MAANPUOLUSTUSKORKEAKOULU

VERKKOTUETUN MONIMUOTO-OPETUKSEN TIETOTURVARISKIT, ESIMERKKINÄ ILMAVOIMIEN TEKNILLINEN KOULU

Pro Gradu

Kadetti
Tatu Köykkä

Kadk 89
Ilmavoimien lentoteknillinen linja

2006

MAANPUOLUSTUSKORKEAKOULU

Kurssi	Linja
Kadk 89	Ilmavoimat, lentoteknillinen linja
Tekijä Kadetti Tatu Köykkä	
Tutkielman nimi **VERKKOTUETUN MONIMUOTO-OPETUKSEN TIETOTURVARISKIT, ESIMERKKINÄ ILMAVOIMIEN TEKNILLINEN KOULU**	
Oppiaine, johon työ liittyy Tekniikka	Säilytyspaikka Kurssikirjasto (MpKK:n kirjasto)
Aika 2006	Tekstisivuja 63 Liitesivuja 3

TIIVISTELMÄ

Viime vuosien informaatioteknologian kehitys on avannut uusia mahdollisuuksia koulutusjärjestelmille. AVOT- kehittämisohjelma (avoin oppimis- ja työskentely-ympäristö) käynnistettiin puolustusvoimien komentajan käskystä vuonna 2000. Ohjelman yhtenä tarkoituksena on tehostaa puolustusvoimien henkilöstön, reserviläisten ja varusmiesten koulutusta mahdollistamalla tietotekniikkaa hyväksi käyttävä verkkotuettu monimuoto-opetus. AVOT-hankkeen tuloksena on syntynyt puolustusvoimien ja rajavartiolaitoksen verkko-opetusympäristö, koulutusportaali. Ilmavoimien teknillisellä koululla on tarve tuoda koulutusportaaliin lentoteknillistä opetusmateriaalia, joka on tietoturvatasoltaan luokiteltu viranomaiskäyttöön. Pyrin kirjallisuustutkimuksen ja haastattelun perusteella kartoittamaan tietoturvariskit, jotka syntyvät käyttäjien asenteista, osaamisesta ja välineistä.

Tutkimuksessa ilmeni: Ennen kuin koulutusportaalissa voidaan käsitellä turvaluokiteltua materiaalia, käyttäjien tiedot, taidot, asenne ja työkalut on koulutuksella ja ohjeistuksella saatettava yhdenmukaisiksi.

AVAINSANAT:
Tietoturvallisuus, internet, sähköposti, verkko-opetus, AVOT, koulutusportaali, oppimiskeskus.

SISÄLLYSLUETTELO

1. JOHDANTO

1.1 Tutkimuksen tausta ja perustelut aihevalinnalle 1
1.2 Tutkimusongelma ja aiherajaukset 3

2. TUTKIMUKSEN TEOREETTISET LÄHTÖKOHDAT

2.1 Taustaa etä- ja verkko-opetuksesta 4
2.1.1 Etäopetuksen historiaa 4
2.1.2 Tietoverkko syntyy 6
2.1.3 Internet 7
2.1.4 Tiedon valtatie 9

2.2. PUOLUSTUVOIMIEN VERKKO-OPETUKSEN TILA
2.2.1 AVOT 9
2.2.2 Koulutusportaali 10
2.2.3 Oppimiskeskus 13
2.2.4 Oppimiskeskus Ilmavoimien Teknillisessä Koulussa 14

2.3. TIETOTURVA 16
2.3.1 Käsitteitä 17
2.3.1.1 Tunnistaminen, todentaminen ja kiistämättömyys 18
2.3.1.2 Suojauksesta ja salauksesta 18
2.3.1.3 Mikä meitä uhkaa? 21
2.3.2 Haittaohjelmat 24
2.3.3 Ohjelmistojen tietoturva-aukot 28
2.3.4 Langattomuus 34

2.4 SUOJAUTUMINEN
2.4.1 Virustorjunta 36
2.4.2 Palomuuri 37
2.4.3 Sähköpostin turvallisuus 39

2.4.4 Salasanat 39

3 TUTKIMUSMENETELMÄT
3.1 Yleistä tutkimuksesta 40
3.2 Kyselyn suorittaminen 41

4 TUTKIMUSTULOKSET 43

5 YHTEENVETO 62

LÄHTEET 64

LIITTEET

1. JOHDANTO

1.1 Tutkimuksen tausta ja perustelut aihevalinnalle

Tutkija on toiminut lentoteknillisenä opetusupseerina Ilmavoimien teknillisessä koulussa, joka vastaa ilma- ja maavoimien lentoteknillisen henkilöstön koulutuksesta. [11] Työnsä ohella hän on toiminut työpisteensä ATK-tukihenkilönä ja tässä tehtävässä hän on usein joutunut tekemisiin tietoturvaongelmien kanssa niiden kaikessa monimuotoisuudessa.

Vaikka ihmisten tietoisuus tietoturva-asioista lisääntyy, eivät ongelmat ole kuitenkaan vähentyneet. Ohjelmistohaavoittuvuuksia löytyy edelleen tiheään tahtiin ja ongelmakenttä kasvaa, koska verkkorikolliset ovat siirtyneet maineen tavoittelusta taloudellisen hyödyn tavoitteluun.

Suomi etenee tietoturva-asioissa maana ensimmäisten joukossa ja meillä laadittiin ensimmäisenä maailmassa kansallinen tietoturvakatsaus sekä hahmotettiin ensimmäisenä Euroopassa yhteiskunnan tason tietoturvastrategia. Suomi on tietoyhteiskunta, jolle tietoturvauhka on todellinen. Suomalaisten kotitalouksien tietokoneistuminen ja verkottuminen näyttää saavuttaneen huippunsa, mutta tietoturvariskit kasvavat, koska laajakaistaliittymien määrä kasvaa nopeasti. Kannettavien tietokoneiden ja siirrettävin muistimedioiden lisääntyminen kasvattavat tietoturvariskiä, koska liikuteltavuus ja käytön helppous houkuttelevat käyttäjiä siirtämään tietoa tietokoneesta toiseen. Kansainvälisen vertailun perusteella Suomalaisten kotitalouksien tietoturva on hoidettu kohtuullisesti, mutta ei hyvin. Tässä vertailussa Suomi ei ole parhaimpien joukossa. Yritysten tietoturvavertailussa Suomi sijoittuu EU-maiden kärkipäähän.

Viime vuosien informaatioteknologian kehitys on avannut uusia mahdollisuuksia koulutusjärjestelmille ja Ilmavoimat on puolustusvoimien osana haasteen edessä. AVOT-kehittämisohjelma eli avoin oppimis- ja työskentely-ympäristö – ohjelma käynnistettiin puolustusvoimien komentajan käskystä vuonna 2000. [42] Sen seurauksena on syntynyt muun muassa internet-pohjainen koulutusportaali, jonka tarkoituksena on tehostaa puolustusvoimien henkilöstön, reserviläisten ja varusmiesten koulutusta mahdollistamalla tietotekniikkaa hyväksi käyttävä verkkotuettu monimuoto-opetus. AVOT-ohjelman taustalla vaikuttavat tietoyhteiskunnan vaatimukset sekä puolustusvoimien organisaation muutostarpeet, joita ovat esimerkiksi koulutusjärjestelmän pedagogi-

nen uudistaminen, työntekijöiden osaamisen kehittäminen, asiantuntijuuden korostaminen ja yleinen pyrkimys avoimuuteen. Avoimuus tässä yhteydessä tulee ymmärtää siviiliyhteiskuntaan suuntautuvana avoimuutena.

Ilmavoimien teknillisen koulun opetus on edelleen pääsääntöisesti lähiopetusta. Tämä tarkoittaa luokkaopetusta ja sitä, että opintokokonaisuuden suorittaminen edellyttää fyysistä läsnäoloa Ilmavoimien teknillisellä koululla. Osasyynä lähiopetuksen suureen määrään on lentotekniikan opetuksessa käytettävien havaintomateriaalien, lentokoneiden ja niiden osien tila- ja turvallisuusvaatimukset. Toisaalta lähiopetuksella on pitkät perinteet puolustusvoimissa ja sotilaat ovatkin kautta aikojen saaneet koulutuksensa käytännön harjoitteiden ja luokkaopetuksen kautta. Tekniset edellytykset opetuksen monimuotoistamiseen ovat Ilmavoimien teknillisessä koulussa olemassa: Opetusmateriaali on pääsääntöisesti sähköisessä muodossa ja on olemassa oppimisympäristö, koulutusportaali, jota oppilaat voivat käyttää kotoaan tai työpaikalta.

Tällä hetkellä koulutusportaalin käyttöä lentokonetekniikan opetuksessa rajoittaa ohjeistus, jonka mukaan verkko-opetusmateriaalin tulee olla turvaluokitukseltaan julkista. Poikkeuksen tällä hetkellä tekee erillislupa, jolla on tehty mahdolliseksi luottamuksellisuusluokan VIRANOMAISKÄYTTÖ (TLL IV) tietojen käsittely koulutusportaalissa tietyin ehdoin. Puolustusvoimien koulutuksen kehittämiskeskus anoi Pääesikunnan turvallisuusosastolta lupaa, joka mahdollistaisi esiupseerikurssin monimuotoopiskeluun liittyen viranomaiskäyttö- luokitellun aineiston käsittelyn koulutusportaalissa. Lupa myönnettiin määräaikaisena ja se päättyy 31.12.2006. Turvallisuusosasto määritteli tietoturvallisuuden perusvaatimukset.

1. Kaikki koulutusportaalin palvelimilla tallennettava salassa pidettävä tieto on salattu valtionhallinnon hyväksymällä salaustuotteella ja menetelmällä.

2. Salassa pidettävän tietoaineiston tuottajien tulee tiedostaa ne suuret riskit, mitä avoin tietoverkko, kuten tässäkin tapauksessa on kyse, tuo tullessaan. Tästä syystä tietoaineiston tuottajien tulee tarkoin harkita, millaista tietovarantoa järjestelmään tarjotaan.

3. Tietoaineistojen tuottajien ja käyttöoikeuksien hallinnasta vastaavien tulee ehdottomasti noudattaa koulutusportaalin ylläpitäjien antamaa ohjeistusta salassa pidettävän tiedon käsittelemisestä koko elinkaaren ajan. Tarpeeton tietovaranto tulee poistaa palvelimilta käyttötarpeen päätyttyä.

4. Käyttäjät, joille tarjotaan oikeus lukea ja tallentaa salassa pidettävää tietoaineistoa koulutusportaalin puitteissa, tulee ensin kouluttaa ja varmistua, että he hallitsevat salassa pidettävän tiedon käsittelyyn liittyvät menettelyt

5. Koulutuksessa tulee erityisesti painottaa sitä, että KOPO:ssa tarjottavaa salassa pidettävää tietoa käsitellään vain Maanpuolustuskorkeakoulun tietohallinnon opettajille ja opiskelijoille tätä varten luovuttamilla laitteilla.

6. Käyttäjiltä edellytetään välitöntä raportointia tietoturvaloukkaustilanteita ja niiden epäilyjä kohdatessa.

7. Maanpuolustuskorkeakoulu ja Puolustusvoimien koulutuksen kehittämiskeskus seuraavat ja valvovat KOPO-järjestelmän käyttöä ja raportoivat tietoturvallisuuteen liittyvistä käyttökokemuksista. [31]

Suuri osa Ilmavoimien teknillisen koulun perusopetuksen opetusmateriaalista on niin kutsuttua luokittelematonta tietomateriaalia, eikä tietoturvallisuus siltä osin ole ongelma. Potentiaalisen uhkan muodostaa hävittäjäkaluston järjestelmäopetuksessa käytettävä opetusmateriaali, joka on osittain turvaluokiteltu viranomaiskäyttöön. Tässä tutkimuksessa pyritään lentotekniikan opettajille ja oppilaille tehdyn tietoturvakyselyn perusteella luomaan kuva siitä henkilökohtaisesta tietoturvan tasosta, joka koulutusportaalin käyttäjillä Ilmavoimien teknillisessä koulussa on.

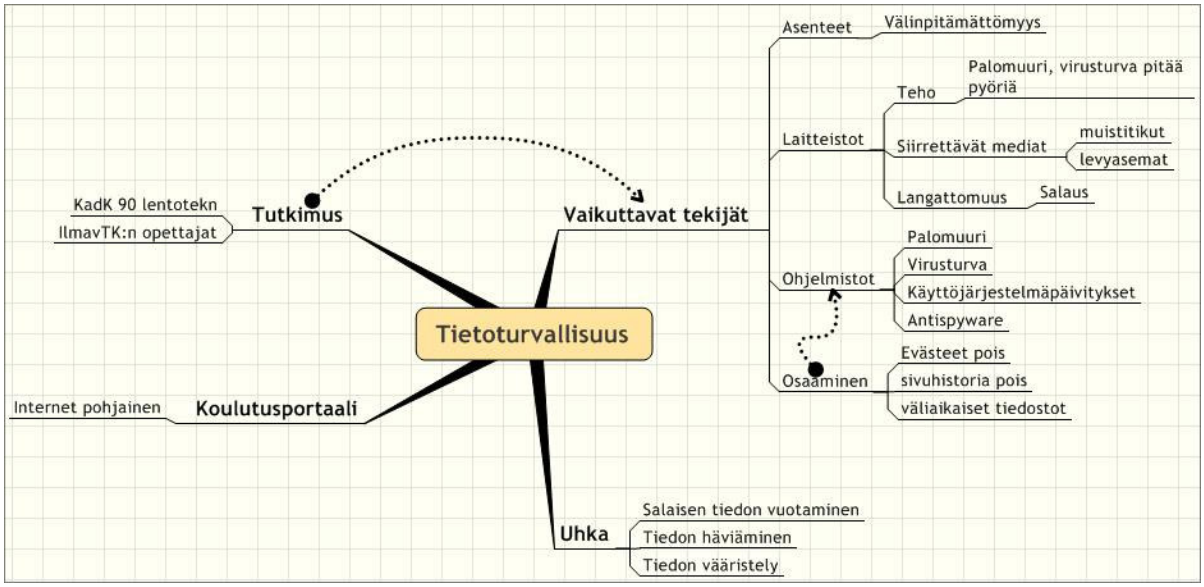
1.2 Tutkimusongelma ja aiherajaukset

Tutkimuksen pääongelma on:

- Mitkä koulutusportaalin käyttäjien toimet ja välineet aiheuttavat tietoturvallisuusriskejä?

Alaongelmia ovat:

- Miten riskejä voitaisiin pienentää?
- Onko tarvetta koulutukselle?



Kuva 1. Tutkijan ajatuskartta tietoturvallisuuteen vaikuttavista tekijöistä

Aihe on rajattu siten, että tietoturvakysely on tehty ainoastaan Ilmavoimien teknillisen koulun kurssiosaston henkilöstölle sekä koulussa opiskeleville 90.kadettikurssin lentoteknillisen linjan kadeteille. Kyselytutkimus on internetin käyttöön painottuva, mutta sisältää myös kysymyksiä käyttäjän tietoteknisistä välineistä, ohjelmistoista ja varmentamismenettelyistä.

2. TUTKIMUKSEN TEOREETTISET LÄHTÖKOHDAT

2.1 Taustaa etä- ja verkko-opetuksesta

Suomi on pitkien ja välimatkojen ja hankalien kulkuyhteyksien maa, jossa etäopetus on lähentänyt opiskelijoita ja opettajia jo liki sadan vuoden ajan. Suomen kansanvalistusseuran kirjeopisto toimi etäoppimisen välineenä jo 1900-luvun alussa. Teknistymisen myötä etäopetus siirtyi radioon ja televisioon. Kotitietokoneet ja verkottuminen toi oppimiseen uuden vuorovaikutuksen tason. [29]

2.1.1 Etäopetuksen historiaa

Etäopetus juontaa juurensa 1800-luvulta alkaneesta kirjeopetusmallista. Tuolloin oppilas ja opettaja keskustelivat kirjeitse, joten kysymykset ja vastaukset saattoivat viipyä matkalla viikkoja, jopa kuukausia. Tänään tietoa siirretään tietoverkkojen ja inter-

netin välityksellä. Viiveet ovat olemattomat ja valtameret ylitetään silmänräpäyksessä.

Randy Garrisonin mukaan etäopetuksen kehitys voidaan jakaa kolmeen vaiheeseen:

- kirjeopetukseen
- televiestinnän ja tiedotusvälinen käyttöön (radio, televisio, videot, äänitteet)
- tietokoneiden ja tietoverkkojen käyttöön

Kirjeopetuksen ongelma oli tiedon siirron hitaus. Palaute viipyi matkalla ja opettaja oli etäinen, vaikka esimerkiksi puhelinvastaanotot saattoivat olla mahdollisia.

Myöhemmin kun teknologia kehittyi, etäopetukseen saatiin uusia välineitä. Radion ja television opetusohjelmat, videot ja äänitteet lienevät kaikille viime vuosikymmeninä opiskelleille tuttuja. [27] Suomessa radion kautta tapahtuva etäopetus alkoi vuonna 1926 kun Yleisradio lähetti ensimmäisen englannin kielen kurssin. Toiminta laajeni vuonna 1934 Kouluradion myötä. Kohderyhmänä olivat kansakoululaiset, eikä systemaattisia opetuskokonaisuuksia tuolloin vielä ollut. Uutuus viehätti, mutta pedagoginen merkitys oli vähäinen.

