funktsioone leidub piisavalt. Rohkem kasutatavad funktsioonid on avalehel kiiresti käivitatavad. Samuti on mugav lisa antud viirusetõrje juures see, et viirusetõrjest väiksem versioon jookseb koguaeg töölaual, kus saab käivitada põhilisi funktsioone. Lisaks saab seda panna ükskõik kuhu töölaual ning samas saab selle seadete all üldse ära kaotada. (vt Pilt8)

Pilt8: Comodo Antivirus

Eripärad

Alustangi siinkohal selle lisa nimetamisega, mida mainitud sai eelmises lõigus. Liivakasti olemasolu on kindlasti suureks plussiks, sest nagu töölaual saab faile kontrollida, saab neid ka käivitada liivakastis. Samuti saab viirusetõrjele seada salasõna. Mängimise režiimi mainiks ka ära. Kahjuks ei saa viirusetõrje avalehte suuremaks ega väiksemaks muuta. Automaatseid kontrolle saab seada, aga need seaded olid esmapilgul nii ära peidetud. Viirusetõrjega tuli kaasa oma lehitseja ja programmike, kus saab abi küsida probleemide korral. Virtuaalne tööölaud tasub ka siinkohal äramärkimist. Reklaami rohkuse üle ei saa ka kurta.

Katsetused

1. Kolm põhilist kontrollimise tüüpi

Quick scan ehk kiire kontroll - Objekte: 23 399, Aeg: 00:00:10

Custom scan ehk valikuline kontroll(kontrollisin Windowsi kausta) - Objekte: 98 205, Aeg: 00:19:42

Full scan ehk kõikide failide kontroll - Objekte: 277 017, Aeg: 00:33:18

2. Jälgisin ka kontrollide käigus protsessori kasutust(*CPU Usage*) ja protsessori maksimaalset sagedust(*Maximum Frequency*), mõlemaid 5 minutit, mille jooksul kogunes vähemalt 200 näitajat ning kirja läks tulemus, mida esines vähemalt viis korda. Testitaval arvutil on Intel(R) Pentium(R) CPU B960 @ 2.20GHz. Esimesena toon välja samad näitajad, kui viirusetõrje veel ei kontrollinud(*CPU Usage*: 2-6% ja *Maximum Frequency*: 36-43%). Kontrolli käigus esinesid järgnevad näitajad:

CPU Usage: 15-99%

Maximum Frequency: 37-98%

3. Et katsetada viirusetõrje käitumist, kui viirus satub süsteemi, kasutasin EICAR(*European Institute for Computer Anti-virus Research*) faile. Tegemist on failidega, kus esineb ainult üks rida teksti, mis peaks aga äratama iga viirusetõrje tähelepanu. Alla sai tõmmatud neli dokumenti: eicar.com, eicar.com.txt, eicar_com.zip ning eicarcom2.zip. Failid laaditi töölauale, aga neid

avades, väideti et avatav fail on tühi ehk ohtlik sisu on juba eemaldatud. Viimase faili puhul tühjendati sisu peale lahti pakkimist. (EICAR).

1.1.6 Malwarebytes Anti-Malware (Free)

Nõuded arvutile

Koduleht: http://www.malwarebytes.org/

Operatsioonisüsteem: MS Windows 10/8.1/8/7/Vista/XP

Mälu: 1024 MB RAM(256 MB MS Windows XP)

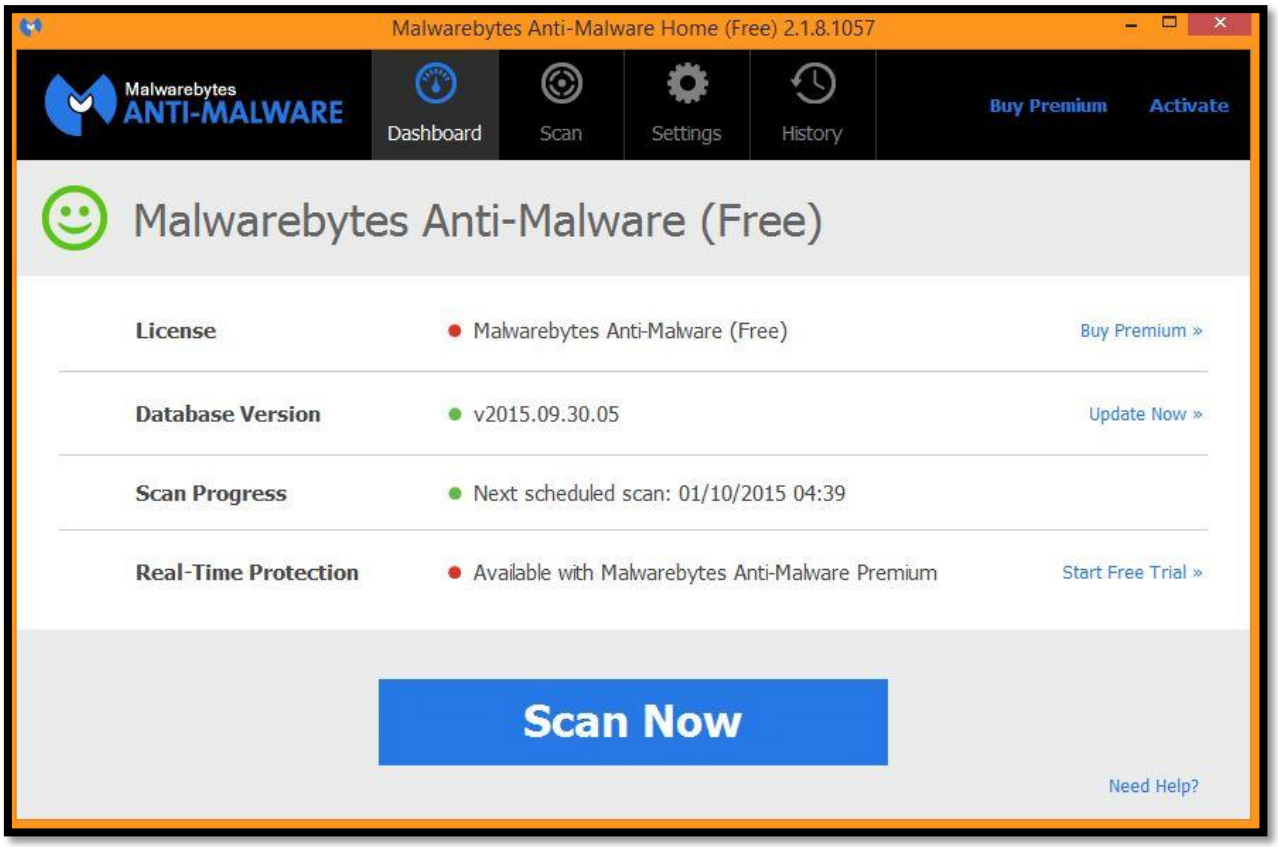
Protsessor: 800 MHz

Lehitseja: Internet Explorer 6 või uuem

Vaba ruumi vajadus kettal: 20 MB (Malwarebytes Anti-Malware).

Paigaldamine

Paigaldamine algab keele valikuga. Valikus on 33 keelt, kuhu kuulub ka eesti keel. Järgmiseks nõustume litsentsiga. Liikudes edasi annab võimaluse muuta paigaldamise asukohta. Soovitakse luua start menüü alla otsetee. Järgneb sarnane soov, aga nüüd juba töölauale. Kuvatakse kokkuvõte valikutest ja asutakse paigaldama. Pakutakse veel tasulist versiooni 30 päevaks. Esimesel käivitamisel kontrollitakse andmebaasi ja seejärel uuendadakse seda. Peale esimest failide kontrolli, paneb viirusetõrje järgmise kontrolli paika järgmiseks päevaks. Kuna viirusetõrje ei ilmu olekualale ikoonina ega jää seal töötama, siis sulgemisel ja uuesti avamisel kaob järgmise päeva kontrolli aeg ja mingit kontrolli järgmisel päeval ei toimu. Sama asi juhtub, kui vahetada viirusetõrje keelt. Et järgmisel päeval kontroll ikka sooritataks, peab viirusetõrje olema koguaeg tegumiribal ja arvuti töötama sellel kellaajal. Kui arvutit juhuslikult samal ajal ei kasutatud, nullitakse aeg ja uue kontrolli peab algatama kasutaja manuaalselt.



Pilt9: Malwarebytes Anti-Malware (Free)

Kasutajaliides

Töökeskkond on jagatud nelja kasti vahel. Kõik neli kasti asuvad viirusetõrje ülemises osas. Lisaks neile saab sealt osta tasulise versiooni (*Buy Premium*) või koodi olemasolul selle aktiveerida (*Activate*). Esimene neist kastidest on *Dashboard* ehk avaleht. Avalehe alumises osas saab algatada kontrolli failidele (*Scan Now*). Avalehe keskelt saab välja lugeda, mis litsentsiga on antud viirusetõrje puhul tegemist (*Licence*). Vajadusel saab tasuta versiooni tasuliseks uuendada. Lisaks näeme, mis andmebaasi versiooni peal oleme (*Database version*) ning kontrollimise edenemist (*Scan Progress*). Kui kontrolli pole toimunud, ollakse järgmise kontrolli ootel. Kui kontroll on toimunud, määratakse järgmise kontrolli toimimise aeg. Viimaseks näeme, et püsikaitse ehk *Real-Time Protection* ei kuulu tasuta versiooni funktsioonide hulka.

Teiseks osaks on *Scan* ehk kontroll. Antud viirusetõrjel on kolm erinevat kontrollimise tüüpi. Nendest kaks on kasutatavad tasuta versiooni juures. Kolmas kuulub tasulise juurde. Kahest toimivast esimene on *Threat Scan* ehk ohtude kontroll. Kontrollib pahavara teadatuntud kohtadest. Näiteks mälust, käivituskohtadest, registritest ja failisüsteemi objektidest. Teiseks

tüübiks on *Custom Scan* ehk valikuline kontroll. Siinpuhul on võimalik kasutajal valida, mida ta kontrollida soovib.

Kolmandaks on *Settings* ehk Seaded. Seadete all kohtab samuti tasulise viirusetõrje alla kuuluvaid funktsioone. Tasuta versiooni puhul saame muuta põhilisi seadeid ehk *General Settings*. Siin all saame muuta ka viirusetõrje keelt. Lisaks saame teavitused välja lülitada või kontrollida ajaliselt, kui kiiresti nad sulguvad. Järgmiseks on *Malware Exclusions* ehk erandid, kuhu saame lisada faile ja kaustu, mida viirusetõrje ei pea kontrollima. *Detection and Protection* ehk tuvastamine ja kaitse on järgmine. Saame muuta tuvastamise valikuid, määrates ära, mida kontrollida ja mida mitte ning määrata ära, mida tehakse kui leitakse soovimatu tarkvara või soovimatu muudatus. Neljandana saame muuta *Update Settings* ehk uuendamise seadeid. Siin juhul saame määrata, kui mitme päeva tagant teavitatakse andmebaasi uuendusest ning seada viirusetõrje andmebaasi uuendamise ajal ka programmiuuendusi otsima. Viiendaks on *History Settings* ehk ajaloo seaded, kus saab määrata, kas kontroll-logid salvestatakse kettale või mitte ning määrata salvestamise asukoht. Veel saame lugeda teavet antud viirusetõrje kohta (*About*).

Viimaseks jupiks on *History* ehk ajalugu. Siin asub *Quarantine* ehk karantiin, kuhu suunatakse kõik pahavara, mis leidakse. Lisaks asub ajaloo all ka rakenduste logid ehk *Application Logs*, kuhu tekkivad igapäevased kaitselogid koos kontrollimiste kokkuvõtetega. (vt Pilt9)

Kasutajamugavus

Programm on kergesti kasutatav, kuna nii funktsioone kui seadeid mida muuta on vähe. Tähtsamad seaded ja nende muutmine kuuluvad tasulise versiooni alla. Kasutajana pean iga kord manuaalselt käivitama nii viirusetõrje kui kontrollimised ning kontrollid toimuvad igapäevaselt vaid siis, kui viirusetõrjet vahepeal kinni ei panda ega keelt muudeta. Siiski kui kasutaja ei ole arvutis kontrollimise ajal, siis kontrolli ei toimu, aga vähemalt viirusetõrje enda uuendusi kontrollib igapäevaselt.

Eripärad

Siiamaani ainuke viirusetõrje, mida saab muuta täisekraani suuruseks. Püsikaitse ja kontrollide automatiseerimine ajaliselt ei kuulu priivaralise versiooni juurde. Samuti ei saa muuta täpsemaid seadeid, mille alla kuulub näiteks viirusetõrje käivitamine koos arvutiga. Kontroll algab andmebaasi uuenduste otsimisega. Kui siiamaani oli MS Windows Defender end automaatselt välja lülitatud samal ajal kui teine viirusetõrje tegeles pahavaraga, siis antud viirusetõrje puhul see nii ei ole. Töölaualt ei saa faile kontrollida parema hiire klahvi alt.