60-luvulla aikuisväestöön panostettiin perustamalla aikuisopetuksen toimitus. Ohjelmatarjontana oli mm kieliohjelmia. Televisio yleistyi ja vuonna 1963 aloitettiin ensimmäiset Koulu-tv:n lähetykset. [34] Yleisradio on tarjonnut opetusohjelmia koko lähes 80-vuotisen olemassaolonsa ajan. Lähetystuntimäärät ovat kasvaneet erityisesti vuoden 1994 jälkeen, jolloin tuli voimaan YLE- laki joka määritteli yleisradion tehtäväksi mm seuraavaa: *Yhtiön tehtävänä on tuoda täyden palvelun televisio- ja radio-ohjelmisto siihen liittyvine oheis- ja lisäpalveluineen jokaisen saataville yhtäläisin ehdoin. Toiminnan tulee julkisen palvelun erityisinä tehtävinä: edistää ohjelmiston sivistävää luonnetta, tukea kansalaisten opiskelua ja tarjota hartausohjelmia*. [17] Vuonna 2000 Yleisradio lähetti opetusohjelmia radiosta ja televisiosta yhteensä yli 3000 tuntia. Osa kasvusta on selitettävissä alueellisten opintoradioiden perustamisella sekä etäopiskeluun liittyvien palvelujen, kuten etälukion ja Ylen avoimen yliopiston perustamisella. [35]

2.1.2 Tietoverkko syntyy

ARPA-järjestö (The Advanced Research Projects Agency) perustettiin Yhdysvalloissa 1958. Myöhemmin ARPA muuttui DARPA:ksi D-kirjaimen tarkoittaessa Defense (puolustus). DARPA oli tieteellinen yhteisö, mutta sen toimintaa rahoitti sotilaalliset hallintoelimet. DARPA:n syntyminen oli seurausta siitä, että Neuvostoliitto oli ehtinyt avaruuteen ennen Yhdysvaltoja. Sputnik oli laukaistu avaruuteen vuonna 1957 ja Yhdysvallat koki, että avaruuden valloituksen myötä Neuvostoliitolla oli kyky myös mannerten välisiin ohjusiskuihin.

DARPA perustettiin tutkimaan ja kehittämään tietokoneisiin perustuvaa valvonta- ja komentojärjestelmää (CCR, Command and Control Research). Vuonna 1962 tutkimusryhmän johtoon valittiin Tohtori J.C.R Licklider Cambridegen yliopistosta. Ryhmän henki oli kehittää tietokonetta ihmisten kommunikointi- ja tiedonhankinta välineenä. [10] Syyskuussa 1969 kytkettiin ensimmäinen tietokone DARPANETin solmukoneeseen UCLA:ssa (University of California Los Angeles). Saman vuoden loppuun mennessä verkkoon oli kytketty kolmen eri yliopiston tietokoneet eli verkossa oli neljä tietokonetta. Koneet pystyivät kommunikoimaan tasavertaisesti vaikka kaikki käyttivät toisistaan poikkeavia käyttöjärjestelmiä.

70-luvulla DARPANET laajeni ja yhdisti pian useita laboratorioita ja tutkimuskeskuksia ympäri yhdysvaltoja. Kaikille DARPANETiin kuuluville oli yhteistä Yhdysvaltain puolustusministeriön tuki. Vuonna 1972 DARPANETissa otettiin käyttöön sähköpostiohjelma, jota voidaan pitää nykyisten internet-sähköpostiohjelmien esi-isänä.

Suomessa verkottuminen alkoi 1970 kun Suomen Pankki osti Univavac1108 tietokoneen, jota voitiin etäkäyttää tietoliikenneyhteyksien välityksellä. Kone maksoi 11,5 miljoonaa markkaa ja se sijoitettiin Valtion Tietokonekeskukseen (VTKK). Vuoden 1971 aikana kaikki Suomen tiedekorkeakoulut oli kytketty 1200 bit/s ja 2400 bit/s yhteyksillä verkkoon. Laitteistot koostuivat DCT2000 etäeräpäätteistä jotka oli varustettu rivikirjoittimella ja reikäkorttilaitteilla. [13]

2.1.3 Internet

Internetin peruspilari TCP/IP protokolla (Transmission Control Protocol / Internet Protocol tiedonsiirtokäytäntö) syntyi 70-luvulla DARPANETin ympärillä tehdyn tutkimuksen tuloksena. 1980- luvulla TCP/IP tiedonsiirtokäytännöstä tuli Yhdysvaltain puolustusministeriön virallinen verkkostandardi. [38] TCP/IP on reitittävä protokolla, koostuen Internet-protokollista. Niillä määritellään tietokoneiden välinen tiedonsiirto, kuinka verkot kytkeytyvät ja kuinka reititys tapahtuu. [14]

Www eli World Wide Web nimityksen Internet-pohjaisesta hypertekstijärjestelmästä keksi Tim Berners-Lee vuonna 1990. www:n tarkoituksena oli yhdistää verkoissa hajallaan oleva valtava tietomäärä yhden käyttöliittymän alle. Tähän tarkoitukseen Berners-Lee kehitti kuvauskielen Hypertext Markup Language lyhyesti HTML.

HTML-kieli kuvaa dokumenttia ja sen rakennetta kertomalla mikä osa tekstistä on esimerkiksi korostusta, otsikkoa, kuvaa tai kehystä. Esitysasu määräytyy käyttäjän ohjelman (selaimen) ja näyttölaitteen ominaisuuksien mukaan. Jotta HTML-kielestä syntyisi www eli maailmanlaajuinen hypertekstiverkko tarvitaan tapa määritellä linkkejä toisiin dokumentteihin ja resursseihin. Tätä tehtävää hoitaa URL eli Universal Resource Locator. Se määrittelee tiedon siirtomenettelyn eli protokollan. Protokollia on esimerkiksi FTP (File Transfer Protocol), telnet ja http eli Hypertext Transport Protocol. Http on nimenomaan www-käyttöön tehty yhteysmenetelmä. [38]

Matka DARPANETistä tämän päivän internetiin on ollut pitkä, mutta perusperiaate on pysynyt samana. Sotilaiden oli tärkeää saada käskyt ja viestit kulkemaan verkossa kaikissa olosuhteissa. Tänään sähköpostien, pankkisiirtojen ja tilausten on kuljettava vaikka yhteys olisi jostakin kohdasta poikki. Www perustuu seittimäiseen (web) rakenteeseen, joka mahdollistaa ongelmakohtien, kuten kaatuneiden palvelimien tai vioittuneiden kaapelien kiertämisen.

Internetiä voidaan kutsua verkkojen verkoksi, jossa on kolme tasoa:

- Ensimmäinen taso on yritysten lähiverkot ja yksityisten ihmisten kotiverkot. Nämä on toteutettu Ethernet- kaapelilla tai langattomasti wlan- yhteydellä (wireless local area net). Pienin yksikkö internetissä on yksittäinen tietokone esimerkiksi kotona tai työpaikalla.

- Toisen tason verkko muodostuu verkko-operaattoreiden järjestelmistä. Operaattorit keräävät yritys- ja kotiverkkojen liikenteen ja välittävät sen eteenpäin. Tällä verkkotasolla tietoa siirretään puhelinkaapeleita, televisiokaapeleita, sähköjohtoja ja wlan- verkkoja pitkin.

- Kolmannen tason muodostavat runkoyhteydet jotka yhdistävät operaattoreiden verkot toisiinsa luoden varsinaisen globaalin internetin.

Runkoyhteydet toteutetaan lähes poikkeuksetta valokaapeliyhteydellä, sillä muiden tällä hetkellä käytössä olevien yhteystyyppien kapasiteetti ei riitä valtavien datamäärien siirtämiseen maiden ja maanosien välillä. Suomesta lähtee ulkomaille useita runkoyhteyksiä. Useimmat ovat merikaapeleita, joista neljä kulkee Ruotsiin, kaksi Viroon ja yksi Venäjälle. Yhteys Euroopasta Amerikkaan on toteutettu 8000 kilometriä pitkällä valokuidulla joka kulkee Atlantin valtameren pohjassa. Signaali vahvistetaan muutaman kymmenen kilometrin välein sijoitetuilla signaalivahvistimilla. Näiden Euroopasta pohjois- Amerikkaan kulkevien TransAtlantic- kaapeleiden siirtonopeus on 560 megabittiä sekunnissa. [20]

Suomessa oli vuonna 2005 noin 2,4 miljoonaa kotitaloutta, joista vuoden 2005 lopulla 1,1 miljoonaa oli kytkeytyneenä laajakaistaiseen internetliittymään. Perustason laajakaistayhteyden nopeus on 256 kilobittiä sekunnissa, mikä tarkoittaa noin viisinkertaista siirtonopeutta modeemiyhteyteen verrattuna. Tilastokeskuksen mukaan suomalaiset käyttävät internetyhteyttä pääasiassa sähköpostin lähettämiseen ja vastaanottamiseen, tiedon hakuun, pankkipalveluihin sekä online-lehtien lukemiseen. Tietoa etsitään mm. palveluista, tuotteista ja matkailusta. Sähköinen kaupankäynti kaksinkertaistui pohjoismaissa vuoden 2005 aikana ja sen arvellaan kasvavan voimakkaasti myös tulevaisuudessa. Kasvua hidastaa kuluttajien huoli tietoturvasta. 70% niistä suomalaisista, jotka eivät tee web-ostoksia, ilmoitti ostamatta jättämisen syyksi huolen luottokorttinumeron tietoturvasta. [25]

2.1.4 Tiedon valtatie

Edellä on esitetty etäopetuksen kehitystä sekä verkkotekniikan historiaa ja nykypäivää tekniseltä näkökannalta. Verkottumista voi kuitenkin tapahtua monella eri tasolla. Sosiaaliseksi verkoksi kutsutaan ihmisten välistä verkottumista.
Koneiden välistä verkottumista, esimerkiksi Internetiä kutsutaan fyysiseksi verkoksi. Viestintäverkko- nimitystä (communications network) käytetään ihmisten välisestä viestinnästä.

”Tietoverkko” kuvaa tiedon siirtoa fyysistä verkkoa hyväksikäyttäen. Miljoonat verkkoon kytketyt tietokoneet muodostavat rakennelman joka avaa valtaisat tietovarannot. On syntynyt käsite tiedon valtatiestä (information highway). [18]

Kaikki edellä esitelty tekniikka tarjoaa uusia mahdollisuuksia niin opiskelijalle kuin opettajalle. Tietotekniikka lyhentää välimatkoja ja tekee kommunikoinnista lähes viiveettömän. Tekniikka ja uusi oppimisympäristö eivät kuitenkaan yksin riitä takaamaan hyviä oppimistuloksia, vaan ne ainoastaan luovat mahdollisuuden oppimiselle. [27] Teknologian myötä opiskelijan vastuu omasta oppimisesta korostuu. Puolustusvoimat on muiden mukana uusien haasteiden edessä.

2.2 PUOLUSTUVOIMIEN VERKKO-OPETUKSEN TILA

2.2.1 AVOT

Suomi on tieto- ja viestintätekniikan kärkimaita ja näiden tekniikoiden käyttöönotto työssä ja koulutuksessa on katsottu myös tärkeäksi kilpailutekijäksi. Opetusministeriön koulutuksen ja tutkimuksen tietostrategia 2000-2004 vuodelta 1999 määritteli kansalliseksi visioksi: ”V*uoteen 2004 mennessä Suomi on maailman kärkimaiden joukossa oleva osaamis- ja vuorovaikutusyhteiskunta”.* [34] Puolustusvoimat yhteiskunnan osana on ollut osallisena toteuttamassa tätä tavoitetta.

Puolustusvoimien AVOT (Avoin oppimis- ja työskentely-ympäristö) -ohjelma on tietoverkkojen käyttöön työssä ja opiskelussa kohdistuva kehittämisohjelma. Ohjelma käynnistettiin puolustusvoimien komentajan linjauksen mukaisesti vuonna 2000 ja sen on tarkoitus jatkua vuoteen 2012 asti. Vuonna 2002 vahvistettiin linja, jossa puolustusvoimat ohjataan toimimaan oppivan organisaation periaatteiden mukaisesti.

Tässä periaatteessa oppiminen on olennainen osa jokaisen yhteisön ja työntekijän toimenkuvaa. Jatkuvan oppimisen merkityksen painottaminen luo haasteita koulutusjärjestelmälle vaatien siltä joustavuutta ja verkottumista. AVOT on tarkoitettu palvelemaan palkattua sotilas- ja siviilihenkilökuntaa, reserviläisiä ja varusmiehiä.

Avoin oppimis- ja työskentely-ympäristö-ohjelman tavoitteena on ohjata opetusta ja opiskelua nykyistä avoimempaan suuntaan. Opiskelijalla tulisi olla mahdollisuus vaikuttaa siihen, missä, milloin ja millä tavalla hän opiskelee. Jossain määrin myös opiskelun tavoitteet ja arviointitavat lähtisivät opiskelijan tarpeista. Edellä esitetyt vaatimukset toteutuvat verkkotuetussa monimuoto-opetuksessa, jossa opiskelija voi vaikuttaa opiskelunsa paikkaan ja aikaan. Etäjaksolla opiskellaan itsenäisesti esimerkiksi kotona internetin avulla. Verkossa voidaan käydä keskusteluja, esittää kysymyksiä ja argumentteja. Opettaja voi antaa tehtävät sähköpostilla ja tehtävien palautus ja muu palautteen anto onnistuu myös verkon välityksellä.

AVOT ei ole kehittämisohjelmana ainutlaatuinen. Useissa maissa on asevoimissa käynnissä saman suuntaisia hankkeita, laajimpana Yhdysvaltain ADL-projekti (The Advanced Distributed Learning Initiative). [42]

2.2.2 Koulutusportaali

27.1.2004 avattiin puolustusvoimien koulutusportaali. Sitä edelsi kolmen vuoden pilotointivaihe, jonka aikana toteutettiin 96 verkkokurssia yhteensä noin 8000 käyttäjälle. Koulutusportaali toimii internetissä ja portaalin käyttö vaatii sisään kirjautumisen, jolla pyritään varmistamaan tietoturva. Liikenteen kaappaus ja muuntaminen on tehty vaikeaksi pankkipalveluista tutulla salakirjoitusmenetelmällä. Puolustusvoimien Koulutuksen Kehittämiskeskus on vastannut koulutusportaali- hankkeen kehittämisestä ja ulkopuoliset tietotekniikkayritykset ovat vastanneet järjestelmän teknisestä toteuttamisesta

Koulutusportaali pitää sisällään muun muassa sähköpostitoiminnot, tietopankin ja verkkosotakoulun, jota käytetään verkkotuettujen kurssien oppimisympäristönä. Verkkosotakoulun avulla on mahdollista toteuttaa verkkotuettua monimuoto-opetusta, joka rakentuu lähiopetusjaksoista ja etäopetusjaksoista

Verkossa tapahtuva etäopiskelu voi olla ryhmätöitä, itsenäistä tiedon hakua tai oppimistehtävien tekemistä. Lähijaksoilla syvennetään ja sovelletaan opittua tietoa, anne-

taan tietokatsauksia ja kootaan yhteen opiskelijoiden ajatuksia sekä etsitään vastauksia esille nousseisiin kysymyksiin. Tietopankkiin tallennetaan oppimateriaalia, ohjesääntöjä, oppaita ja esittelymateriaalia. [1] Tietopankki toimii nimensä mukaisesti tiedon varastona. Kaikilla käyttäjillä on pääsy tietopankin julkiseen materiaaliin ja puolustusvoimien henkilöstöllä myös luokiteltuun materiaaliin.

Materiaalia voi tallentaa esimerkiksi tekstimuodossa, esitysformaateissa tai html-muodossa. Tämän lisäksi kaikki portaaliin viety materiaali automaattisesti tallentuu pdf- formaatissa (Portable Document Format). Siten tiedostojen aukaisu ei ole riippuvainen maksullisista ohjelmista vaan se on mahdollista lukea maksuttomalla Acrobat Reader-ohjelmalla. Portaaliin tallennettuun materiaaliin liitetään ns. meta- eli kuvailutietoja, joiden avulla voidaan tehdä esintöjä haku-toimintoa käyttäen. [15]

Sähköposti on käyttäjän henkilökohtainen viestintäväline, jonka avulla hän voi olla yhteydessä opettajiin tai opiskelutovereihin, mutta myös ulkopuolisiin henkilöihin normaalin, selainpohjaisen sähköpostin avulla.

Puolustusvoimien koulutuksen kehittämiskeskus on määritellyt portaalin toteutusperiaatteen nousujohteiseksi. Määrittelyn lähtökohta on, että palveluiden ja käyttäjien määrä on aluksi pieni, jolloin hankitaan ja hyödynnetään saatu palaute ja pyritään vastaamaan yleisiin kysymyksiin. Samalla osoitetaan konseptin toimivuus ja rakennetaan toimiva perusratkaisu jatkokehityksen pohjaksi. Perusteiden ollessa kunnossa voidaan palvelua laajentaa uusiin kohderyhmiin ja sisältöalueisiin. Toiminnallisuutta laajennetaan ja hyödynnetään yhteisiä sovelluksia. Tavoitteet asetetaan korkealle, puhutaan visiosta, yhteisestä tahtotilasta ja asiakaskeskeisyydestä. [16]

Kuva 2. Visio koulutusportaalista. Koulutusportaalityöryhmän materiaali.

Koulutusportaali on puolustusvoimien henkilöstön ja reserviläisten käytössä. Tulevaisuuden suunnitelmiin kuuluu muun muassa kielten opetuksen lisääminen opetustarjontaan ja varusmiesten lisääminen käyttäjien piiriin. Koulutusportaali on työkalu jolla puolustusvoimat toteuttaa AVOT -ohjelmaa joka on osa hallituksen tietoyhteiskuntapolitiikkaa.

AVOT-ohjelman tavoitteena on kehittää puolustusvoimissa annettavaa koulutusta tietoyhteiskunnan tarjoamien mahdollisuuksien mukaisesti, mutta kuitenkin niin, että koulutusympäristö perustuu käytännön tarpeisiin. Uuden teknologian käyttöönotto ei saa olla itseisarvo. Kehittämisohjelmassa keskeisessä roolissa on myös työnteon ja opiskelun yhdistäminen sekä elinikäinen oppiminen. [41]

2.2.3 Oppimiskeskus

Käsitteenä oppimiskeskus on levinnyt suomalaiseen kielenkäyttöön, mutta käsitteen merkitys on monelle varmasti epäselvä. Yleisesti oppimiskeskuksella tarkoitetaan paikkaa, joka tarjoaa työvälineitä ja palveluja oppimiselle. Se tarjoaa opiskeluun ja oppimiseen tarvittavan pedagogisen, fyysisen ja sosiaalisen ympäristön. Oppimiskeskusajattelun lähtökohta on oppimisen helpottaminen ja kokonaisvaltainen edistäminen. Kaikki oppimista tukevat palvelut on koottu yhteen paikkaan.