Katsetused

1. Kaks põhilist kontrollimise tüüpi

Threat scan ehk ohtude kontroll - Objekte: 382 510, Aeg: 00:36:40

Custom scan ehk valikuline kontroll(kontrollisin Windowsi kausta) - Objekte: 496 456, Aeg: 01:29:37

2. Jälgisin ka kontrollide käigus protsessori kasutust(*CPU Usage*) ja protsessori maksimaalset sagedust(*Maximum Frequency*), mõlemaid 5 minutit, mille jooksul kogunes vähemalt 200 näitajat ning kirja läks tulemus, mida esines vähemalt viis korda. Testitaval arvutil on Intel(R) Pentium(R) CPU B960 @ 2.20GHz. Esimesena toon välja samad näitajad, kui viirusetõrje veel ei kontrollinud(*CPU Usage*: 2-6% ja *Maximum Frequency*: 36-43%). Kontrolli käigus esinesid järgnevad näitajad:

CPU Usage: 10-39%

Maximum Frequency: 38-98%

3. Et katsetada viirusetõrje käitumist, kui viirus satub süsteemi, kasutasin EICAR(*European Institute for Computer Anti-virus Research*) faile. Tegemist on failidega, kus esineb ainult üks rida teksti, mis peaks aga äratama iga viirusetõrje tähelepanu. Alla sai tõmmatud neli dokumenti: eicar.com, eicar.com.txt, eicar_com.zip ning eicarcom2.zip. Viirusetõrje ei reageerinud ja kõik failid jäid töölauale. Sai käivitada ja lahti pakkida, viirusetõrje poolt endiselt mitte mingit tegutsemist. (EICAR).

1.1.7 Panda Free Antivirus

Nõuded arvutile

Koduleht: http://www.pandasecurity.com/

1. Operatsioonisüsteem: MS Windows 10/8.1/8/7/Vista/XP SP2 või uuem, Mac OS X 10.6.x kuni 10.10 (Yosemite)/iOS 6 ja uuem, Linux Fedora 19,20 ja 21/CentOS 6, 7/Debian 7, 8/Ubuntu 12,13,14 ja 15

Mälu: 256 MB RAM

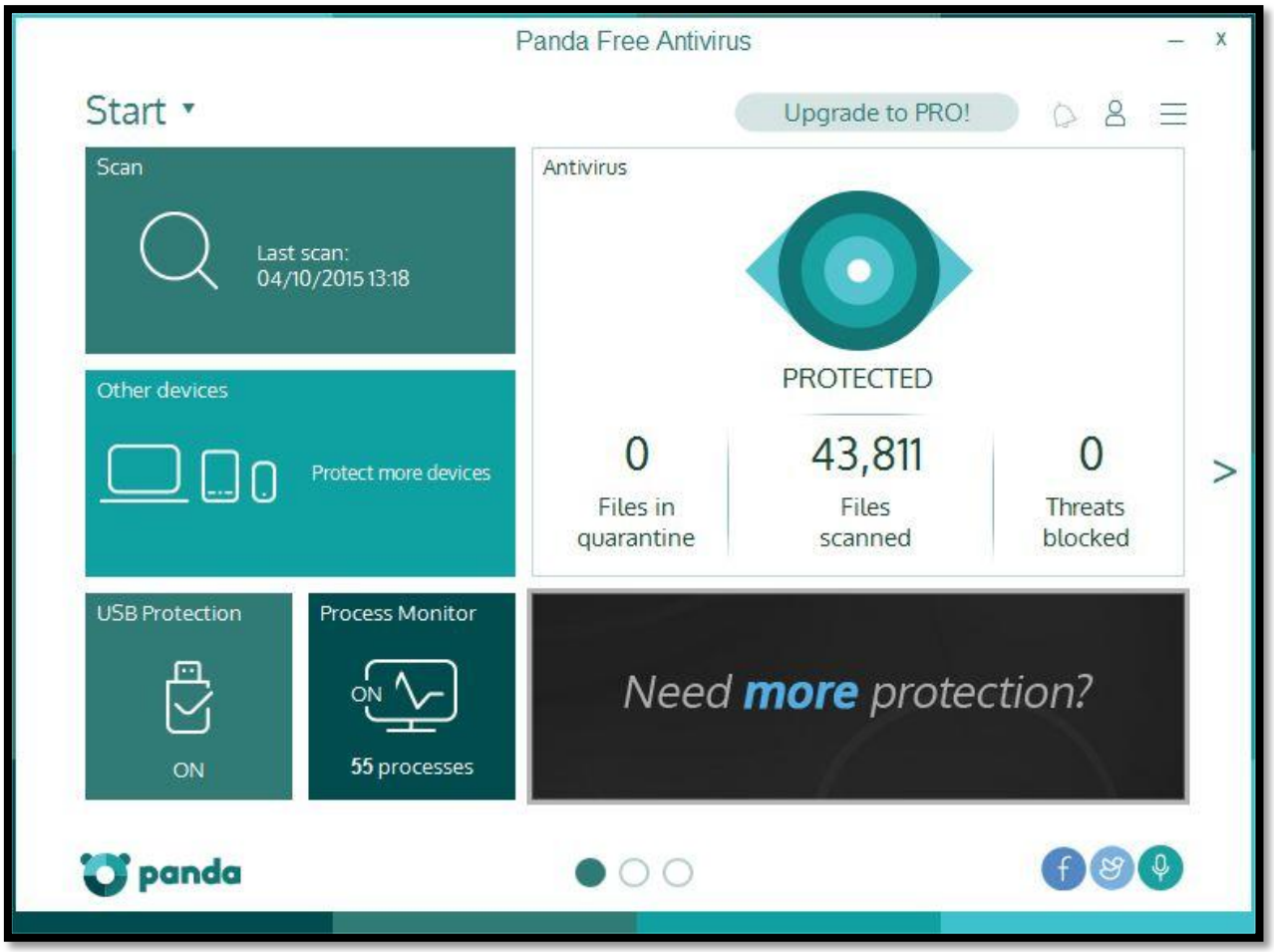
Protsessor: 800 MHz või kõrgem

Vaba ruumi vajadus kettal: 1 GB

2. Operatsioonisüsteem: Android 2.3.3 (Panda Free Antivirus).

Paigaldamine

Kõige esimesena pean valima koha, kuhu antud toode paigaldatakse. Järgneb keele valik, kuhu kuulub 22 keelt, eesti keel aga mitte. Lisaks soovitakse paigaldada *Panda Security Toolbar*, mis peaks aitama mind pahatahtlike veebilehtede vastu. Samuti soovib ta seada *Yahoo* põhiliseks otsingumootoriks ning lehitseja avaleheks. Linnukeste eemaldamisega seda ei juhtu. Enne paigaldamist nõustun veel litsentsilepinguga. Annab võimaluse valida tasuta versiooni või tasulise 30 päeva prooviversiooni vahel. Peale paigaldamist tahab kasutaja loomist. Tegin kasutaja ära. Sisse logides näen ära, millist toodet kasutan ja koodi olemasolul saan uuendada tasuliseks. Samuti saan osta tasulist versiooni. Priivaralise litsentsi kehtivuseks loen välja 9000 päeva.