Kehittämispäällikkö Tomi Tura Helsingin yliopistosta määrittelee oppimiskeskukselle kaksi toisistaan poikkeavaa merkitystä.

- Kun ammatillisessa koulutuksessa on etsitty uusia toimintamalleja, on syntynyt oppilaitosten yhteenliittymiä. Näitä on kutsuttu oppimiskeskuksiksi. Tämän kaltaisia alueellisia ammatillisen koulutuksen oppimiskeskuksia on muun muassa Keski-Suomessa, Kainuussa ja Kymenlaaksossa. Oppimiskeskus -käsitteellä ei tässä tapauksessa viitata yksittäiseen luokkahuoneeseen tai opetustilaan, vaan koko opetuslaitokseen ja sen tarjoamiin oppimismahdollisuuksiin ja palveluihin.

- Toinen, täsmällisempi määritys oppimiskeskukselle on puolustusvoimien käytössä. Oppimiskeskuksesta puhuttaessa tarkoitetaan fyysistä opetus- ja oppimisympäristöä joka on tarkoitettu lähi- ja etäopiskeluun. Tilaan on koottu kaikki opiskelua tukevat välineet ja palvelut. Tässä suppeammassa merkityksessä oppimiskeskus voi Turan mukaan sisältää esimerkiksi itseopiskeluun ja tiedonhakuun liittyvät tilat ja tietotekniset välineet, sekä ryhmätyöskentelyyn tarvittavat tilat ja laitteet ,opetustilat ja opettajien pedagogisen ja teknisen tuen. [42]

AVOT- kehittämisohjelman tavoitteena oli, että vuosien 2001- 2003 aikana kaikki puolustusvoimien sotilasopetuslaitokset saatettaisiin AVOT- ympäristön piiriin ja joukko-osastoihin luotaisiin valmius ottaa vastaan tietokoneavusteista opetusta. Oppimiskeskukset tuli olla käytössä kaikissa joukko-osastoissa vuoden 2003 loppuun mennessä.

Pääesikunnan budjetointiohje oppimiskeskuksen perustamiseksi määrittelee oppimiskeskuksiin kuuluvaksi mm. 2-10 henkilön rauhallisen työhuoneen tai kirjastotilan,

jonne pääsee joukko-osaston kulkuluvalla ja jonka käyttö on mahdollista virka-ajan ulkopuolella. Tilassa tulee olla puolustusvoimien hallinnollinen tietojärjestelmän (esikuntajärjestelmä) työasemat ja yhteydet sekä internet-työasemat ja -yhteydet. Tilassa on oltava muita ATK-työskentelyvälineistä mm. skanneri, piirto-ohjelma ja väritulostin.

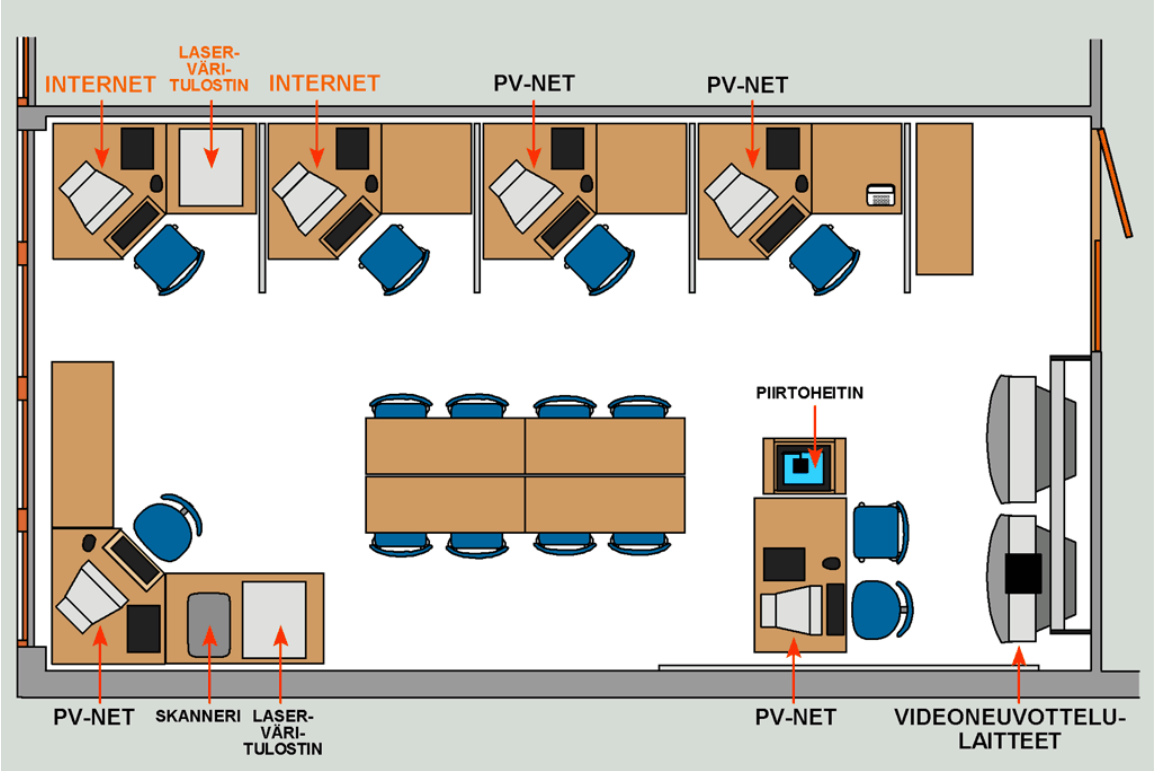
Oppimiskeskusta tulee kehittää liittämällä sinne kevyt videoneuvotteluvalmius, jolla voidaan olla sekä kuva- että ääniyhteydessä muihin joukko-osastoihin. Digitaaliset ohjesäännöt, koulutusmateriaalipalvelut ja opetusmateriaalin tuottamista palvelevat sovellukset ovat myös kehittämisen kohteena. Käsikirjaston tulee pitää sisällään puolustusvoimien ohjesäännöt, käsikirjat, oppaat ja digitaaliset julkaisut. Tilassa tulee olla opiskeluvälineitä ja sen läheisyydessä pitää olla muita opiskelu- ja ryhmätyötiloja. Sijainniksi ohje ehdottaa esimerkiksi kirjastoa, oppimateriaalikeskusta, ATK-luokkaa, varuskuntakerhon tai esikunnan tiloja.

Oppimiskeskuksen tulisi olla viihtyisä ja riittävän hyvin varusteltu opiskelupiste puolustusvoimien palkatulle henkilökunnalle ja opiskelijoille. [30]

2.2.4 Oppimiskeskus Ilmavoimien teknillisessä koulussa

Ilmavoimien teknillinen koulu toteutti oman oppimiskeskushankkeensa aikataulun mukaisesti. Tilaksi valittiin pieni luokkahuone, joka aiemmin toimi pelastuspalvelukoulutusluokkana. Kulku tilaan on järjestetty niin, että opiskelijat pystyvät käyttämään oppimiskeskusta myös virka-ajan ulkopuolella. Oppimiskeskus on kooltaan noin 20 m^2 suuruinen ja sinne on sijoitettu seuraavat laitteet.

- opettajan tietokone, josta on yhteys esikuntajärjestelmään
- videotykki
- piirtoheitin ja valkokangas
- kaksi puolustusvoimien esikuntajärjestelmään kytkettyä tietokonetta
- kuvankäsittelytietokone, jossa on tallentava CD-asema, väriskanneri ja kuvankäsittelyohjelmisto sekä värilasertulostin
- kaksi Internettyöasemaa, joihin on kytketty värilasertulostin
- videoneuvottelulaitteisto, joka koostuu kahdesta televisiosta ja kamerayksiköstä. [12]



Kuva 3. Ilmavoimien teknillisen koulun oppimiskeskus

Tilan keskellä on kahdeksan hengen ryhmätyöskentelypöytä ja seinällä valkotaulu. Valkotauluun voidaan liittää tunnistimet, joilla voidaan muuttaa järjestelmään kuuluvan erikoiskynän liikkeet kuvaksi. Kuva voidaan lähettää verkon välityksellä opiskelijoille tai opettajalle esimerkiksi toiseen joukko-osastoon.

Ilmavoimien teknillisessä koulussa oppimiskeskus ja kirjasto on erotettu toisistaan. Kirjasto on pinta-alaltaan noin 100 m^2, työllistää kaksi henkilöä ja on avoinna virka-aikana. Nimekkeitä kirjastossa on noin 4500, joista suurin osa on oppi- ja tietokirjoja. Niteitä kirjastossa on noin 17000, joista enemmistön muodostavat lentokoneiden ohjekirjat. Muita nimekkeitä ovat lehdet, kartat, videot, CD-rom-mediat ja muu kurssimateriaali. Ohjesäännöt päivitetään puolustusvoimien koulutuksen kehittämiskeskuksen ja lentokoneiden ohjekirjallisuus Lentotekniikkalaitoksen toimesta. Muu materiaali tilataan opettajien pyynnöstä kirjakaupoista. Kaikki kirjaston nimekkeet on luokiteltu kansainvälisen, yleisissä kirjastoissa käytössä olevan UDK- luokituksen mukaan. Kirjaston niteistä noin puolet on jatkuvasti lainaajilla, joita ovat koulun henkilökunta, kurssilaiset sekä varusmiehet.

Myös kaukolainaaminen on mahdollista PrettyLib- järjestelmän avulla. PrettyLib on puolustusvoimien joukko-osastojen välinen yhteistietokanta jonka avulla käyttäjä voi hakea nimekkeitä useiden joukko-osastojen kirjastoista. [36] Kirjastossa on myös opiskelijoiden käytössä internetyhteydellä varustettu tietokone.

2.3 TIETOTURVA

Tietoturvallisuus on mielenkiintoinen tarkastelualue, koska sillä on yhteys kaikkiin tietojenkäsittelyn osa-alueisiin. Edellä kuvattujen verkko-opetusympäristöjen ja tietopankkien turvallinen käyttö edellyttää sekä opiskelijalta että opettajalta tietoturvakäsitteen ymmärtämistä ja vain hyväksyttyjen toimintatapojen noudattamista. Jotta Ilmavoimien teknillinen koulu voisi menestyksekkäästi tuottaa ja julkaista lentoteknillistä opetusmateriaalia verkkotuetun monimuoto- opetuksen keinoin, on sekä sisällöntuottajien että opiskelijoiden tietoturva-asenteet, -välineet ja -osaaminen kartoitettava sekä saatava riittävälle tasolle.

Yksityiselämän suoja on perustuslaissa säädetty perusoikeus ja tietokoneen sisältö ja tietoliikenne kuuluvat sen piiriin. Tietoturvallisuus perustuu viranomaisen toiminnan julkisuudesta annetun lain (621/1999) ja asetuksen (1030/1999) lisäksi useisiin eri lakeihin, joista tärkeimpiä ovat:

- Perustuslaki (731/1999) 2.luku 10§ (Yksityiselämän suoja ja luottamuksellisen viestin salaisuus)
- Perustuslaki (731/1999) 2.luku 12§ (Viranomaisten hallussa olevien asiakirjojen ja tallenteiden julkisuus)
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Henkilötietolaki (523/1999) (Henkilötietojen käsittelyä koskevat yleiset periaatteet)
- Arkistolaki (831/1994) (Asiakirjojen laatiminen, säilytys ja käyttö)
- Valtion virkamieslaki (750/1994 17§ (Säädös valtion virkasuhteesta)
- Työsopimuslaki (55/2001)
- Rikoslaki (39/1888)34.luku 9a§ (Vaaran aiheuttaminen tietojenkäsittelylle)
- Rikoslaki (39/1888)38.luku 8§ (Tietomurto)
- Rikoslaki (39/1888)38.luku 1.kohta (Henkilötietorikos)
- Henkilötietolaki (523/1999) 48§ (Henkilörekisteririkkomus)
- Vahingonkorvauslaki (41/1974)
- Laki yksityisyyden suojasta työelämässä (477/2001)

- Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (565/1999) [32]

2.3.1 Käsitteitä

Tietoturvalla tarkoitetaan tietojen, järjestelmien ja palveluiden suojaamista uhkia vastaan normaaleissa sekä poikkeusoloissa. Uhkia on moninaisia kuten myös suojausmenetelmiä. Tietoturvaa suunniteltaessa on mietittävä:

- Mitä ja ketä vastaan suojaudutaan?
- Mitä järjestelmiä halutaan suojata?
- Kuinka tiukkaan tietoturvaan organisaatiolla on varaa? [5]

Yritysten ja muiden yhteisöjen on suhteutettava tietoturvansa uhkien vakavuuteen, tietoturvan kustannuksiin ja uhkien tekniseen kehitystasoon. Toisin sanoen tietoturvatoimet on oltava uskottavia, mutta kustannukset on kyettävä pitämään järkevässä suhteessa muuhun yritystoimintaan tai esimerkiksi koulun ollessa kyseessä, opetusmäärärahoihin. [8]

Kirjassaan ”Sähköisen viestinnän tietosuoja” Helopuro jakaa tietoturvallisuuden neljään kategoriaan. Kategoriat perustuvat Viestintäviraston luokitteluihin:

- *Toiminnan turvallisuudella* tarkoitetaan muun muassa kirjallisten ohjeiden ylläpitoa. Ohjeista tulee selvitä se miten tietoturvavaatimukset toteutetaan ja miten oman tietoturvan tasoa seurataan ja kuinka laitteet ja tiedostot suojataan luvatonta käyttöä ja pääsyä vastaan. Toiminnan turvallisuutta on myös se, että järjestelmien käyttäjätunnuksista pidetään rekisteriä. On tarpeellista pystyä valvomaan tietojen, asiakirjojen, verkkojen laitteistojen, palveluiden ja tiedostojen tietoturvaa havaitsemalla merkittävät tapahtumat. Nämä voidaan havaita järjestelmien lokitiedostoista ja verkon valvontatyökalujen avulla.

- *Tietoliikenneturvallisuudella* viitataan viestintäverkkojen turvallisuuteen. Viestintäverkoissa välitettävät viestit sekä tunnistetiedot eivät saa paljastua ulkopuolisille eikä asiaankuulumattomat saa päästä muuttamaan tai tuhoamaan viestiverkossa välitettäviä viestejä. Tietoliikenneturvallisuuteen kuuluu myös viestiverkon todentamismenettelyt, pääsynvalvontamenettelyt ja kiistämättömyysmenettelyt.

- *Laitteistoturvallisuuteen ja ohjelmistoturvallisuuteen* kuuluu ohjelmistojen ja laitteistojen valinta niin, että tietoturvauhka on vähäinen sekä tärkeiden ohjelmistojen varmuuskopiointi ja asianmukainen säilytys.

- *Tietoaineistoturvallisuuteen* kuuluu tietoaineiston käsittely turvallisesti. Tietoaineiston varmuuskopiointi, säilytys sekä asiakirjojen ja yksittäisten tietojen suojaaminen. [8]

2.3.1.1 Tunnistaminen, todentaminen ja kiistämättömyys

Tunnistaminen on menetelmä, jolla yksilöidään käyttäjä tai järjestelmä. Yksinkertaisimmillaan tunnistaminen on työtovereiden tunnistamista työympäristöön kuuluviksi.

Todentaminen on menettelyä, jolla varmistetaan, että tunnistettaessa annetut tiedot ovat paikkansapitäviä. Useat järjestelmät suorittavat tunnistamisen ja todentamisen samanaikaisesti. Esimerkiksi henkilötietoja tarkastettaessa käyttäjän tiedot tarkastetaan ajokortista ja samalla käyttäjä tunnistetaan ajokortin kuvasta. Jotkut järjestelmät tekevät valtuutuksen ja todentamisen samanaikaisesti. Esimerkkinä kulunvalvontajärjestelmä joka lukee kulkukortin ja avaa oven.

Kiistämättömyys on menettely, jolla voidaan jälkikäteen todeta jonkun henkilön suorittaneen tietyn toimenpiteen. Tietoaineistoissa tämä tarkoittaa esimerkiksi lokitiedostoja, joista nähdään kuka on muokannut tietoja. Sähköisessä viestinnässä kiistämättömyys tarkoittaa toimenpiteitä, joilla varmistutaan viestin lähettäjästä ja vastaanottajasta. [44]

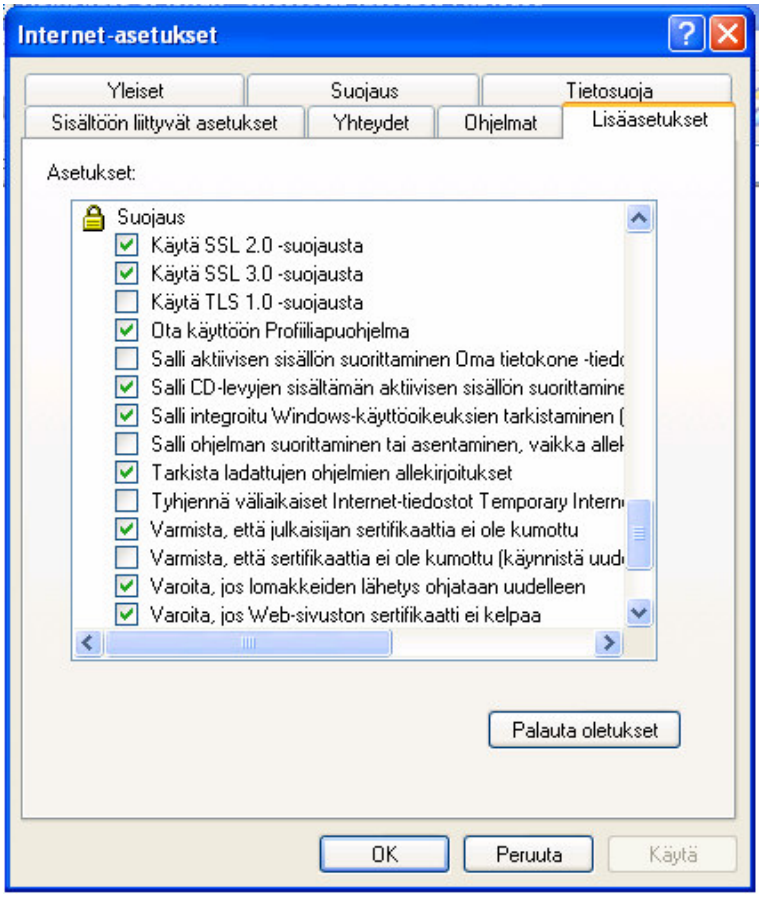
2.3.1.2 Suojauksesta ja salauksesta

Kuten aikaisemmin todettiin, internet koostuu valtavasta määrästä toisistaan riippumattomia verkkoja, reitittimiä, palvelimia ja muita tietoliikennelaitteita. Verkon alkuaikoina painopiste oli avoimuudessa, eikä suunnittelussa osattu ajatella nykyisiä tietoturvaongelmia. Internetin perusprotokolla TCP/IP on rakennettu niin, että Internetissä asioiminen sellaisenaan on turvatonta. Tätä ongelmaa korjaamaan on täytynyt kehittää salaavia yhteyskäytäntöjä sekä vahvaa todentamista käyttäviä todennusmenetelmiä.