Pilt10: Panda Free Antivirus

Kasutajaliides

Töökeskkond natukene sarnaneb MS Windowsi viimaste versioonide start menüüga. Antud viirusetõrje avalehel on 6 kastikest. Neist esimene on *Scan* ehk kontroll. Tema sisse on kuvatud viimase kontrolli toimumise aeg. Temale hiirega klõpsides saame käivitada sealt kolme tüüpi kontrolle. Esimene neist on *Full scan* ehk kõigi failide kontroll. Teine kannab nime *Critical areas* ehk kriitliste alade kontroll, mis vaatab üle mälu, hetkel jooksvad protsessid ja küpsised, otsides aktiivseid viiruseid arvutist. Selle kontrolli pikkus on lühike, jäädes mõne minuti piiridesse. Kolmandaks tüübiks on *Custom scan* ehk valikuline kontroll, kus kasutaja saab ise valida, millist faili või kausta kontrollida soovitakse.

Liikudes vasakult paremale, näeme töölaua suurimat kasti. Kannab ta üldnime *Antivirus* ehk viirusetõrje. Tema pealt on näha, mitu faili on hetkel karantiinis. Lisaks veel kui palju faile on kontrollitud ning mitu ohtu on blokeeritud. Kastile hiirega vajutades ilmub uus leht, kus saame

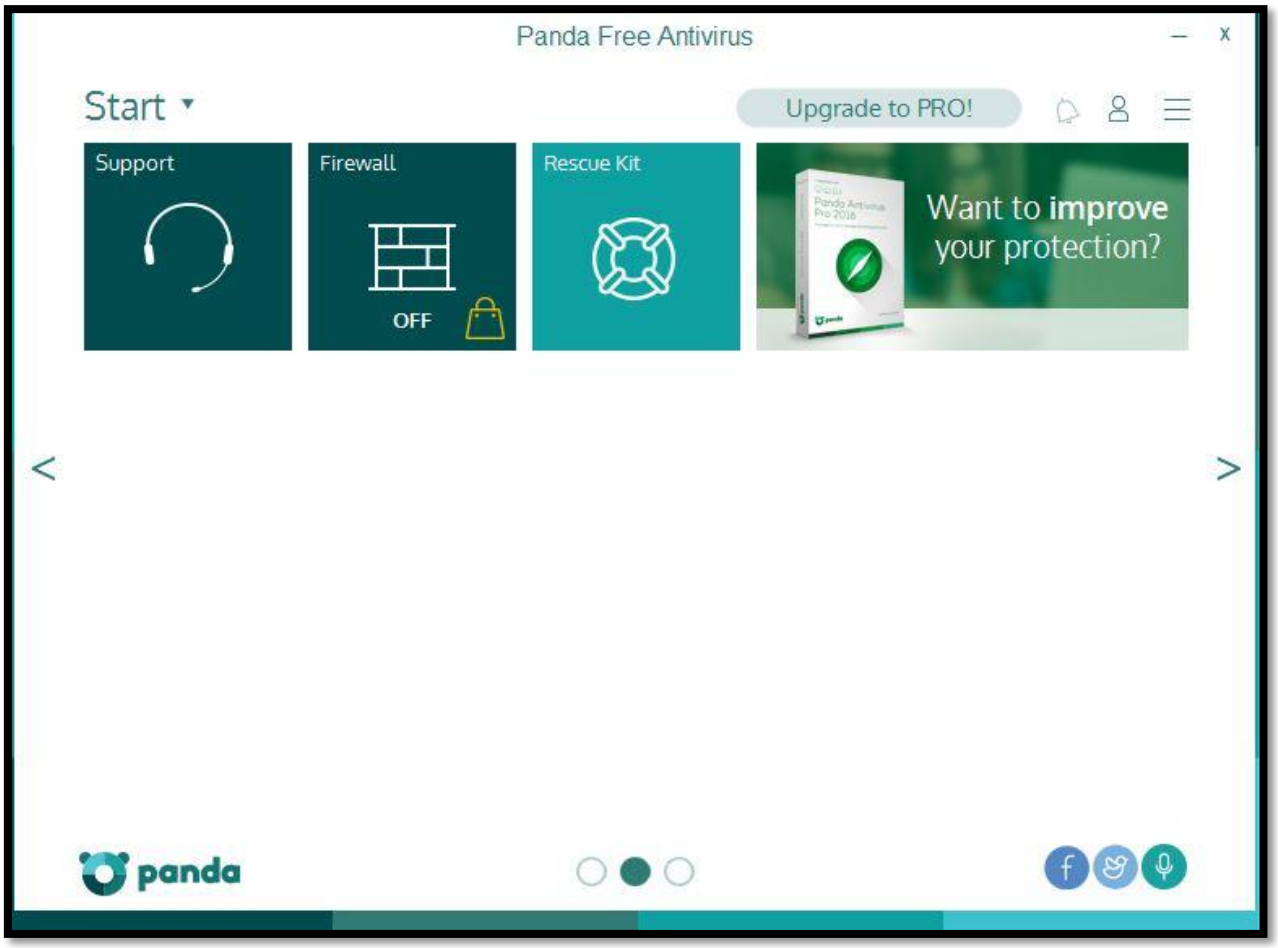
algatada kontrolli, viirusetõrje vajadusel välja lülitada, karantiini vaadata ning automaatseid kontrolle seada. Lisaks näeme ka sündmuste kokkuvõtet ning saame seadeid muuta.

Liikudes tagasi vasakule, kohtame kastikest nimega *Other devices* ehk teised seadmed. Teiste seadmete all mõeldakse tasuta viirusetõrjet android ja apple tarkvaral töötavatele telefonidele ja mac operatsioonisüsteemil töötavat arvutit.

Jätkame alumisest reast vasakult kus asub kastike nimega *USB Protection* ehk USB kaitse. See funktsioon aitab kontrollida ükskõik millist seadet, mis ühendatakse arvutiga läbi USB otsa. Vajutades kastile saate muuta seadeid. Näiteks saate selle funktsiooni välja lülitada vajadusel või paika panna selle, kas iga USB otsaga seadet peab kindlasti kontrollima automaatselt.

Liikudes järgmise kasti juurde, milleks on *Process Monitor* ehk koht, kus saab aktiivseid protsesse jälgida. Kastil kuvatakse hetkel aktiivsete protsesside arv ning vajutades ilmuvad nad teie ette. Seadete alt saate sellegi funktsiooni välja lülitada, kui seda peaks vaja olema.

Viimaseks kastiks on reklaam, mille peale vajutades suunab ta meid tasuliste versioonide valiku juurde. (vt Pilt10)



Pilt11: Panda Free Antivirus

Järgmisel lehel on veel neli kastikest, millest kaks kuuluvad tasuta versiooni juurde. Esimene neist on *Support* ehk kus peaks saama abi probleemide korral. Abi saamiseks on kaks võimalust. Neist esimene on viirusetõrje foorum, kuhu saab oma probleemiga pöörduda, kus moderaatorid või teised viirusetõrje kasutajad sulle vastavad. Foorumisse pead registreerima uue kasutaja, seda muidugi turvalisuse tõttu. Teine võimalus on saada kontakti tehnilise toega, mis kuulub tasulise versiooni juurde muidugi.

Teine toimiv funktsioon on *Rescue Kit* ehk päästerõngas. Siin saab luua puhta koopia oma süsteemist USB kettale. Kui viirus on sattunud süsteemi, saad oma USB ketta pealt käivitada puhta süsteemi. Lisafunktsioonina saab alla laadida *Panda Cloud Cleaner-i*, mis otsib viiruseid, mida traditsionaalne viiruse kontroll ei suuda tuvastada. Antud lisa peab alla laadima eraldi, et ta saaks kontrollimisega alustada.

Lisaks on teisel lehel välja toodud tasulise viirusetõrje funktsioon nimega *Firewall* ehk tulemüür ja veel üks reklaam, mis suunab sind tasulist ostma. (vt Pilt11)

Kasutajamugavus

Vajalikud funktsioonid on enamuses olemas. Töötab sujuvalt, ilma et raiskaks liigselt ressurse. Väljanägemine silmasõbralik ning funktsioone saab enda järgi seada, kui ei meeldi praegune paigutus. Automatiseeritud kontrollid sooritatakse tagaplaanil ja tulemused kuvatakse siis, kui midagi ohtlikku on leitud. Kui kõik on korras, siis tulemusi ette ei kuvata, kuid kui kasutaja soovib, saab ta sündmustest järele vaadata.

Eripärad

Viirusetõrjet ei saa täisekraani suuruseks teha. Töölaual saab kiiresti faile kontrollida hiire parema klahvi alt. Automaatselt käivituvate kontrollide seadmine olemas. Viirusetõrjele salasõna peale panemise võimalus. Mänguri reziim aktiveerub automaatselt, kui mingi programm jookseb täis ekraanil. Uudiste teavitamist saab välja lülitada. On olemas pood, kus saab tasulisele versioonile uuendada.

Katsetused

1. Kolm põhilist kontrollimise tüüpi

Critical areas ehk kriiliste alade kontroll - Objekte: 55 913, Aeg: 00:05:00

Custom scan ehk valikuline kontroll(kontrollisin Windowsi kausta) - Objekte: 455 266, Aeg: 00:34:00

Full scan ehk kõikide failide kontroll - Objekte: 1 059 769, Aeg: 01:40:00

2. Jälgisin ka kontrollide käigus protsessori kasutust(*CPU Usage*) ja protsessori maksimaalset sagedust(*Maximum Frequency*), mõlemaid 5 minutit, mille jooksul kogunes vähemalt 200 näitajat ning kirja läks tulemus, mida esines vähemalt viis korda. Testitaval arvutil on Intel(R) Pentium(R) CPU B960 @ 2.20GHz. Esimesena toon välja samad näitajad, kui viirusetõrje veel ei kontrollinud(*CPU Usage*: 2-6% ja *Maximum Frequency*: 36-43%). Kontrolli käigus esinesid järgnevad näitajad:

CPU Usage: 40-62%

Maximum Frequency: 46-98%

3. Et katsetada viirusetõrje käitumist, kui viirus satub süsteemi, kasutasin EICAR(*European Institute for Computer Anti-virus Research*) faile. Tegemist on failidega, kus esineb ainult üks rida teksti, mis peaks aga äratama iga viirusetõrje tähelepanu. Alla sai tõmmatud neli dokumenti: eicar.com, eicar.com.txt, eicar_com.zip ning eicarcom2.zip. Neist esimese ja kaks viimast suunatakse kohe karantiini, ilma, et ma saaks neid avada. Teise faili puhul muutes faililaiendit, leiab ka selle koheselt karantiinist. Esialgse faililaiendiga sain ma faili avada. (EICAR).

2. Võrdluse tulemused

Selleks, et lihtsustada tasuta viirustõrjete võrdlemist, koostas autor tabeli (vt Tabel1). See tabel annab lihtsa ülevaate sellest, millised funktsioonid viirusetõrjel olemas on ja millised mitte.