Käyttötarkoitus määrittää salausmenetelmät ja salaavat yhteyskäytännöt ja yleistäen salaus toteutetaan joko kuljetus- tai sovellusprotokolla tasolla. Käytettäessä kuljetusprotokollatason suojausta on kaikkien ylemmän tason protokollien, kuten SMTP, FTP, HTTP liikenne suojattu. Sovellusprotokollasuojaus suojaa aina kyseisen sovelluksen, esimerkiksi www-selaimen tai sähköpostiohjelman.

Www-sivujen selaamisen suojauksessa yleisimmin käytetty protokolla on nimeltään SSL-protokolla. SSL tulee englanninkielisistä sanoista Secure Sockets Layer ja tämä protokolla tekee www-selaimen ja www-palvelimen välisen yhteyden vahvan salaamisen mahdolliseksi. Salaamisen lisäksi SSL-protokolla voi käyttää varmenteita osapuolten todentamiseksi. [44]

Microsoftin Internet Explorer selainohjelman Internet-asetuksista voidaan määrittää mitä SSL-protokollaa halutaan käyttää. SSL 2.0-protokolla on suojattujen lähetysten standardi jota kaikki web-sivustot tukevat. Toinen protokollavaihtoehto on SSL 3.0, jonka suojaus on suurempi kuin SSL 2.0:n. Ongelmaksi saattaa kuitenkin muodostua se, että kaikki web-sivut eivät tue 3.0 protokollaa. [21]



Kuva 4. Windows XP- käyttöjärjestelmän suojausasetuksia

Www-palvelimen todentaminen tapahtuu palvelimella olevan palvelinvarmenteen avulla, jonka myöntää Suomessa Väestörekisterikeskus. Niitä voidaan käyttää sekä julkishallinnon että yksityissektorin palveluiden tunnistamisessa. Palvelinvarmenteen avulla palvelun käyttäjä voi varmistua palvelun tarjoajan oikeellisuudesta ja todentaa käyttävänsä oikeaa internet-sivustoa tai muuta palvelinta eikä esim. niiden kopiota. Palvelinvarmenteet mahdollistavat myös palvelimen ja sen käyttäjän välisen tietoliikenteen salaamisen.

Käyttäjä todistaa henkilöllisyytensä www-palvelimelle tällä hetkellä yleisimmin käyttäjätunnukseen ja salasanaan perustuvalla mekanismilla, mutta myös henkilövarmenteen käyttäminen on SSL-protokollassa mahdollista. Henkilövarmenteet ovat vahvasti yleistymässä ja Väestörekisterikeskus sanookin tiedotteessaan 01.10.2005: *Syyskuun loppuun mennessä kansalaisvarmenteita oli myönnetty yhteensä 89900 henkilölle. Heillä oli voimassaolevia kansalaisvarmenteita 76200 kpl. 13000 henkilöä oli yhdistänyt henkilökorttiinsa sairausvakuutustietonsa.* Kansalaisvarmenne on standardimuodossa kerrottu henkilötieto eli sähköinen henkilöllisyys, joka perustuu julkisen avaimen menetelmään. Se sisältää mm. etu- ja sukunimen sekä sähköisen asiointitunnuksen. Kansalaisvarmenne voidaan tallentaa sähköisen henkilökortin siruun tai jopa puhelimen sim-korttiin. Varmennetta voidaan käyttää tunnistamiseen sähköisessä asioinnissa ja sähköiseen allekirjoittamiseen. [50]

Pankkipalveluista tuttuja kertakäyttösalasanoja käyttää Suomessa lähes neljä miljoonaa ihmistä. Näitä tunnuksia käytetään todentamiseen noin sadassa sähköisessä palvelussa pankkipalvelujen lisäksi. Nordean varatoimitusjohtajan Bo Harald sanoo Digitoday -lehden haastattelussa, että kertakäyttösalasanat ovat tässä vaiheessa ainoa varteen otettava ja turvallinen vaihtoehto verkkopalvelujen tunnistamismenetelmäksi. Hänen mukaansa kyse on ennen kaikkea käyttäjien valinnasta. Kertakäyttösalasanat tulivat Ruotsin verkkopankkiin 90-luvun lopulla. Samaan aikaan Pki-tunnistusta (public key infrastructure), joka on vastaava kuin edellä mainittu kansalaisvarmenne, käyttävien asiakkaiden määrä nousi 20000:sta 60000:een, mutta myöhemmin laski noin 30000 käyttäjään. Samaan aikaan kertakäyttösalasanat saivat 1,6 miljoonaa käyttäjää.

Tietojen luottamuksellisuus, eheys ja kiistämättömyys pyritään varmistamaan käyttämällä salausmenetelmiä. Salausmenetelmien käytön tavoitteena tulisi olla salaus, jonka murtaminen ei olisi mahdollista kohtuullisessa ajassa ja kohtuullisin resurssein. Tiedon tärkeys on se tekijä, joka määrittää kulloinkin mikä on kohtuullinen aika ja resurssit. On ilmiselvää, että Pentagonin tietokannat vaativat vahvemman salauksen kuin tavallisen internetin käyttäjän sähköposti.

Vahvoiksi salausmenetelmiksi kutsutaan menetelmiä joiden murtaminen ei ole mahdollista hyökkääjän laskentakapasiteetilla. Hyvässä salausmenetelmässä salaus voidaan purkaa vain käymällä läpi salausmekanismin koko avainavaruus ja kokeilemalla salauksen purkamiseen kaikkia mahdollisia salausavaimia. [45] Esimerkkinä huonosta salaustekniikasta voidaan pitää Windows käyttöjärjestelmän salasanoja. Sveitsiläiset tutkijat pystyivät jo vuonna 2003 demonstroimaan Windowsin salasanan murtamisen tavallisen kotitietokoneen laskentakapasiteetilla. Käyttäen hyväksi suurta 1,4 gigatavun taulukkoa tutkijat onnistuvat murtamaan käyttöjärjestelmän salasanan 13,6 sekunnissa. [2]

Seuraavana esimerkki salausavaimien bittimäärään vaikutuksesta salaamisen tehokkuuteen: Jos oletetaan, että yksi tietokone pystyy läpikäymään miljoona avainta sekunnissa ja yhdistetään miljoona tällaista tietokonetta, niin 40-bittisen salausavaimen purkaminen kestäisi hieman yli sekunnin. Jos käytetään 128-bittistä salausta niin vastaava aika olisi 11 triljoonaa vuotta. Valtava ero perustuu siihen että jokainen yhden bitin lisäys avainpituuteen kaksinkertaistaa mahdollisten avainten määrän.

Salausmenetelmät jakaantuvat jono- ja lohkosalaukseen. Jonosalauksessa selväkielinen teksti salataan yleensä merkki kerrallaan ja sitä käytetään lähinnä suurta nopeutta vaativissa reaaliaikaisissa sovelluksissa. Lohkosalauksessa selväkielinen teksti salataan lohko kerrallaan. Sitä käytetään yleisimmissä symmetrisissä ja epäsymmetrisissä salausalgoritmeissa. [45]

2.3.1.3 Mikä meitä uhkaa?

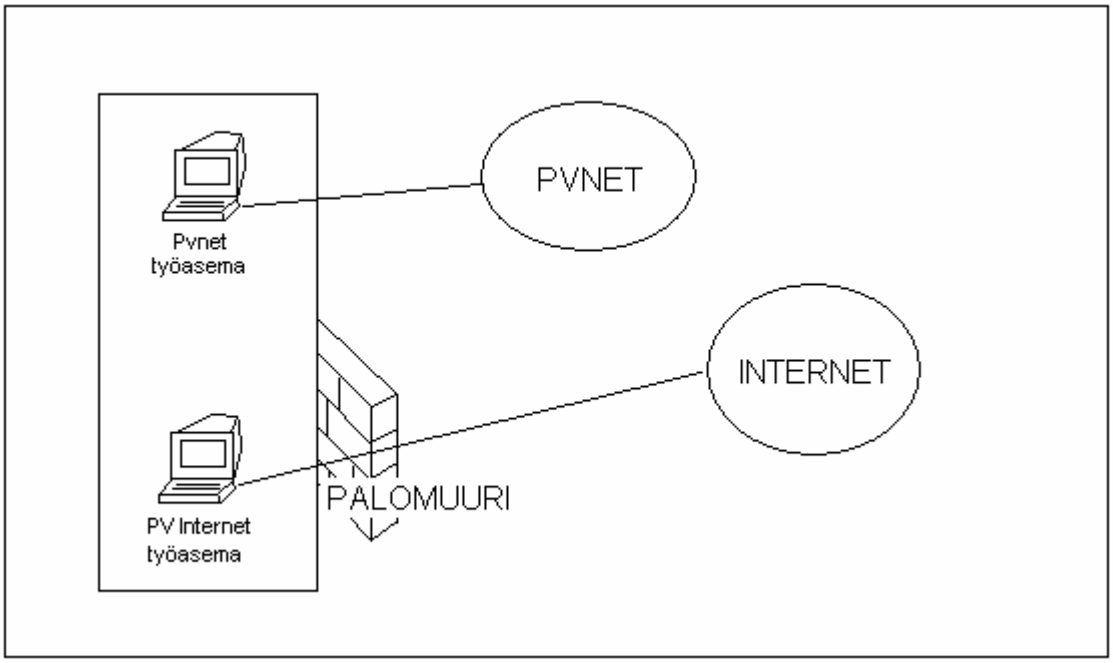
Tietoturvaa vaarantavia tekijöitä ovat muun muassa laiterikot, tietokonevirukset, sähköhäiriöt, tulipalot ja vesivahingot. Tietojen varastaminen verkkoon tai tietokoneeseen tunkeutumalla, ohjelmistoviat ja tiedostojen tahaton poistaminen ovat myös uhkia tietoturvalle. [19] Jotta vältyttäisiin tietojen tahattomalta tai tahalliselta katoamiselta, on niistä syytä ottaa säännöllisesti varmuuskopioita. Kopioita ja alkuperäistä tietoa

ei tule säilyttää samassa paikassa koska tällöin menetysriski kasvaa suureksi. Tietoja voidaan menettää eri tavoin, esimerkiksi virukset voivat poistaa tai vioittaa tiedostoja. Sähkökatkokset voivat tuhota tiedostoja ja käyttöjärjestelmän osia. Jännitepiikit saattavat fyysisesti rikkoa tietokoneen osia niin, että tietojen palauttaminen on kotikonstein mahdotonta.

Tässä tutkimuksessa painotutaan tietoturvariskeihin näkökulmasta, jossa päähuomion saa tietojen joutuminen ulkopuolisten henkilöiden käsiin. Hypoteesina voi todeta, että pääuhkan koulutusportaaliin tallennetun opetusmateriaalin tietoturvallisuudelle muodostavat rikolliset, jotka murtautuvat yksittäisen käyttäjän tietokoneelle ja sitä kautta saavat käsiinsä joko tarkoituksella tallennettua tai väliaikaisiin tiedostoihin tallentunutta tietomateriaalia.

Brittiläinen Gary McKinnon on ollut syytettynä Yhdysvalloissa tunkeuduttuaan valtionhallinnon tietokoneisiin. Syyttäjän mukaan McKinnon oli pyyhkinyt tiedostoja yli kahdestatuhannesta tietokoneesta Washingtonin sotilaspiirissä vuonna 2002 ”merkittävästi vaikeuttaen hallinnon työskentelyä”. McKinnonin väitetään aiheuttaneen tiedostojen pyyhkimisellä 300 tietokoneen verkon kaatumisen merivoimien aseasemalla. Kaiken kaikkiaan McKinnonia syytetään kahdestakymmenestä tietokonerikoksesta, joiden kohteena on ollut Yhdysvaltain armeija, merivoimat, ilmavoimat, NASA ja puolustusministeriö. [38]

Suomen puolustusvoimat on toistaiseksi säästynyt edellisen kaltaisilta rikoksilta. Tietojärjestelmämme on suunniteltu ja toteutettu siten, että PvNet on erillinen, internetistä irrotettu järjestelmä. Internetin käyttöä varten on rakennettu erillinen reititinverkko, jonka kautta internetpalveluja käytetään erillisillä työasemilla. Tämä tarkoittaa käytännössä sitä, että työntekijällä, joka tarvitsee internetpalveluja työssään, on kaksi erillistä työasemaa työpöydällään.



Kuva 5. Puolustusvoimien verkkojärjestelyt

Liikennöinti internetiin tapahtuu yhdysväylän kautta, joka on suojattu palomuurijärjestelmällä. Käytettävät palomuuriohjelmistot ovat kaupallisia COTS- tuotteita (commercial off-the-shelf), jotka eivät takaa absoluuttista turvallisuutta etenkään sodan aikana, koska mahdollinen kriisi saattaa pysäyttää ohjelmistojen vaatiman jatkuvan päivityksen. PvInternet onkin rajattu käytettäväksi ainoastaan puolustusvoimien tiloista pois lukien eräät sähköpostitoiminnot.

Pääesikunnan turvallisuusosaston pysyväisasiakirjat määrittelevät puolustusvoimien turvallisuustoiminnan päämäärät, joista tärkein on varmistaa tietojen, henkilöstön ja materiaalin turvallisuuden toteutuminen kaikissa olosuhteissa. Tietoturvallisuus on yksi turvallisuustoiminnan keskeinen osatekijä ja puolustusvoimien tavoitteena on ylläpitää korkeata tietoturvallisuuskulttuuria koko henkilöstön osalta. puolustusvoimat keskittyy myös imagon luomiseen muun yhteiskunnan keskuudessa vastuullisena ja osaavana turvallisuuden ylläpitäjänä.

Ohjeistuksen mukaan jokainen puolustusvoimissa palveleva on velvollinen ylläpitämään itsensä ajan tasalla tietoturvallisuudelle asetettujen menettelytapojen hallitsemiseksi omien tehtäviensä edellyttämässä laajuudessa. Vaikka tietoturvallisuus on paljolti teknisten apuvälineiden ja ohjelmien käyttöä, pohjimmiltaan puolustusvoimien tietovarantoon liittyvä turvallisuus on kiinni jokaisen henkilökohtaisesta panoksesta.

Tietoturvallisuus on kokonaisuus, joka puolustusvoimissa jaetaan seuraaviin osa-alueisiin:

- hallinnolliseen tietoturvallisuuteen
- henkilöstöturvallisuuteen
- tilaturvallisuuteen
- tietoliikenneturvallisuuteen
- laitteistoturvallisuuteen
- ohjelmistoturvallisuuteen
- tietoaineistoturvallisuuteen
- käyttöturvallisuuteen

Puolustusvoimien toiminnan luonne on varautumista poikkeusoloihin ja siksi sen tietoturvallisuuden tavoitteena on mahdollistaa osaltaan puolustusvoimien toimintakyky kaikissa tilanteissa, mikä tarkoittaa tietojen korkean käytettävyyden, hallitun eheyden sekä luottamuksellisuuden turvaamista hyvää tiedonhallintatapaa noudattaen.

Puolustusvoimat rakentavat tietojärjestelmänsä sekä tiedonkäsittelymenetelmänsä siten, että edellä esitetyt tavoitteet toteutuvat sekä puolustusvoimien että sidosryhmien henkilöstön osalta. Tulevaisuudessa tietoturvallisuuden merkitys puolustusvoimissa tulee kasvamaan voimakkaasti lisääntyvän kansainvälisen toiminnan myötä. [33]

2.3.2.1 Haittaohjelmat

Haittaohjelmiin kuuluvat virukset, troijan hevoset, vakoiluohjelmat ja madot. Haittaohjelmat toimivat kuten muutkin ohjelmat, mutta niiden tarkoituksena on vahingoittaa tietokonetta tai sen käyttäjää. Esimerkiksi vakoiluohjelmilla voidaan kerätä käyttäjän henkilötietoja ja käyttää niitä rikollisiin tarkoituksiin. Käyttäjä saattaa tietämättään asentaa vakoiluohjelman internetistä ladatun freeware- ohjelman (ilmaisohjelma) osana. Madot ja virukset voivat asentaa itsensä suojaamattomaan tietokoneeseen ja kopioitua myös muihin samassa verkossa oleviin koneisiin.

Virus

Virus on ohjelma, joka aiheuttaa häiriöitä tai vahinkoa tietokoneelle tai ohjelmille. Yleensä tämä tapahtuu käyttäjän huomaamatta. Viruksen ensisijainen tehtävä on kopioitua ja levittäytyä mahdollisimman moneen tietokoneeseen. Virus saattaa pysyä huomaamatta kunnes se käynnistää siihen ohjelmoidun toimenpiteen tai kun virustorjuntaohjelma varoittaa siitä. Viruksia esiintyy omana tiedostonaan, toisten tiedostojen liitännäisenä tai se voi piileskellä levyaseman käynnistyslohkossa. Virukset pääsevät tietokoneisiin useimmiten sähköpostin liitetiedostojen tai internetistä ladattujen tiedostojen kautta. Viruksia voidaan sijoittaa myös web-sivuihin, joista ne pääsevät tunkeutumaan vierailijan tietokoneeseen.

Kuva 6, Brian-virus 5,25” levykkeellä tietoturvayhtiö F-Securen arkistossa.

Ensimmäinen virus havaittiin PC-mikrossa tammikuussa 1986. Brian-niminen virus tartutti levykkeitä muuttamalla niiden käynnistyssektoria. Viruksen tehtävä oli kirjoittaa levykkeen nimeksi © Brian. Tänä päivänä virukset tai kuvaavammin haittaohjelmat eivät ole yhtä harmittomia kuin Brian. Vuoden 2004 keväällä maailmalla koettiin laaja haittaohjelmakoodaajien välinen ”virussota”. Tuolloin tietoverkoissa havaittiin runsaasti Netsky-, Mydoom- ja Bagle- perheiden haittaohjelmia.

Uusia viruksia ilmaantuu joka päivä, ja virusten leviämistavat lisääntyvät jatkuvasti. Vuonna 2000 liikkeellä oli 45 000 erilaista virusta ja vuonna 2005 virusten määrä oli lisääntynyt 150 000:een. F-Secure tietoturvayhtiön tutkimuspäällikkö Mikko Hyppönen ennustaa, että seuraava virussukupolvi hyödyntää levittäytymiseensä langattomia wlan-verkkoja. [6]

Koodaajien ja liikkeellelaskijoiden motiivit ovat muuttuneet maineen tavoittelusta taloudelliseen hyötyyn. Enää päätarkoituksena ei ole tuhota saastunut järjestelmä vaan saada saastunut järjestelmä haltuun. Kaapattuja järjestelmiä on käytetty roskapostin levittämiseen, uusien haavoittuvien tietojärjestelmien etsimiseen, www-palvelimina huijaussivustoille sekä alustoina palvelunestohyökkäyksille. [19]

Palvelunestohyökkäys (Denial of Service, DoS) tarkoittaa tietyn verkkopalvelun lamauttamista niin, että palvelu ei ole käytettävissä. Palvelunestohyökkäyksiin liittyy yritysten uhkailua ja kiristämistä. Esimerkiksi kesäkuussa 2004 brittiläisiä vedonvälitystoimistoja, jotka aiemmin olivat kieltäytyneet maksamasta tuhansien puntien suuruisia kiristysrahoja, joutui järjestelmällisten palvelunestohyökkäysten kohteeksi. Periaate on yksinkertainen. Maailmalla on internet- verkkoon kytkeytyneenä lukematon määrä huonosti suojattuja tietokoneita, jotka ovat saastuneet vakoiluohjelmilla, viruksilla, troijalaisilla ja madoilla. Rikollisilla on kyky alistaa näitä koneita hallintaansa ja pakottaa ne yhdistämään itsensä esimerkiksi yhteen web-sivuun. Kun tuhannet tietokoneet yrittävät yhtäaikaisesti yhteyttä sivustoon sen liikenne tukkeutuu eivätkä todelliset asiakkaat saa haluamaansa palvelua. Palvelunestohyökkäystä on lähes mahdoton estää, koska orjatietokoneita voi olla tuhansia ja ne ovat sijoittuneet ympäri maailmaa.

Madot

Madot leviävät tietokoneesta toiseen nopeammin kuin virukset. Madot jaetaan kahteen pääluokkaan: Sähköpostimadot ja verkkomadot.

- Sähköpostimadot voivat kerätä tietokoneesta tietoa, kuten liitetiedostoja. Madot leviävät lähettämällä itsensä sähköpostiohjelman osoitekirjaan tallennettuihin sähköpostiosoitteisiin. Vuonna 2004 arvioitiin, että kaikesta sähköpostiliikenteestä jopa 10 % oli Mydoom- sähköpostimatojen leviämisestä aiheutuvaa liikennettä. [3] Operaattoreilla on mahdollisuus säätää sähköpostipalvelimiensa suodattimia siten, että madot eivät pääse kohteeseen. Uuden madon ilmestyessä operaattorien nopea reagointi saattaa pelastaa suurilta vahingoilta, silti osa madoista pääsee kohteeseensa, jolloin sen leviämisen ja tietojen varastamisen voi estää ainoastaan käyttäjän nopeasti päivittyvä tietoturvaohjelmisto.

- Verkkomadot skannaavat avonaisia verkkoon kytkettyjä tietokoneita. Kun mato löytää koneen, jossa ei ole ajan tasalla olevaa palomuuria, se pyrkii ottamaan koneen haltuunsa. Verkkomadot eivät juuri tuhoa koneiden tietoja vaan kaapatut koneet alistetaan niin kutsuttujen bot- tai zombieverkkojen osaksi, jolloin haltuun ottaja voi käyttää niiden tietojenkäsittelykapasiteettia palvelunestohyökkäyksiin ja roskapostin lähettämiseen. Bot- verkko -termi juontuu robotti-sanasta. Verkon jäseninä tahtomattaan olevat tietokoneet ovat isäntänsä komennossa kuin valtava zombie- tai robottiarmeija. [4] [6]

Troijan hevoset

Myyttinen Troijan hevonen vaikutti lahjalta kreikkalaisilta troijalaisille, mutta sen sisällä oli kreikkalaisia sotilaita, jotka valloittivat Troijan. Tietokoneisiin tunkeutuvan troijan hevosen harmillinen ominaisuus on, että se saattaa näyttää tavalliselta ohjelmalta. Esimerkiksi tietokonepeli saattaakin olla troijan hevonen, joka poistaa tietokoneesta tiedostoja. Troijan hevoset ovat ongelmallisia koska virustorjuntaohjelmistot eivät pysty niitä poistamaan. Virustorjuntaohjelma tosin osaa tunnistaa troijan hevoset ja nimeää ne uudelleen estäen niiden automaattisen käynnistymisen, mutta lopullinen poistaminen täytyy tehdä käyttäjän toimenpitein. Vuonna 2005 liikkeellä oli sähköpostimuotoinen troijan hevonen, jonka liitetiedostojen väitettiin olevan Microsoftin tietoturvapäivityksiä. Todellisuudessa liitteet olivat viruksia, joiden tarkoituksena oli virustorjunta- ja palomuuriohjelmien poistaminen käytöstä. Tutkija vastaanotti 4.9.2005 sähköpostin, jonka lähettäjäksi väitettiin Microsoft Corporation Security Section. Viestissä oli liitteenä tiedosto, jonka sanottiin korjaavan kaikki Microsoftin tuotteissa olevat tunnetut tietoturva-aukot. Viestiin oli uskottavuuden lisäämiseksi liitetty aitoja linkkejä Microsoftin internetsivuille. Microsoft, kuten myös monet tietoturvayhtiöt ovat ilmoittaneet, etteivät he lähesty asiakkaitaan sähköpostitse. Näin ollen voidaan olettaa, että kaikki heidän nimissään tuleva sähköposti on niin sanottua roskapostia tai rikollisissa aikeissa lähetettyjä haittaohjelmia sisältävää sähköpostia.

Vakoiluohjelmat

Vakoiluohjelma seuraa tietokoneen käyttäjätietoja ja lähettää niitä sivullisille internetin välityksellä käyttäjän sitä tietämättä. Usein vakoiluohjelma kerää tietoa internetin käyttäjän selauskäyttäytymisestä mainostarkoituksiin. Käyttäjä voi huomata tämän muun muassa aloitussivun vaihtumisena, epäilyttävien pop-up- (ponnahdus) ikkunoi-

den ilmestymisenä tai selaimen osoiterivin alapuolelle ilmestyvänä näppäinpalkkina, joka mainostaa esimerkiksi lääkkeitä tai asuntolainoja. Ikävimmillään vakoiluohjelmat voivat siirtää henkilökohtaisia tiedostoja tietokoneesta tai seurata mitä näppäimistöllä kirjoitetaan. Vakoiluohjelmat voivat asentaa itsensä tietokoneeseen käyttäjän tietämättä jonkin ohjelmiston osana. Tällaisia ovat esimerkiksi suosittu Kazaa vertaisverkko-ohjelma, useat ilmaispelit ja monet mediasoittimet. Paras tapa suojautua vakoiluohjelmilta on tietokoneen säännöllinen tutkiminen ja puhdistaminen haitallisten mainosten (adware) poisto-ohjelmalla, joita ovat esimerkiksi ilmaiset Ad-Aware ja Spybot. Adware puhdistusominaisuus on liitetty myös useimpiin kaupallisiin tietoturvaohjelmistoihin. Julkiset ja jaetut tietokoneet ovat houkuttelevia kohteita vakoiluohjelmille, joten henkilökohtaisten tietojen käsitteleminen ja salasanoja vaativien palvelujen käyttäminen niillä ei ole suotavaa.

Rootkit-ohjelmat

Rootkitit ovat esimerkiksi näkymättömiä vakoiluohjelmia tai troijalaisia, joiden avulla tietokoneesta voidaan varastaa tietoa. Rootkit nimi on periytynyt Unix-ympäristön pääkäyttäjältä (root=juuri), jolla on järjestelmän ylimmän tason käyttöoikeudet. Root-oikeudet tarkoittavat siis järjestelmänvalvojan oikeuksia, joilla voidaan esimerkiksi muokata käyttöjärjestelmää ja korvata perustoimintoja. Tätä ominaisuutta hyödyntäen rootkit- ohjelma voi piilottaa itsensä, muokata tiedostojen ominaisuuksia, laitteen rekisterimerkintöjä tai käynnissä olevia toimintoja. Rootkit- ohjelma voi piilottaa näkyvistä myös muita haittaohjelmia. Vahingollinen koodi piilotetaan niin hyvin, että käyttöjärjestelmä tai tavanomaiset tietoturvatuotteet, kuten virustorjuntaohjelmat ja vakoiluohjelmien poistoon erikoistuneet ohjelmat, eivät pysty havaitsemaan niitä.

2.3.3 Ohjelmistojen tietoturva-aukot

Käyttöjärjestelmät

Kräkkerit eli tietomurtoja tekevät tietokonerikolliset ovat erityisen kiinnostuneita hyökkäämään ohjelmistojätti Microsoftia vastaan. Syy tähän arveluttavaan suosioon on se, että Microsoftin tuottamat Windows-käyttöjärjestelmät ovat maailman käytetyimpiä ja uuden tietoturva-aukon löytäminen Windowsista ja sen hyväksikäyttäminen tuo kräkkerille mainetta omiensa joukossa.

Yleensä Microsoft onnistuu julkaisemaan ohjelmistopäivityksen ennekuin löydettyä tietoturva-aukkoa hyväksikäyttävät haittaohjelmat leviävät verkkoon. Julkaistut tietoturvapäivitykset on ladattavissa internetistä ja käyttöjärjestelmä asentaa päivitykset automaattisesti tai vaihtoehtoisesti ilmoittaa käyttäjälle, että uusi päivitys on saatavilla. Microsoft julkaisee tuotteilleen myös päivityskokoelmia. Nämä niin kutsutut Service Pack:it koostuvat kunkin ohjelmiston siihenastisista päivityksistä ja niitä on usein saatavissa valmistajan web-sivujen lisäksi myös CD-levyllä. Tietoturvaongelman muodostavat ne miljoonat internetiin kytketyt tietokoneet, jotka eivät päivitä itseään automaattisesti. Näissä tietokoneissa käyttäjä on tietoisesti tai epähuomiossa evännyt käyttöjärjestelmän päivitykset. Myös väärällä todennuskoodilla asennetut piraattikopiot ovat vaarassa, koska Microsoft on ottanut käyttöönsä kovat aseet piratismia vastaan ja estää ohjelmistopäivitykset niihin ohjelmistoihin, jotka se uskoo olevan laittomia. [26]

Joulukuussa 2005 Microsoft Windows- käyttöjärjestelmissä havaittiin vakava tietoturva-aukko, jonka paikkaamiseen ei ollut saatavissa työkalua. Ongelmasta uutisoitiin laajasti ja siitä on saatavilla paljon tietoa, jota tutkija käyttää havainnollistaakseen sitä aikajännettä, jolla ohjelmistovalmistajat ja toisaalta ohjelmistohaavoittuvuuksien hyväksikäyttäjät toimivat pystyvät reagoimaan.

Seuraavassa havaitun tietoturva-aukon havaitseminen, hyväksikäyttö ja korjaamistoimet päivämääriin sitoen:

Keskiviikko, 28. joulukuuta, 2005

Maailmalla leviää tieto, jonka mukaan Windows käyttöjärjestelmissä on havaittu vakava tietoturva-aukko. Mm. Viestintävirasto tiedottaa, että ilmeisesti Windows-käyttöjärjestelmän grafiikan käsittelyrutiineihin kohdistuvaa haavoittuvuutta hyödyntävää haittaohjelmakoodia on julkaistu tietoturva-aiheisella postituslistalla. Tällä hetkellä haavoittuvuuteen ei ole saatavilla korjausta. Ainakin Internet Explorer -käyttäjät voivat saada haittaohjelmatartunnan käymällä haitallisen tiedoston sisältävällä www-sivustolla. Haavoittuvuutta voidaan mahdollisesti hyväksikäyttää myös muiden selainohjelmistojen kautta. Haavoittuvuuden sisältävä tiedosto voidaan välittää myös sähköpostiviestin liitetiedostona.

Suojautumissuosituksena on tällä hetkellä estää WMF (Windows Metafile) -kuvatiedostojen siirtyminen organisaation www- proxypalvelimen (välityspalvelin)

kautta sekä estää yhteydenotot unionseek.com -domainissa sijaitsevaan www-palvelimeen. [46]

Torstai, 29. joulukuuta, 2005

Microsoft julkaisee turvallisuustiedotteen ja vahvistaa tietoturva-aukon. Microsoft luokittelee aukon kriittiseksi. Ongelma koskee käyttöjärjestelmiä Windows ME, Windows 2000, Windows XP and Windows 2003. Tietoturvayhtiö F-Secure kertoo, että toistaiseksi aukkoa on hyödyntänyt vain vakoiluohjelmat sekä epäaidot vakoiluohjelmien poisto-ohjelmat. F-Secure toteaa pahoitellen, että pian oikeat virukset tulevat käyttämään haavoittuvuutta hyväkseen.

Perjantai, 30. joulukuuta, 2005

Viestintäviraston CERT-FI –yksikkö (Computer Emergency Response Team) julkaisee Windows WMF -haavoittuvuuden johdosta CERT-FI –varoituksen, jossa kerrotaan, että haavoittuvuuden hyödyntäminen on kehittymässä yksittäisistä haitallisista www-sivustoista www-sivujen banner-mainontaan. Viestintävirasto varoittaa, että tämä kehitys voi laajentaa vaarallisten www-sivustojen määrää huomattavasti. Ensiavuksi tarjotaan varovaisuutta www-sivujen selailussa ja kehotetaan huolehtimaan siitä, että Windows-käyttöjärjestelmän sekä virustorjuntaohjelmiston automaattipäivitykset ovat päällä. Kevin Kean MSRC:stä (Microsoft Security Response Center) vastaa lukuisiin kyselyihin siitä, voiko haavoittuvuutta hyödyntää sähköpostin kautta? Keanin mukaan asiakkaan pitäisi avata liitetiedosto tai sähköpostin web-linkki, jotta vahinkoa voi tapahtua. Kean sanoo myös, että järjestelmänvalvojan käyttäjätunnuksilla tietokonetta käytettäessä on suurempi riski saada virus, kuin matalamman tason käyttäjätunnuksia käytettäessä. F-Secure kertoo aukkoa hyväksikäyttävien troijan hevosten määrän kasvavan voimakkaasti. Yhtiön tiedotteen mukaan voi olla järkevää olla käyttämättä kuvankäsittelyohjelmia loppuvuonna. [23]

Lauantai, 31. joulukuuta, 2005

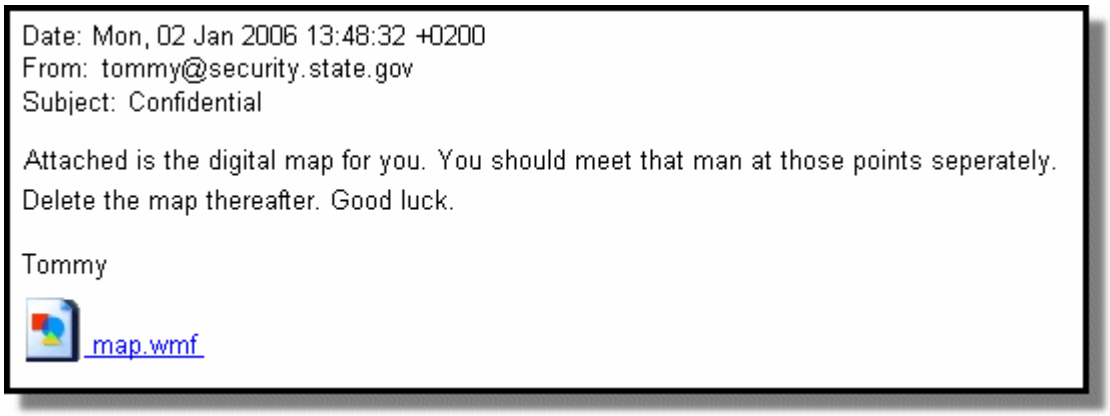
”Ensimmäinen WMF-haavoittuvutta hyväksikäyttävä mato on löytynyt”, kertoo F-Secure ja jatkaa ”Onneksi se ei näytä olevan kovin vakava. Liikkuu tietoa, että pikaviestiohjelma MSN Messengerin välityksellä leviää linkki kuvatiedostoon nimeltään "xmas-2006 FUNNY.jpg". Kuvatiedostoon viittaavasta jpg- päätteestä huolimatta linkki pitää sisällään vahingollisen WMF- tiedoston, jota virustorjuntaohjelmat eivät tunnista. [7]

Sunnuntai, 1. tammikuuta, 2006

Uutta WMF- haittaohjelmakoodia levitetään roskasähköpostiviestin liitetiedostona, viestin otsikkona on "Happy New Year". Ilfak Guilfanov julkaisee epävirallisen korjaustiedoston WMF- haavoittuvuuteen. Useat eri tietoturvatoimijat ovat analysoineet korjaustiedostoa ja todenneet sen toimivaksi. Viestintävirasto suosittelee, että kyseinen epävirallinen korjaustiedosto poistetaan, kun virallinen Microsoftin laatima korjaustiedosto julkistetaan. Guilfanovin päivityksellä ei ole Microsoftin tukea eikä hyväksyntää.