Tabel1: Funktsioonide võrdlus

Programm/ Funktsioon	360 Total Security	Avast	AVG	Avira	Comodo	Malwar ebytes	Panda
Full Scan/Täielik kontroll	Olemas	Olemas	Olemas	Olemas	Olemas	-	Olemas
Quick Scan/Kiire kontroll	Olemas	Olemas	-	Olemas	Olemas	Olemas	Olemas
Custom Scan/Valikuline kontroll	Olemas	Olemas	Olemas	Olemas	Olemas	Olemas	Olemas
Scheduled Scan/Plaanitud kontroll	Olemas	Olemas	Olemas	Olemas	Olemas	-	Olemas
Real-Time Protection/Püsikaitse	Olemas	Olemas	Olemas	Olemas	Olemas	-	Olemas
Firewall/Tulemüür	Olemas	-	-	Olemas	-	-	-
Rescue Kit/Päästerõngas	-	Olemas	-	-	Olemas	-	Olemas
WiFi Security Check/Traadita võrgu turvalisuse kontroll	Olemas	Olemas	-	-	-	-	-
Game mode/Mänguri reziim	-	-	-	-	Olemas	-	Olemas
Sandbox/Liivakast	Olemas	-	-	-	Olemas	-	-
USB Protection/USB kaitse	Olemas	-	-	-	-	-	Olemas
Estonian Languaeg/Eesti keel	-	Olemas	-	-	Olemas	Olemas	-
Account dont need to create/Kasutajat ei ole vaja luua	Kasutaja ei ole vaja	Kasutaja on vaja luua	Kasutaja ei ole vaja	Kasutaja ei ole vaja	Kasutaja ei ole vaja	Kasutaja ei ole vaja	Kasutaja on vaja luua

Kokkuvõte

Käesoleva seminaritöö eesmärgiks oli tutvustada ning anda ülevaade tasuta viirusetõrjetest ning olulisematest nendega seotud omadustest. Samuti anda enda poolt objektiivne vastukaja. Lisaks sai ära seletatud mõningad mõisted ja jagatud soovitusi oma arvuti turvalisemaks muutmiseks ja kasutamiseks.

Autor alustuseks seletas tähtsaimad mõisted, mis asuvad lisas. Seejärel sai valitud välja need seitse priivaralist viirusetõrjet, mida katsetama hakatakse. Järgmiseks võrreldi katsealuseid kindlate funktsioonide alusel ning lõpuks koondati nõuanded, kuidas kaitsta oma arvutit viiruste eest. Nõuanded leiab samuti lisast. Tulemuseks on, et võrreldud programmidest keegi ei omanud kõiki funktsioone, mille autor oli püstitanud. Siiski nelja viirusetõrje funktsioonide listiga võib rahule jääda. Ülejäänutel oli juba liigselt puudusi, et neid esile tõsta. Lisaks tuleb ära mainida, et leidus üllatavaid funktsioone tasuta viirusetõrjetel, mis muudavad arvuti veel turvalisemaks.

Antud töö on suunatud eelkõige inimestele, kes kasutavad ja omavad arvutit ning soovivad end kaitsta viiruste eest valides endale selle õige viirusetõrje, mis antud töö puhul on tasuta kättesaadav.

Kasutatud kirjandus

360totalsecurity. (2015). What are the minimum system requirements of 360 Total Security? Loetud 14.09.2015 aadressil http://www.360totalsecurity.com/.

Avast. (2015). Minimum System Requirements. Loetud 17.09.2015 aadressil https://www.avast.com/.

AVG. (2015). System Requirements. Loetud 21.09.2015 aadressil http://www.avg.com/eu-en/homepage.

Avira. (2015). What are the minimum system requirements for an Avira product? Loetud 25.09.2015 aadressil http://www.avira.com/en/avira-free-antivirus.

Comodo. (2015). System Requirements. Loetud 27.09.2015 aadressil https://www.comodo.com.

Malwarebytes Anti-Malware. (2015). Tech Specs. Loetud 30.09.2015 aadressil http://www.malwarebytes.org/.

Panda Free Antivirus. (2015). Technical Requirements. Loetud 03.10.2015 aadressil http://www.pandasecurity.com/homeusers/solutions/free-antivirus/.

Kirna, A. (2009). *Arvutikaitse ABC*. Tallin: Vaata Maailma.

Vabar, M. (2004). *Igamehe arvuti-turvaja: käsiraamat Windows-arvuti Interneti-kindlaks muutmiseks ja tasuta tarkvara selleks otstarbeks.* Tallinn: M. Vabar.

Arvutikaitse. (2015). Kuidas muuta oma arvuti turvalisemaks? Loetud 01.09.2015 aadressil http://www.arvutikaitse.ee/.

Semper, A., Liikane, L. (2000). *Inglise-eesti-inglise seletav arvutisõnastik.* Tallinn: Estada Kirjastus.

Vallaste. (2015). e-teatmik. Loetud 09.10.2015 aadressil http://vallaste.ee/.

PCMag. (2015). The Best Free Antivirus for 2015. Loetud 09.10.2015 aadressil http://www.pcmag.com/article2/0,2817,2388652,00.asp.

EICAR. (2015). Anti-Malware Testfile. Loetud 22.10.2015 aadressil http://www.eicar.org/.

FreeOnlineBackupServices. (2015). 100 Free Online Backup Services. Loetud 30.10.2015 aadressil http://www.free-online-backup-services.com/.

PrivaatneR. (2015). Turvaline surfamine. Loetud 31.10.2015 aadressil http://abi.rvg.edu.ee/.

Lisad

Lisa1. Mõistete seletusi

Selles lisas annan ma ülevaate, mida kujutab endast viirusetõrje. Samuti tutvustan erinevad viiruste vorme ja mõningaid abivahendeid nendega võitlemisel.

Viirusetõrje - Viiruste avastamiseks ja võimalike parandusmeetmete soovitamiseks või rakendamiseks määratud programm. Tavaliselt kontrollib viirusetõrje arvutis käimasolevaid protsesse ning mälus ja kõvakettal olevaid ja veebist allatõmmatavaid või elektronkirjadega saabuvaid faile, võrreldes neid varem teadaoleva pahavara koodinäidistega. Kui mõni osa kontrollitavast koodist sarnaneb viirusedefinitsioonis oleva näidisega, püüab viirusetõrje nakatunud osa eemaldada, kui see aga ei õnnestu, paigutatakse nakatunud fail karantiini või kustutatakse.

Tulemüür - Tavakasutajal on tulemüürist põhiliselt vaja teada seda, kas tema arvuti tulemüür on sisse lülitatud või ei ole. Kui mõni uus rakendus üritab pärast paigaldamist esimest korda internetti pääseda, võib tulemüür üle küsida, kas sellenimelist rakendust peaks internetti laskma või mitte. Kui rakenduse nimi on tundmatu, tasuks enne loa andmist internetifoorumitest üle kontrollida.

Turvaaugud - Turvaauk on arvutiprogrammi või -süsteemi niisugune omadus, mida selle loomise ajal kas ei mõeldud korralikult läbi, ei osatud ette näha, tehti hooletult või otsustati ignoreerida ning mille kaudu saab sedasama süsteemi kuritarvitada. Enamik vigu lähtekoodis õnnestub välja selgitada ja kõrvaldada testimise käigus, kuid kõikide mõeldavate vigade väljaselgitamine on tavaliselt ebamõistlikult kallis ja aeganõudev, nii et midagi jääb kindlasti märkamata. Tavaliselt ei mõjuta niisugused vead arvutisüsteemi tööd üldse või avalduvad vaid äärmusliku koormuse tingimustes. Samuti kaldub enamik programmeerijaid alahindama kasutajate leidlikkust ning eeldama, et nende loodud tarkvara kasutataksegi selleks, mida ta oli programmeeritud tegema.