Maanantai, 2. tammikuuta, 2006

Tietoturvayhtiö F-secure kertoo tapauksesta, jossa viestinnän tietoturvapalveluja tarjoava Messagelabs on pysäyttänyt WMF- hyökkäyksen. Etelä-Koreasta liikkeelle lähteneen sähköpostin kohteena on ollut korkean joukko profiilin osoitteita. Viestin liitteenä oli kartaksi väitetty WMF- tiedosto, joka todellisuudessa avasi tietokoneesta takaportin ja mahdollisti ulkopuolisen tunkeutumisen tietokoneelle.


Date: Mon, 02 Jan 2006 13:48:32 +0200
From: tommy@security.state.gov
Subject: Confidential

Attached is the digital map for you. You should meet that man at those points seperately.
Delete the map thereafter. Good luck.

Tommy

map.wmf

Kuva 7. Vaarallinen viesti

Tiistai, 3. tammikuuta, 2006

Microsoft päivittää tietoturvatiedotettaan kertoen, että WMF- haavoittuvuuteen on saatu valmiiksi päivitys. Tietoturvapäivitys täytyy kuitenkin vielä testata yhteensopivuus- ja laatuseikkojen vuoksi. Tietoturvatiedotteen mukaan Microsoftin tavoitteena on julkaista tietoturvapäivitys tiistaina 10. tammikuuta 2006 normaalin päivitysaikataulunsa mukaisesti. Viestintävirasto suosittelee käyttäjän toimenpiteiksi pidättäytymistä kuvankäsittelystä ja varauksella suosittelee epävirallista Guilfanov- päivitystä.

Keskiviikko, 4. tammikuuta, 2006

WMF- aukkoa hyväksikäyttäviä troijalaisia levitetään sähköpostin välityksellä. F-Secure ilmoittaa, että valtava liikennemäärä Ivan Guifanovin sivustoille on tukkinut liikenteen ja sivut on ajettu alas palveluntarjoajan toimesta.

Torstai, 5. tammikuuta, 2006

Microsoft on julkaissut WMF-haavoittuvuuden korjaavan tietoturvapäivityksen. Yhtiö on julkaissut päivityksen nopeammalla aikataululla eli normaalin päivitysaikataulunsa ulkopuolella. Microsoft keskeytti päivityksen testaamisen ja julkaisi päivityksen viisi päivää ennakoitua aikaisemmin.

Tapahtumien kulku antaa kuvan siitä, minkälaisella aikajänteellä ohjelmistotalot ja hyväksikäyttäjät reagoivat uusiin haavoittuvuuksiin. On merkittävää, että Microsoft kykeni julkaisemaan käyttöjärjestelmän korjauspäivityksen näinkin nopeasti, sillä uusia hyväksikäyttömenetelmiä ilmestyi päivittäin. Tietoturvayhtiöt pelkäsivät päivityksen viivästymisen aiheuttavan maailmanlaajuisen hyökkäyksen, jonka taloudelliset seuraukset olisivat saattaneet olla merkittävät. [23], [7], [46]

Internet-selaimet

Microsoft Internet Explorer -selaimesta on löydetty jälleen uusi haavoittuvuus, johon on myös julkisesti saatavilla oleva hyväksikäyttömenetelmä. Haavoittuvuuden hyväksikäyttö on suhteellisen yksinkertaista, joten sen laajamittainen hyväksikäyttö lähitulevaisuudessa voi olla mahdollista. Haavoittuvuuteen ei ole tällä hetkellä saatavissa korjauspäivitystä. [49]

Internetselainten turvallisuudesta on keskusteltu viimeaikoina vilkkaasti. Kohteena on ollut pääasiassa Microsoftin Explorer-selaimeen, koska se on ollut hakkereiden ja virusten kirjoittajien erityisen mielenkiinnon kohteena. Toinen suosittu selain Firefox on saanut olla hyökkäyksiltä melko rauhassa aina viimeaikoihin saakka. Firefoxin lisääntynyt käyttö on lisännyt myös tietoturva-aukkoja hyväksikäyttävien ohjelmistojen määrää internetissä. Viestintävirasto kehottaa 9.8.2005 julkaistussa varoituksessa käyttäjiä päivittämään Firefox- ja Mozilla-selainohjelmistot sekä Thunderbird sähköpostiohjelmistot uusiin versioihin. Mozilla.org on määritellyt ohjelmistojen haavoittuvuuksista kaksi kriittiselle ja neljä korkealle vakavuustasolle ja osaan on jo julkistet-

tu hyväksikäyttömenetelmiä. Osa haavoittuvuuksista mahdollistaa hyökkääjän oman ohjelmakoodin suorittamisen kohdetietojärjestelmässä. [47]

Selainhaavoittuvuuksia on siis havaittu kaikissa ohjelmistoissa ja Windows-ympäristön lisäksi myös Linux-käyttöjärjestelmässä. Käyttäjän kannalta onkin tärkeää seurata oman selaimensa tietoturvatiedotteita ja asentaa selainpäivitykset säännöllisesti.

Internet selaimiin liittyvät myös evästeet (cookie, pipari) eli pienet tekstitiedostot, joita selain tallentaa käyttäjän tietokoneelle. Evästeistä ja niiden käyttötarkoituksesta on selkeästi kerrottava www-sivuston käyttäjälle ja niiden tallentaminen ja käyttö on oltava mahdollista kieltää. (Sähköisen viestinnän tietosuojalaki 7§). Evästeitä käytetään esimerkiksi, kun halutaan säilyttää käyttäjän web-istuntoon liittyviä tietoja käyttäjän siirtyessä sivulta toiselle. Se voi pitää sisällään satunnaisen tunnusluvun, joka nopeuttaa sivustolla tapahtuvia kirjaustapahtumia. Evästeen avulla on myös mahdollista seurata käyttäjän sivustolla tekemiä valintoja ja muokata sivustoja tekijän määrittämällä tavalla. Evästeet tallentuvat tietokoneen kiintolevylle cookies- nimiseen tiedostoon koodattuina, eikä niiden tietoja voida lukea selkokielisenä.

Pysyvä (persistent) eväste ei poistu kun selain suljetaan ja näin web-sivu lukee evästeen myös seuraavalla vierailukerralla.

Tilapäinen (session) eväste tallentuu vain kyseisen yhteyden ajaksi ja poistuu tietokoneelta kun selain suljetaan.

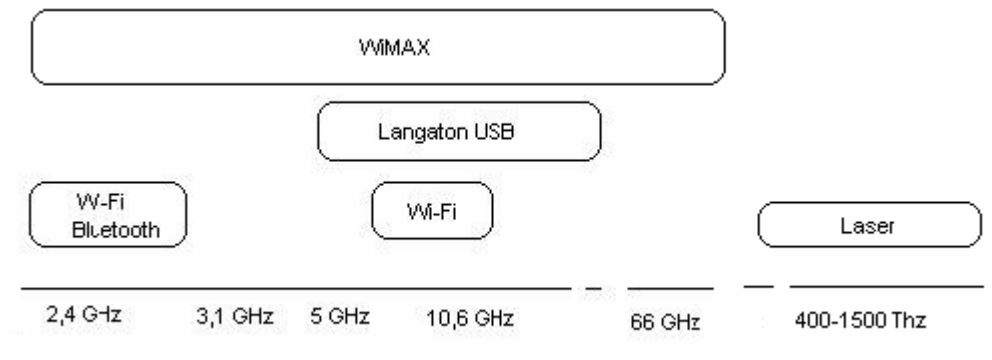
Jäljittävä eväste (tracking cookie) tallentaa tietoja web-sivuista joilla käyttäjä on vieraillut ja käyttää näitä tietoja mm. markkinoinnissa. Tietokoneeseen jääneet tracking cookiet aiheuttavat esimerkiksi harmillisia ponnahdusikkunoita sekä saattavat avata selaimeen ei toivottuja web-sivustoja. [5, s407]

2.3.4 Langattomuus

Langattomat tiedonsiirtotekniikat ovat viime aikoina yleistyneet kodeissa sekä kotiverkon perusrakenteena että yksittäisten laitteiden ja tietokoneen välisessä kommunikoinnissa. Perinteisessä, johtoihin perustuvassa tiedonsiirrossa digitaalinen tieto siirtyy elektronien liikkeenä, eli sähkövirtana laitteiden välillä. Johtimissa kulkee yleensä siniaaltomuotoinen kantoaalto, johon voidaan koodata digitaalista informaatiota moduloimalla taajuutta tai vaihetta. Valokuiduissa tieto liikkuu lasersäteen pulsseina valon voimakkuuden pysyessä vakiona.

Langattomissa yhteyksissä tieto siirtyy säteilynä eli sähkömagneettisen kentän aaltoliikkeenä. Edetäkseen säteily ei tarvitse väliainetta, joten se etenee niin tyhjössä kuin aineiden läpi, mutta säteilyn aallonpituus vaikuttaa sen läpäisykykyyn. WiFi –tavaramerkkiä käyttävän langattoman kotiverkon taajuusalue on 2,4 GHz alueella. Lähettimissä käytetään tavallisesti ympärisäteileviä antenneja, jotka lähettävät ja vastaanottavat säteilyä kaikkialta. Tämän hyvän vastaanottokyvyn haittapuolena ovat turvallisuusongelmat, sillä radioliikenne on helposti ulkopuolisten kuultavissa ja ainoa tehokas vastakeino salakuuntelulle on lähetteen vahva salaaminen.

Langattomiin yhteyksiin lukeutuu myös lyhyisiin yhteysväleihin tarkoitettu Bluetooth, langaton USB-väylä (Universal Serial Bus), Gsm-puhelimilla muodostetut GPRS-yhteydet ja tuleva WiMAX (Worldwide Interoperability for Microwave Access), jota kehitetään kotiverkkoja järeämpiin, ulkoilmaan rakennettaviin langattomiin verkkoihin. Yksi WiMAX-verkon sovellus voisi olla laajakaistayhteyksien tarjoaminen syrjäseuduille. Myös muut operaatiotason ratkaisut, joissa maahan kaivettava kaapelointi ei ole kannattavaa, voivat olla tulevaisuudessa WiMAX-pohjaisa. WiMAX:n kantamaksi luvataan maksimissaan 50 kilometriä ja tiedonsiirtonopeudeksi 70Mbps. [24]



Kuva 8. Langattomien verkkojen taajuusalueita

Langattomiin verkkoihin liittyminen saattaa taajaan asutulla alueella tapahtua jopa huomaamatta. Langattomalla vastaanottimella varustettu tietokone voidaan määritellä niin, että se etsii alueella olevia langattomia verkkoja ja huolimaton käyttäjä saattaa vahingossa hyväksyä liittymisen vieraaseen, salaamattomaan verkkoon. Langattomia yhteyksiä rakennettaessa on syytä käyttää vahvinta mahdollista järjestelmän tarjoamaa salausta. Esimerkiksi Wlan-verkkojen (Wireless Local Area Net) ensimmäisen sukupolven WEP-salaus (Wired Equivalency Privacy) on melko helposti murrettavissa, vaikkakin se estää satunnaisten ohikulkijoiden kytkeytymisen. WEP-salauksen avaimen voi määritellä automaattitoiminnolla tai manuaalisesti, jolloin käyttäjä voi myös määrätä avaimen pituuden (40 tai 104 bittiä). Tämä tarkoittaa, että käyttämällä pidempää avainta saadaan parempi suojaus.

Uudemmat langattomat verkkosovittimet tukevat WPA (Wi-Fi Protected Access) suojausprotokollaa. WPA-salauksessa verkossa olevien tietokoneiden ja laitteiden verkkoavaimet vaihdetaan automaattisesti ja todennetaan säännöllisesti, mikä takaa paremman suojauksen kuin WEP-salaus.

Kahta edellistä protokollaa vahvemman salauksen tarjoaa 802.1x-todennus, joka mahdollistaa käyttäjien ja tietokoneiden käyttäjätietojen tarkastuksen. IEEE 802.1x –todennus (Institute of Electrical and Electronic Engineers) käyttää EAP (Extensible Authentication Protocol) –suojauslajeja, jotka mahdollistavat mm. älykorttien käytön todentamismenetelmänä. Tämä parantaa verkon turvallisuutta huomattavasti avainpohjaiseen salaukseen verrattuna. [51]

Vähemmän tunnettu uhka langattomalle tiedonsiirrolle on lyhyiden etäisyyksin Bluetooth-yhteys. Bluetooth käyttää yhteyden muodostamiseen korkeataajuista radiolinkkiä jonka kantama on suuntaamattomana muutamista metreistä noin kymmeneen metriin. Yleisiä bluetooth- laitteita ovat matkapuhelimet ja niiden lisälaitteet kuten handsfree-laitteet sekä GPS-navigaattorit. Bluetooth-yhteyttä käytetään myös tietokoneiden ja puhelimien väliseen kommunikointiin sekä kameroiden ja tulostimien tiedon siirtoon. [28] Avointa ja salaamatonta Bluetooth-yhteyttä voidaan salakuunnella tehokkaalla suunta-antennilla kaukaakin.

Kuva 9. Itse valmistettu Bluetooth- salakuuntelulaite

Rakennusohjeet sekä tarvittavat ohjelmistot kuvan laitteelle löytyvät internetistä. Tietoturva-ajattelua ravistelevaa laitteessa on se, että väittämän mukaan sillä voidaan skannata bluetooth-yhteyksiä jopa kilometrin päästä. Artikkelissa väitetään, että viidessä minuutissa laitteella löydettiin kaksikymmentä bluetooth-yhteyttä kilometrin päässä olevasta toimistorakennuksesta. Tutkimuksellisesti on huomioitava lähdekritiikki koska kyseessä on harrastajien ylläpitämä internet-sivusto. [43]

2.4 SUOJAUTUMINEN

2.4.1 Virustorjunta

Kotikäyttäjä toteuttaa tietokoneensa virustorjunnan pääsääntöisesti työasemaan asennetulla virustorjuntaohjelmistolla, jonka vaihtoehtona on tiedostopalvelimelle asennettu virustorjuntaohjelmisto. Kuukausittain ilmestyy jopa satoja uusia haittaohjelmia ja tästä syystä virustorjunta on siirtynyt osaksi verkkopalveluja. Virustorjuntaohjelmistoja käytetään erityisesti sähköpostipalvelimissa, tiedostopalvelimissa ja www-palvelimissa, jotka vastaanottavat liikennettä käyttäjän työasemilta ja ulkoverkosta. Esimerkiksi sähköpostiliikenteestä pyritään jo palvelimella poistamaan sellaiset viestit, jotka sisältävät haittaohjelmia. Näin vähennetään virusten ja muiden haittaohjelmien kotikoneille aiheuttamaa vahinkoa. Palvelimella toteutettu virustorjunta ei pysty estämään kaikkien haittaohjelmien pääsyä kotitietokoneelle ja näin ollen myös työasemalla tulee olla ajan tasalla oleva virustorjuntaohjelmisto.

Työasemaan tai tiedostopalvelimeen tarkoitettu virustorjuntaohjelmisto toimii kahdessa perustilassa, joita ovat staattinen tiedostojen tarkastustila ja reaaliaikainen tarkastustila. Staattisessa tarkastustilassa voidaan tarkastaa järjestelmään liitettyjä kovalevyjä, levykkeitä, CD-levyjä, USB-massamuisteja tai muita tietolähteitä virusten varalta. Reaaliaikaisessa tarkastustilassa ohjelmisto tarkkailee työaseman tietoliikennettä ja vertaa vastaanotettuja tiedostoja virustietokantaansa. Virustorjuntaohjelmisto voidaan määrittää siten, että se poistaa havaitsemansa haittaohjelmat tietokoneelta tai asettaa ne karanteeniin myöhempää tarkastelua varten. [48]

Virustorjuntaohjelmistoja on saatavissa kaupallisesti ja internetistä ladattavina ilmaisohjelmina. Oleellinen ero kaupallisten ja ilmaisten virustorjuntaohjelmien välillä on tietokantojen päivittyminen. Kaupalliset ohjelmistoyritykset työskentelevät jatkuvasti ja tarjoavat näin nopean ja automaattisen virustietokantapäivityksen. Ilmaiset virusohjelmistot päivittyvät kaupallisia hitaammin ja virustietokannat on päivitettävä usein manuaalisesti. Ilmaisohjelmat, esimerkiksi Antivir Xp tarjoavat kotikäyttäjälle riittävän virussuojan, mutta vaativat käyttäjältä aktiivisuutta. Kaupalliset tietoturvaohjelmistot kuten F-secure internet security tai Norton internet security tarjoavat automaattisen viruspäivityksen lisäksi myös muut tarvittavat tietoturvapalvelut, kuten palomuurin ja vakoiluohjelmien poistotyökalun yhdessä ohjelmistossa. Pelkkä virustorjuntaohjelma ei estä koneelle tulevia murtoyrityksiä, joten tietomurtojen sekä verkkohyökkäysten estämiseen tarvitaan palomuuri, joka on yleensä tietokoneelle asennettava, verkkoliikennettä valvova ohjelma.

2.4.2 Palomuuri

Internetiin kytketty tietokone on aina alttiina murtautumisyrityksille, joita vastaan on suojauduttava palomuurilla. Isoissa organisaatioissa palomuuri toteutetaan usein niin, että lähiverkon ja Internetin välinen liikenne kulkee erillisen palomuuritietokoneen kautta. Kotikäyttäjälle tehokas ja taloudellinen vaihtoehto on omaan tietokoneeseen asennettava palomuuriohjelmisto. Palomuurin avulla voidaan kontrolloida sekä tietokoneelle tulevaa että sieltä lähtevää liikennettä, joten se estää esimerkiksi tietokoneeseen tunkeutuneita vakoiluohjelmia toimimasta. [25] Palomuuri voidaan määritellä joko niin, että tietyt yhteydet sallitaan ja loput kielletään tai siten, että tietyt yhteydet kielletään ja loput sallitaan. Ensimmäinen vaihtoehto on turvallisempi, mutta se saattaa rajoittaa käyttäjien mahdollisuuksia hyödyntää internet-palveluja.

Kiinteään kuukasimaksuun perustuvien laajakaistayhteyksien lisääntyminen on mahdollistanut sen, että tietokone voi olla jatkuvasti kytkeytyneenä internetiin. Valitettavasti yhteys on samalla avoin myös toiseen suuntaan, joten kodin tietokoneet ovat alttiita verkosta tulevalle ilkivallalle ja näin palomuurista on tullut myös kotitietokoneiden välttämätön ratkaisu.

2.4.3 Sähköpostin turvallisuus

Jos sähköpostia ei ole salattu, on se kaikkien niiden luettavissa, joilla on osaaminen ja välineet verkon kuunteluun.

Viestit on salattava ennen niiden lähettämistä, jotta voidaan varmistua sähköpostiviestinnän luottamuksellisuudesta. Tämän lisäksi sähköpostiviestit on mahdollista allekirjoittaa digitaalisesti, jolloin varmistutaan viestin lähettäjän henkilöllisyydestä sekä siitä, että viesti on välittynyt lähettäjältä vastaanottajalle muuttumattomana. Sähköpostin salaamiseen ja allekirjoittamiseen on tarjolla useita kaupallisia ohjelmistoja.

Sähköpostihuijauksissa käyttäjiä usein houkutellaan avaamaan liitetiedosto, joka tartuttaa tietokoneeseen viruksen. Mikäli käyttäjä ei ole varma liitetiedoston sisällöstä on se syytä jättää avaamatta. Epävarmoissa tapauksissa liitetiedoston voi tallentaa tietokoneen kovalevylle ja tarkastaa sen ajan tasalla olevalla virustorjuntaohjelmalla. Suurimpia tietoturvariskejä ovat suoritettavat tiedostot, joiden pääte on.exe, mutta kaikkiin sähköpostin liitetiedostoihin on suhtauduttava epäluuloisesti.

Vähemmän vaarallista, mutta harmillista on lisääntyvä roskaposti (spam), joka on sähköpostitse tapahtuva massapostitusta, johon ei ole etukäteen saatu vastaanottajan lupaa. Arvioidaan, että noin 70-80% kaikesta sähköpostiliikenteestä on roskapostia.

Roskapostittajat keräävät sähköpostiosoitteita www-sivuilta, uutisryhmistä ja kotisivuilta. Rekisteröitymällä peli- ja viihdesivuilla käyttäjä saattaa tietämättään antaa sähköpostiosoitteensa roskapostittajille. Sähköpostiosoitteita saattaa joutua roskapostittajien käsiin myös tietomurtojen seurauksena. Roskapostilta on vaikea välttyä, mutta yksi tapa on käyttää keskusteluryhmissä ja rekisteröitymisissä niin sanottua ”roskapostilaatikkoa” eli ylimääräistä osoitetta jonne roskaposti saa mennä. Varsinainen sähköpostiosoite on syytä pitää vain sen tarvitsijoiden tiedossa.

2.4.4 Salasanat

Hyvä salasana on luonnollisesti salassa pysyvä ja sen tietää vain tunnuksen haltija. Salasana on sitä vahvempi mitä pidempi se on ja miten monesta merkkiluokasta se koostuu sekä kuinka usein se vaihdetaan. Jotkut pitävät salasanaa vain välttämättömänä pahana, eikä heille tärkeintä ole salasana, vaan se, että salasanan muistaisi hyvin. Vaikka salasanojen muistaminen on usein hankalaa ei niissä kuitenkaan tule käyttää perusmuodossa olevia sanoja. Ne eivät saa liittyä käyttäjään helposti liitettäviin tietoihin kuten omaan, puolison tai lasten nimiin yms. Eri järjestelmissä tulee käyttää eri salasanoja, jotka voivat koostua eri merkkiluokista.

- Isot kirjaimet (A, B, C,...Ö)
- Pienet kirjaimet (a, b, c,...ö)
- Arabialaiset numerot (0, 1, 2,...9)
- Erikoismerkit ({ } [ ]@ £ $,.<>;:!“# %&¤~^¨()+=) ja alt +

Erikoismerkkien ja skandinaavisten kirjaimien käyttö tekee salasanat vaikeasti arvattaviksi ja on siksi erityisen suositeltavaa. Myös isojen ja pienien kirjaimien sekoittaminen kannattaa. [32]

3 TUTKIMUSMENETELMÄT

3.1 Yleistä tutkimuksesta

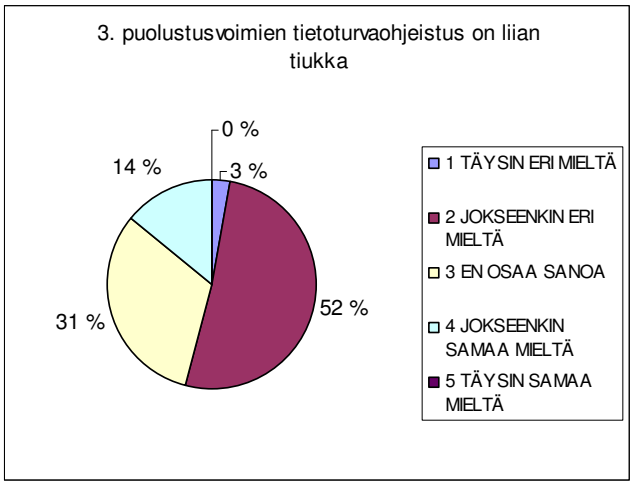
Tutkimus on tehty käyttämällä sekä kirjallisuustutkimusta, että haastattelututkimusta. Menetelmät ovat kvantitatiivisia. Haastatteluissa on käytetty Likterin asteikkoa, jossa vastausvaihtoehdot on arvioitu numeroasteikolla 1-5 ja vastausvaihtoehdot ovat:

- täysin samaa mieltä (5)
- jokseenkin samaa mieltä (4)
- en osaa sanoa (3)
- jokseenkin eri mieltä (2)
- täysin eri mieltä (1)

Numeerisesti vastattavia kysymyksiä sarjassa on 26 kappaletta ja ne ovat laadittu tutkijan tietotekniikan osaamisen pohjalta tutkimusongelmaa lähestyviksi. Kysymykset on arvioinut kaksi tietotekniikan ammattilaista ennen kyselyn suorittamista. Näiden arvioiden ja ohjaajan suositusten perusteella kysymysten määrää on karsittu alkuperäisestä 48 kappaleesta 26:teen.

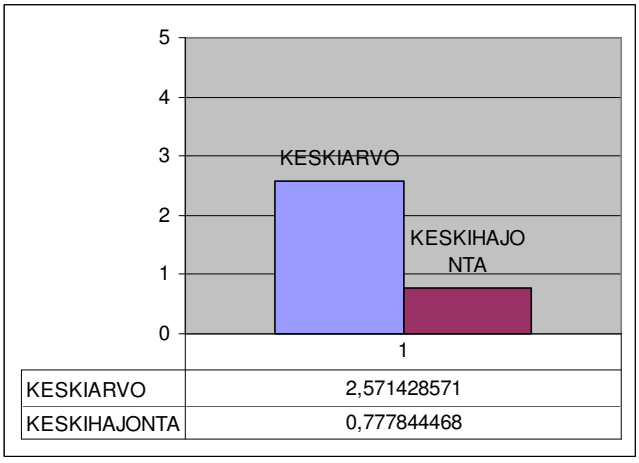
Kysymyksiä laadittaessa on pyritty käytännönläheiseen ajattelumalliin ja haluttu saada kartoitettua mahdollisia tietoturvariskejä seuraavien alaotsikoiden kautta:

- kysymyksiä työpaikan tietoturvaohjeistosta (4kpl)
- kysymyksiä käyttöoikeuksista ja salasanojen käytöstä (5kpl)
- kysymyksiä riskialttiista toimintatavoista (9kpl)
- virustorjuntaan ja riskinhallintaan liittyviä kysymyksiä (6kpl)
- koulutukseen liittyviä kysymyksiä (2kpl)



Esimerkki kyselyn tuloksista

Kysymykseen *Onko puolustusvoimien tietoturvaohjeistus liian tiukka?* 35 vastaajasta yksi on *täysin eri mieltä,* 18 on vastannut j*okseenkin eri mieltä.* 11 vastaajaa *ei osaa sanoa* tai heillä ei ole mielipidettä asiasta. Viisi vastaa *Jokseenkin samaa mieltä.* Yksikään vastaajista ei ole täysin samaa mieltä. Vastausten **keskiarvo** on n. 2.6 joten keskimääräinen vastaus asettuu *jokseenkin eri mieltä* ja *en osaa sanoa* väitteiden väliin.



KESKIARVO	2,571428571
KESKIHAJONTA	0,777844468

Esimerkki 2

Keskihajonta on tärkein ja käytetyin hajonnan mitta. Keskihajonta kuvaa havaintoarvojen keskimääräistä etäisyyttä keskiarvosta. Mitä pienempi on keskihajonta, sitä tiiviimmin havaintoaineisto on keskittynyt keskiarvon ympärille. Laskettu keskihajonta esimerkkivastauksessa on 0,777844468. Keskihajonnaksi saatu tulos tarkoittaa, että yksittäiset havaintoarvot sijaitsevat keskimääräisesti 0,777844468 yksikön päässä

havaintoarvojen keskiarvosta. Ympyrägrafiikka, josta käy ilmi vastausten prosentuaalinen osuus kokonaismäärästä, havainnollistaa vastausten jakautumaa. [40]

Korrelaatio on kahden muuttujan välisen tilastollisen riippuvuuden mitta. Tavallisesti sanalla viitataan Pearsonin tulomomenttikertoimeen, joka on lineaarisen (suoraviivaisen) riippuvuuden mitta. Korrelaatio kahden muuttujan tilastolliselle yhteydelle voidaan laskea korrelaatiokerroin, joka kuvaa lineaarisen (suoraviivaisen) yhteyden voimakkuutta. Lineaarinen yhteys on täydellistä, kun korrelaatiokerroin saa arvokseen 1 tai -1. Kun korrelaatiokerroin on positiivinen, on yhteys kahden muuttujan välillä suora. Korrelaatiokertoimen ollessa negatiivinen, on yhteys käänteinen. Kun lineaarista yhteyttä ei ole, korrelaatiokerroin on nolla. Korrelaatiokerroin saattaa olla lähes nolla ja silti muuttujilla on tilastollista yhteyttä. [37]

Kuva. Korrelaatio

Pearsonin tulomomenttikorrelaatiokerroin lasketaan seuraavasta kaavasta, jossa X_1 ja Y_1 ovat muuttujien havaittuja arvoja, X ja Y ovat muuttujien keskiarvot. N on havaintojen määrä ja S_x ja S_y muuttujien keskihajonnat.

$$r = \frac{\sum (X_1 - \overline{X})(Y_1 - \overline{Y})}{(N-1)S_x S_y}$$

Tutkija on ottanut itselleen vapauden etsiä korrelaatioita niistä vastauksista, joissa hän katsoo korrelaation tai sen puuttumisen olevan merkityksellistä.

Likterin asteikolla pisteytettyjen kysymysten lisäksi haastateltavilta kysytään suoria kysymyksiä, kuten ikä, työtehtävä, mikä käyttöjärjestelmä ja virustorjunta haastateltavan tietokoneessa on. Haastattelussa pyritään siihen, että kysymykset olisivat asiasisällöltään kaikille vastaajille tuttuja ja yksiselitteisiä. Tosiasia kuitenkin on, että mielipiteitä, asenteita, uskomuksia ja aikeita koskevat kysymykset ovat erityisen alttiita

validiusongelmille (luotettavuusongelmille). Näitä ongelmia pyritään minimoimaan suurella otannalla sekä tulosten kriittisellä tarkastelulla.

Kysymyslomakkeet jätettiin vastaajille 5.9.2005 ja vastausten määräajaksi asetettiin 15.9.2005. Kysymyslomakkeita jätettiin 43 kpl, joista vastauksia saatiin määräaikaan mennessä 35 kpl vastusprosentin ollessa 81%.

Menetelmiä valitessaan tutkija tutustui professori Jorma Jormakan artikkeliin kirjassa ”Tekniset tutkimusmenetelmät Maanpuolustuskorkeakoulussa”. *Tekniikan tutkimuksessa on usein havaittavissa tietty välinpitämättömyys tieteellisiä kriteerejä kohtaan sellaisina, kuin ne on tieteen puolella opittu tuntemaan.* Esimerkiksi tietoliikennetekniikan suorituskykytutkimuksesta Jormakka sanoo: *Liian hienot menetelmät tällaisen nopeasti muuttuvan asian selvittämiseksi eivät ole perusteltuja.* Tässä tutkielmassa tulkintoja sekä päätelmiä pyritään tekemään teorian ja tutkimusaineiston pohjalta. Tutkija etsii numeroiden takaa reaalimaailman ilmiöitä, jotka aukikirjoitetaan johtopäätöksissä.

4 TUTKIMUSTULOKSET

Taustatietoja

Tehtävä

Vastaajista 25 ilmoitti taustatiedoissa ammattinsa tai tehtävänsä. Seitsemän vastaajista (28%) oli kadettia, yksi siviiliopettaja (4%), 14 sotilasopettajaa (56%) ja kolme vastasi kohtaan muu (12%).

Ikä

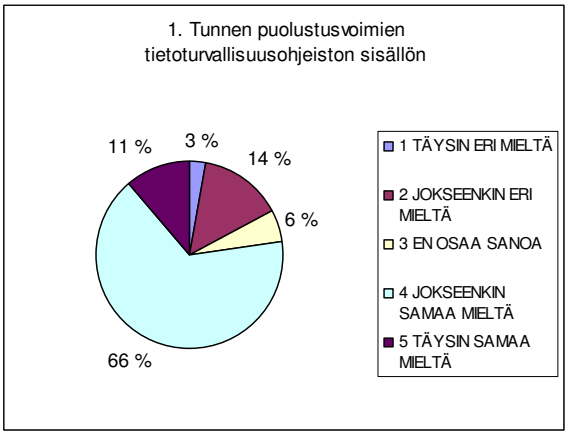
Vastaajista 34 ilmoitti ikäluokkansa. Seitsemän vastaajaa oli 20…27 vuotiasta (21%). Viisi vastaajista kuului ikäluokkaan 28…35 vuotta (15%). Ikäluokkaan 35…42 vuotta kuului 11 vastaajaa (32%). Myös ikäluokkaan 43 ikävuodesta ylöspäin kuului 11 vastaajaa (32%).

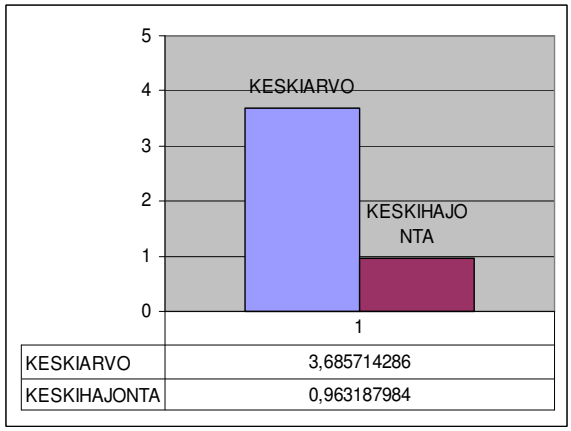
Kotitietokone

Kolmella vastaajalla (8%) ei ollut kotitietokonetta. 30 vastaajista (86%) ilmoitti kotitietokoneensa käyttöjärjestelmäksi Windows XP:n. Yhdellä oli käytössään Windows 98 käyttöjärjestelmä (3%) ja yksi käyttäjistä käytti Windows XP:n lisäksi myös Linux käyttöjärjestelmää (3%). Internetyhteys oli 27 vastaajan kotona (77%). Tietoturvaohjelmistoja oli siten, että 24 vastaajista (68%) käytti kaupallista tietoturvaa ja kahdeksan ilmaisia tietoturva ohjelmistoja (22%). Viisi vastaajaa (14%) ilmoitti käyttävänsä sekä kaupallisia että ilmaisia tietoturvaohjelmistoja.

Kysymyksiä työpaikan tietoturvaohjeistosta

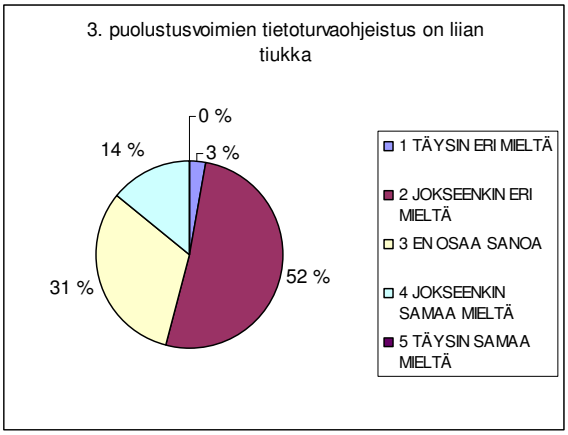
Tunnen puolustusvoimien tietoturvallisuusohjeiston sisällön

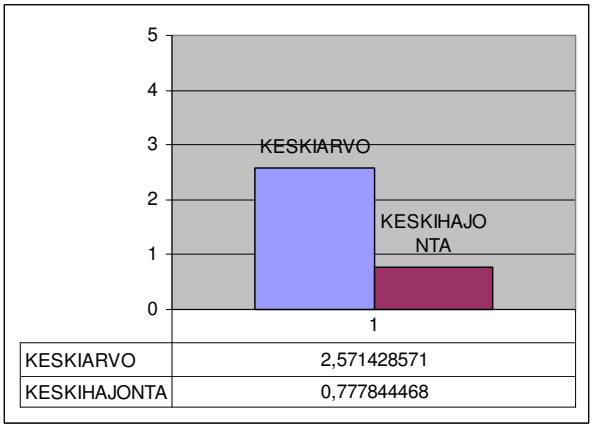




Yksi vastaajista (3%) oli täysin eri mieltä eli ei tunne puolustusvoimien tietoturvallisuusohjeistoa. Jokseenkin eri mieltä oli viisi vastaajaa (14%) ja kaksi vastaa (6%) ei osannut vastata. Suurin osa eli 23 vastaajaa (66%) oli jokseenkin samaa mieltä ja neljä vastaajaa oli täysin samaa mieltä (11%).