Varukoopia - Meetod oluliste andmete säilitamiseks. Juhul, kui andmed kas õnnetuse tõttu või siis kogemata hävinevad, on võimalik need taastada ilma kõike uuesti sisestamata. Varukoopia väärtus on seda suurem, mida värskem on koopia. Et värskeim koopia ei pärineks poole aasta tagusest ajast, tuleks andmete varundamine muuta automaatseks. Mõistagi ei ole kuigi tark oma varukoopiat DVD või CD-na lauanurgale, veel vähem väljajagatud võrgukettale, vedelema jätta. Rohkem kui ühe varukoopia olemasolu oleks veelgi parem, muidugi peaks nad asuma

geograafilises plaanis kahes täiesti erinevad kohas. Siinkohal ulatavad tasuta abikäe pilvepõhised lahendused, mis reaalajas varundavad. (FreeOnlineBackupServices).

Viirused - Pahatahtliku küberkurjategija kirjutatud programmijupp, mis on lülitatud mingi programmi koosseisu ning põhjustab ootamatuid ja kasutajale sageli äärmiselt ebameeldivaid tagajärgi. Viirus põhjustab sageli kahjustusi või pahameelt ning teda võib käivitada mingi sündmus, näiteks etteantud kuupäeva saabumine. Mõned viirused on programmeeritud otseselt arvutit kahjustama - kas siis muutma programme, kustutama faile või vormindama kõvaketast. Ussviirused tegelevad ainult iseenda levitamisega, koormates niimoodi arvuti- ja võrguressursse. Kolmandad võivad olla lihtsalt nii viletsasti kirjutatud, et arvuti jookseb neid käitades kokku.

Lunavara - Krüptoviirus on selline pahavara, mis krüptib kasutaja arvutis kas teatud olulised andmed või terve kõvaketta, misjärel kurikaelad nõuavad andmete lahtikrüptimisvõtme eest lunaraha. Arvutisse satub lunavara, nagu mis tahes muu pahavara, kas rämpsposti, pahatahtliku koduleheküljе või hooletult arvutisse torgatud andmekandja kaudu. Lunavara vastu aitab toimiv viirusetõrje, eriti väärtuslikuks vasturohuks on aga värske varukoopia.

Nuhkvara - Nuhkvaraks nimetatakse faile, mis paigaldatakse teie arvutisse ilma teie teadmata ja mis võimaldab salaja jälgida teie arvutikasutamist. Sageli satub nuhkvara teie arvutisse koos mingi Internetist tasuta allalaaditava tarkvaraga, kui te ei loe tähelepanelikult litsentsitingimusi ja kohe nõustute allalaadimisega. Nuhkvara võib jälgida kasutaja veebisurfamisharjumusi, aga ka salvestada salasõna, klahvivajutusi ja ekraanipilte.

Pahavara - Ka kurivaraks nimetatakse sellist tarkvara, mida kasutatakse ilma omaniku teadmata tema arvutisse tungimiseks ja/või selle kahjustamiseks. Pahavara võib arvutisse sattuda CD-plaadil või muul andmekandjal, olla kaasa pandud e-kirjale, peidetud mõnda programmi või dokumenti, olla veebilehitseja alla laetud või tulla ise, aukliku või puuduva tulemüüri kaudu. Nakatunud arvutil võib kahjustada kõvaketast, emaplaati või mõnda muud seadet, pahavara võib arvutist kustutada olulisi andmeid või kasulikke programme. (Kirna, 2009); (Vabar, 2004); (Semper & Liikane, 2000); (Vallaste).

Lisa2. Soovitused kasutajale

Siinkohal toob autor välja soovitused, millest kinni pidamisel, välditakse suurema tõenäosusega viiruseid ja kõike muud selle kaasnevat.

1. Paigaldage arvutisse viirusetõrjetarkvara, kasutage ja uuendage seda!

Viirusetõrjesüsteem on teie esimene ja kõige võimekam abimees sissetungijatega võitlemiseks.

2. Kasutage tulemüüri!

Tulemüür on piltlikult öeldes valvur, mis otsustab, millistel rakendustel on õigus teie arvutisse siseneda ja millistel mitte.

3. Laadige regulaarselt alla operatsioonisüsteemi ja rakendusprogrammide uuendusi ja täiendusi!

Iga tarkvaratootja üritab reeglina seista hea selle eest, et tema toodang oleks kvaliteetne ja töötaks korralikult, ning parandada avastatud turvaaugud nii kiiresti kui võimalik. Parandused ja täiendused võib tavaliselt alla laadida tootja kodulehelt ning seda on soovitav teha võimalikult kiiresti, sest kiirus kahandab oluliselt võimalust, et keegi juba avastatud turvaauke teie vastu ära ei kasuta. Kindlasti võimalusel kontrollida tähtsamad programmid üle, kuna MS Windows uuendab programme eraldi ja nii võis mõni tähtis jupike uuendamata jääda.

4. Suhtuge kahtlustavalt e-kirjalisadesse. Ärge kunagi avage tundmatult saatjalt tulnud faile, sõprade saadetud failid aga kontrollige kindlasti viirusetõrjega üle!

Paljud viirused ja muud pahalased maskeerivad end pealtnäha ohututeks tekstidokumentideks või piltideks, veebilink aga võib teid suunata lehekülgedele, kust teie arvutisse laaditakse mitmesugust pahavara või kui teie eesti keelt kõnelev sõber hakkab teile ühtäkki võõrkeelseid kirju või kiirsuhtlussõnumeid saatma, paluge tal kontrollida, ega ta arvuti äkki nakatunud pole.

5. Suhtuge ettevaatusega kõigesse, mida internetist alla laete, kui vähegi võimalik, üritage kontrollida selle päritolu!

Pahatihti laetakse koos tarkvaraga alla ka lisatarkvara, mille olemasolust teile ei teatata ning mis asub teie arvutis omatahtsi tegutsema. Samuti ärge võtke tõsiselt ettepanekuid laadida näiteks alla spetsiaalne videovaatamiseprogramm, et ühe konkreetse saidi sisule paremini ligi pääaseda, ning kontrollige kõik allalaetavad failid enne käivitamist viirusetõrjega igaks juhuks üle.

6. Tehke varukoopiaid ning hoidke neid arvutist eraldi!

Arvutis olevad andmeid võivad kahjustada saada paljude erinevate ohtude tagajärjel. Mitte ainult rünnak või viirus, vaid ka tugev voolukõikumine või telefoniliini sisse löönud pikne võivad hävitada kõik teie failid. Kuid kahju pole nii suur, kui teete oma andmetest regulaarselt varukoopiaid, nii võite pärast süsteemi taastamist jätkata oma tegemisi samast seisust, mil te viimase varukoopia tegite. Varukoopiaid tuleks mõistagi hoida mitte arvutis endas, vaid soovitavalt eraldi andmekandjal, näiteks plaadil või välisel kõvakettal. Soovitav oleks neid hoida teises ruumis või koguni teises hoones. Veelgi parem oleks omada mitut varukoopiat, mis asuksid üksteisest eraldi.

7. Kasutage tugevaid salasõnu ja ärge jagage kergekäeliselt oma isiku-, kontakt- ega juurdepääsuõigusi!

Salasõnad on mõeldud selleks, et teatud ressurssidele või rakendustele ei saaks ligi need, kellel selleks õigusi pole. Olge üsna kindlad, et sissetungija proovib esimeses järjekorras teie nime, sünnikuupäeva, auto numbrit või märgikombinatsiooni "admin123". Kui kasutate aga salasõnana pikka, suur- ja väiketähtedest, numbritest ja erimärkidest koosnevaid kombinatsioone, võib salasõna murdmiseks kuluv aeg olla piisavalt kriitiline, et panna sissetungija oma ettevõtmisest loobuma. Salasõnad, PIN-koodid ja muud ligipääsuandmed on mõeldud selleks, et neid kasutaksite ainult teie, seega ei tohi neid mistahes ettekäändel mitte kellelegi edasi anda, isegi kui neid küsib hea sõber, IT-töötaja või pank.

8. Logige end administraatorina sisse ainult siis, kui see on hädavajalik ning seadke vähemalt 16 tähemärgi pikkune salasõna antud kontole - igapäevatöö tegemiseks logige sisse piiratud õigustega kasutajana, kus samuti soovitaks salasõna kasutada. Sedaviisi suudab arvutisse sisseroninud pahalane hoopis väiksemat kahju tekitada.

Administraatoril on piiramatu juurdepääs kõigile süsteemi ressurssidele ning õigus paigaldada mistahes programme ja programmilisasid. Pahalane, kelle te adminstraatorina alla tõmbasite, võib saada teie arvutis samad õigused ning teha hoopis rohkem kurja. Mõni pahalane ei suudagi end ilma piisavate õigusteta teie arvutisse sisse seada. Looge endale ja kõigile teistele arvuti kasutajatele piiratud õigustega konto. Administraatorina logige end sisse ainult siis, kui teil on vaja paigaldada uusi programme, muuta olemasolevate programmide seadeid või teha vajalikke süsteemitoiminguid.

9. Olge ettevaatlik mälupulkade ja teiste andmekandjatega, kontrollige neis sisalduvat kindlasti pärast seda, kui olete neid võõras arvutis kasutanud.

Peale andmekandja kasutamist võõras arvutis on oht, et sinna peale võis sattuda mõni pahalane, kes hiljem nakatab kõiki arvuteid, kus andmekandjat kasutatakse, seepärast on mõistlik ta läbi kontrollida. Isegi kui tegu on sõbra arvutiga, võib temagi arvutis olla pahalane, kelle olemasolust keegi varem ei teadnud.

10. Seal, kus võimalik, kasutage ID-kaarti. Ärge seda pärast kasutamist lugejasse unustage!

ID-kaart on üks lihtsamaid ja turvalisemaid võimalusi kaitsta näiteks oma pangakontot kuritarvitamise või dokumentide võltsimise eest.

11. Veebilehitsejas toimetades kasutage privaatset režiimi!

See tähendab seda, et siis ei jäeta tundlikku infot meelde lehitseja poolt - külastatud aadresside ajalugu, sessioonide küpsised, sisestatud vormide infot ning salasõnu. Vaikimisi jätavad kõik veebilehitsejad sellise tundliku info meelde, kui neid ei ole teisiti seadistatud. Privaatse režiimi saab kiirelt sisse lülitada: Internet Explorer ja Mozilla Firefox - CTRL+SHIFT+P, Google

Chrome ja Opera - CTRL+SHIFT+N. Safari puhul tuleb see käsitsi valida rippmenüüst(*Private browsing*).

12. Kui te ei saa aru või pole kindel, mida arvuti teie käest tahab, siis lugege veelkord, kui vaja, tõlkige teade, küsige mõnelt tuttavalt asjatundjalt üle või kasutage interneti otsimootoreid!

Paljud tarkvaratootjad ei lisa kahjuks oma operatsioonisüsteemide või rakendusprogrammide keelevalikusse eesti keelt. Seda enam pole põhjust klõpsida avanenud dialoogiboksides nuppe "*Yes*" ja "*Next*" ning loota parimat. Üritage välja selgitada, mida arvuti teie käest tahab ning kas see, mida ta tahab, on ikka mõistlik.

Grupipoliitika rakendamine aitaks samuti kaasa arvuti kaitsmisele pahavara eest. Kui näiteks ära keelata MS Windowsi registri ja käsurea kasutamine koos Juhtpaneeliga. Sel juhul on palju asju juba kinni pandud ja pahavara ei saa ligi. Kahjuks ei ole selline asi võimalik aga ei MS Windows Basic ega Home versioonidel.

Kasutage oma tervet mõistust - ärge registreerige kahtlastesse keskkondadesse; ärge osalege kui tahes ahvatlevates loosimistes; ärge saatke edasi kettkirju; ärge klikkige kõike, mida teile näidatakse ning ärge jagage oma andmeid kõigile, kes neid küsivad! Samuti ärge logige sisse igalepoole, samalajal olles avalikus võrgus, sest tuletame meelde, et andmed on kõikidele nähtavad sellistes võrkudes. Samuti ei kehti arusaam, et mida rohkem erinevaid viirusetõrjeid, seda turvalisem arvuti on, sest viirusetõrjed hakkavad üksteist segama ja nende töö kvaliteet langeb sellega. (Kirna, 2009); (Vabar, 2004); (Arvutikaitse); (PrivaatneR).