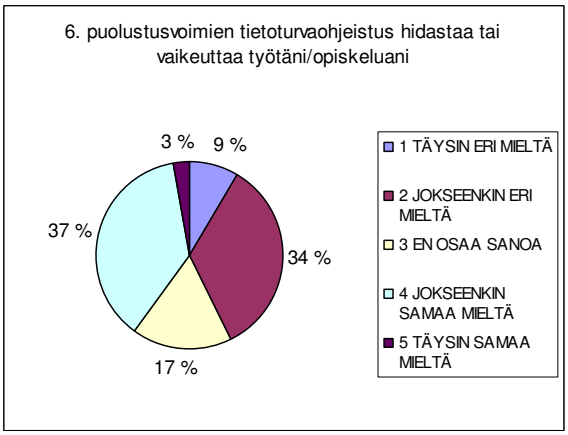
Puolustusvoimien tietoturvaohjeistus on liian tiukka

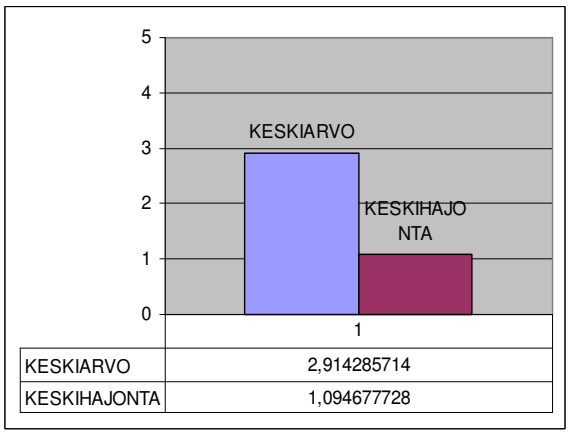




Kukaan vastaajista ei ollut täysin samaa mieltä, mutta viisi vastaajaa (14%) oli jokseenkin samaa mieltä. 11 vastaajalla ei ollut mielipidettä (31%). Jokseenkin eri mieltä oli 18 vastaajaa (52%) ja yksi vastaajista (3%) oli täysin eri mieltä.

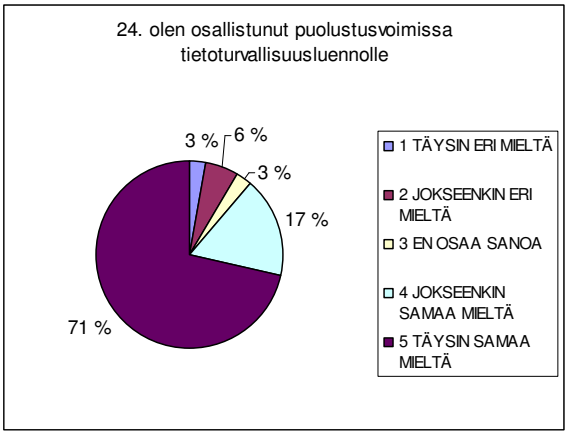
Puolustusvoimien tietoturvaohjeistus hidastaa tai vaikeuttaa työtäni/opiskeluani

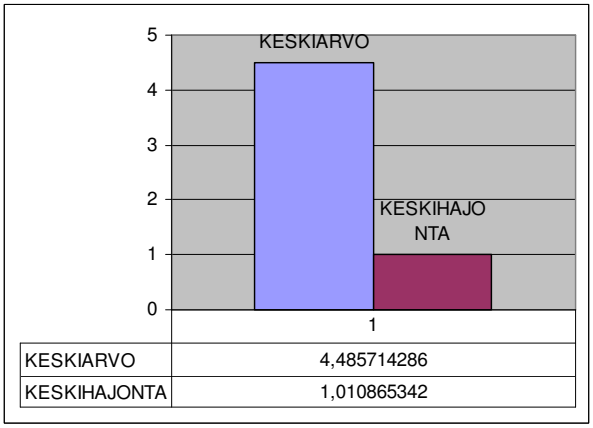




Täysin eri mieltä oli kolme vastaajaa (9%) ja jokseenkin eri mieltä 12 vastaajaa (34%). Kuudella ei ollut asiasta mielipidettä (17%). Jokseenkin samaa mieltä oli 13 vastaajaa (37%) ja täysin samaa mieltä yksi vastaaja (3%).

Olen osallistunut puolustusvoimissa tietoturvallisuusluennolle





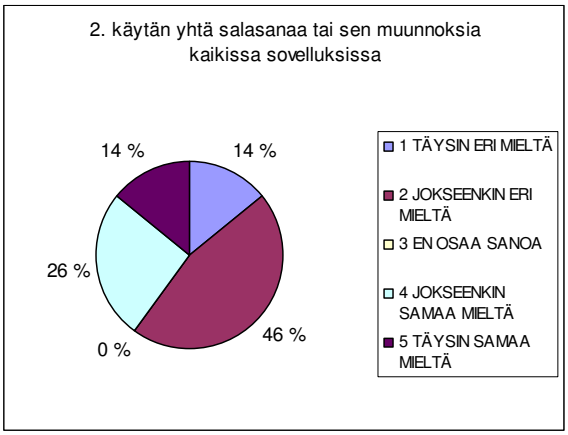
25 vastaajaa (71%) on täysi samaa mieltä ja kuusi jokseenkin samaa mieltä (17%). Yhdellä ei ole mielipidettä (3%) ja kolme jokseenkin eri mieltä (6%). Yksi vastaaja oli täysin eri mieltä (3%).

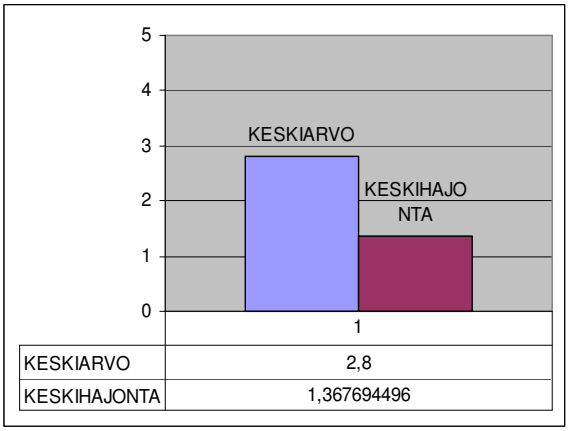
Johtopäätökset

Puolustusvoimien tietoturvallisuutta ohjeistaa Pääesikunnan turvallisuusosasto, joka julkaisee pysyväisasiakirjoja. Ne määrittelevät teknisen tietoturvallisuusarkkitehtuurin puolustusvoimissa. Pysyväisasiakirjat toimivat velvoittavana ohjeistona käyttäjille. Pääesikunnan turvallisuusosasto on myös julkaissut käyttäjän tietoturvaohjeen, joka on tarkoitettu puolustusvoimien henkilöstölle. Ohjeessa annetaan käytännön neuvoja tietoturvallisuuden toteuttamiseen työssä ja se velvoittaa kaikkia puolustusvoimien palveluksessa työskenteleviä. [32] Ainoastaan 11% vastaajista sanoo varauksetta tuntevansa ohjeiden sisällön. 66% vastaajista sanoo jokseenkin tuntevansa ohjeistuksen. Koska vastaajista lähes 90% on osallistunut puolustusvoimien tietoturvaluennoille, voidaan tehdä johtopäätös, että tietoturvaluennot eivät tavoita täysin kuulijakuntaansa. Johtopäätöstä tulee vahvistaa tarkentavilla kysymyksillä kuten: ”Onko tietoturvaluennot sisällöltään ymmärrettäviä ja onko niissä esitetyt toimintamallit omaksuttavissa?” Merkittävä huomio on se, että 40% vastaajista on jokseenkin tai täysin sitä mieltä, että tietoturvaohjeistus hidastaa tai vaikeuttaa heidän työtään/opiskeluaan. Kyselyn kohtien ”Puolustusvoimien tietoturvaohjeistus on liian tiukka” ja ”Puolustusvoimien tietoturvaohjeistus hidastaa tai vaikeuttaa työtäni/opiskeluani”, välillä löytyy myös melko vahva positiivinen korrelaatio (0,612).

Kysymyksiä käyttöoikeuksista ja salasanojen käytöstä

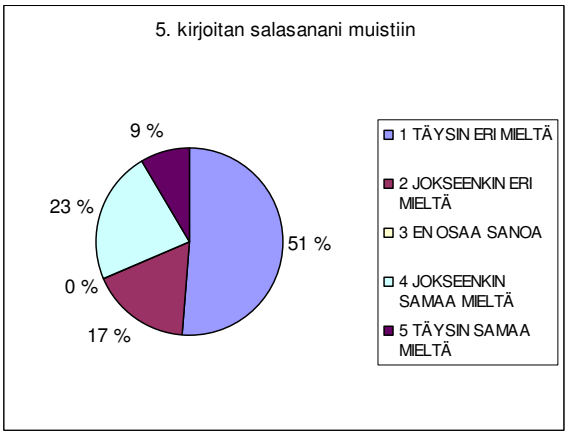
Käytän yhtä salasanaa tai sen muunnoksia kaikissa sovelluksissa

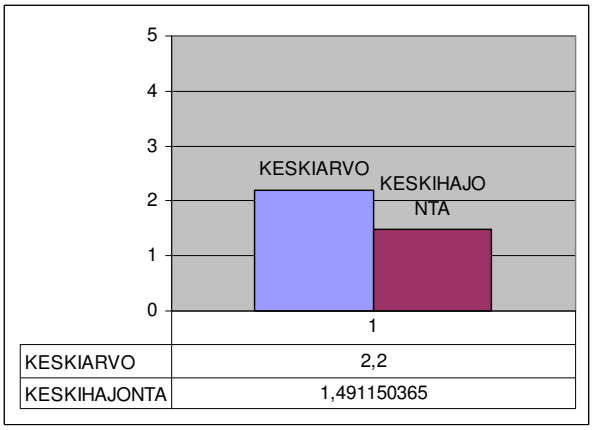




Viisi vastaajaa (14%) oli väitteen kanssa täysin eri mieltä ja peräti 16 vastaajaa (46%) jokseenkin eri mieltä. Jokseenkin samaa mieltä yhdeksän (26%) ja täysin samaa mieltä viisi vastaajaa (14%).

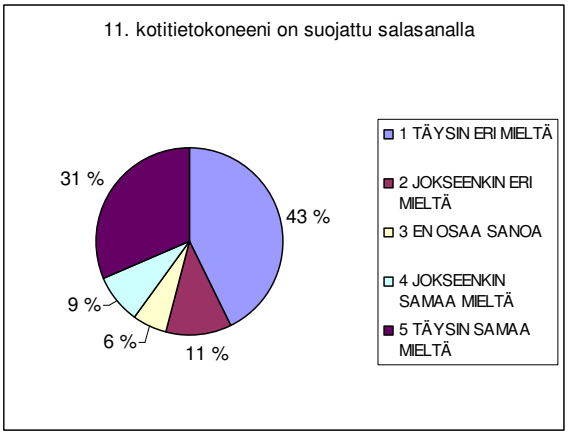
Kirjoitan salasanani muistiin

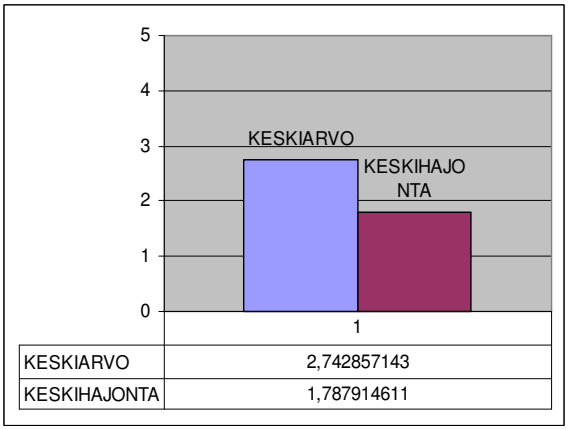




16 ei kirjoita salasanaansa muistiin (51%). Kuusi vastaajaa ei pääsääntöisesti kirjoita salasanaansa muistiin (17%). Kahdeksan vastaajaa joskus kirjoittaa salasanansa muistiin (23%). Kolme vastaajista kirjoittaa salasanansa muistiin (9%).

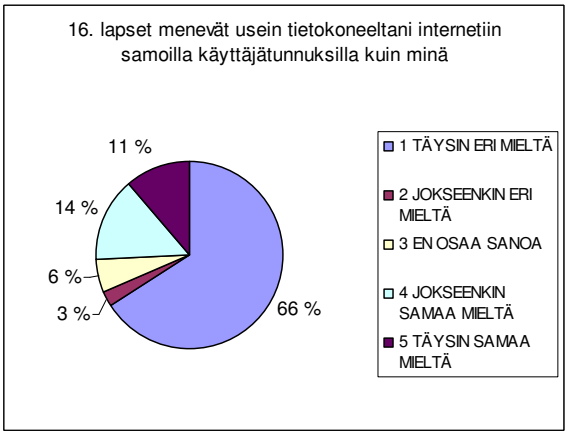
Kotitietokoneeni on suojattu salasanalla

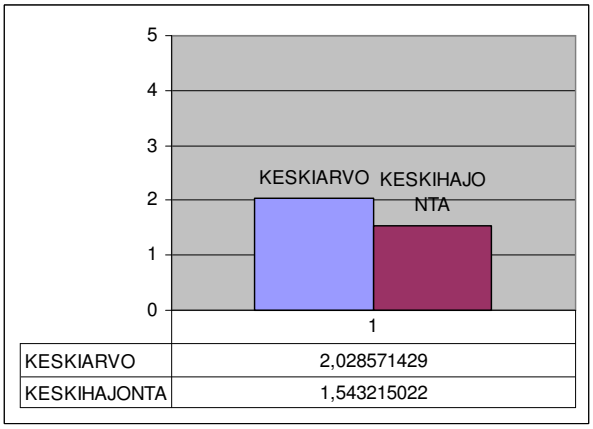




Vastaajista 15 ei ole suojannut kotitietokonettaan salasanalla (43%). 11 vastaaja on (31%). Ei osaa sanoa vastauksen antoi kaksi (6%) ja jokseenkin erimieltä väitteen kanssa oli neljä (11%). Vastaajista kolme oli jokseenkin samaa mieltä (9%). Kysymyksen asettelu jätti tulkinnan varaa, joten vastauksia pitää tulkita erityisellä kriittisyydellä.

Lapset menevät usein tietokoneeltani internetiin samoilla käyttäjätunnuksilla kuin minä

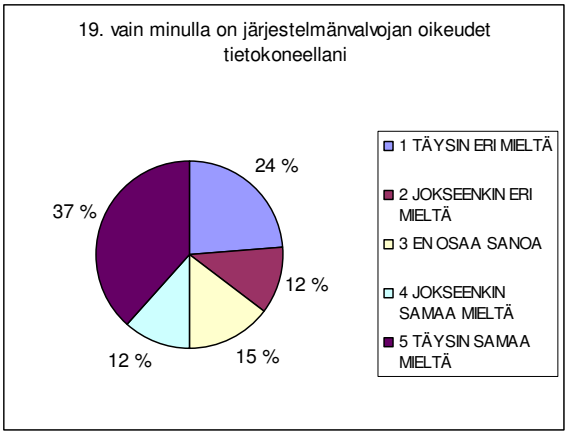


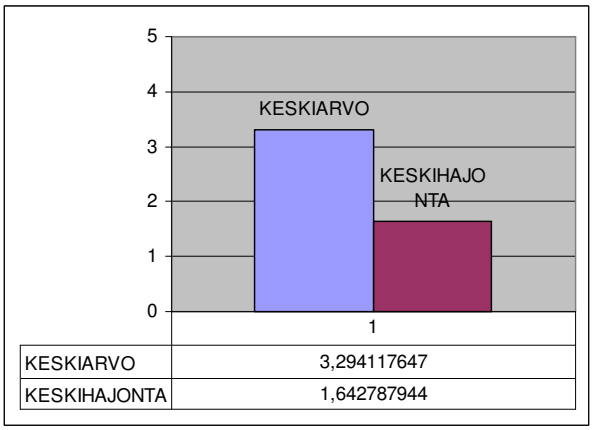


Vastausta ei voida tulkita aukottomasti viitaten edellisen kysymysten vastauksiin, joissa kävi ilmi, että lähes puolella vastaajista tietokone ei ole suojattu salasanalla. Käyttäjätunnus ja salasana eivät ole suorassa yhteydessä toisiinsa, mutta tulkintaa on mahdotonta tehdä ilman tarkentavia kysymyksiä. Vastauksia saatiin seuraavasti: Täysin eri mieltä 23 vastaajaa (66%), jokseenkin eri mieltä yksi (3%). Kaksi ei osannut sanoa (6%) ja viisi vastaajista oli jokseenkin samaa mieltä (14%). Neljä vastaajis-

ta oli varauksetta sitä mieltä, että lapset menevät internetiin samoilla käyttäjätunnuksilla kuin hän (11%).

Vain minulla on järjestelmänvalvojan oikeudet tietokoneellani





KESKIARVO	3,294117647
KESKIHAJONTA	1,642787944

Täysin eri mieltä on kahdeksan vastaajaa (24%) ja jokseenkin eri mieltä neljä vastaajaa (12%). Viisi vastaajaa ei osaa sanoa (15%). Jokseenkin samaa mieltä vastaa neljä henkilöä (12%) ja 13 valitsee vastausvaihtoehdon: täysin samaa mieltä (37%)

Johtopäätökset

Jopa 40% vastaajista käyttää pääsääntöisesti yhtä salasanaa tai sen muunnoksia kaikissa sovelluksissa. Käyttäjän tulee soveltaa eri salasanoja eri järjestelmille koska yhden salasanan paljastuminen ei saa vaarantaa kaikkia järjestelmiä.

Noin kaksi kolmasosaa vastaajista ei kirjoita salasanojaan muistiin. Muistiin kirjoittaminen ei sinällään ole huono käytäntö, sillä sen avulla käyttäjä pystyy hallitsemaan useampia ja monimutkaisempia salasanoja. Kirjoitettuja salasanoja ei tule säilyttää järjestelmää käyttävän tietokoneen läheisyydessä eikä yhdessä käyttäjätunnuksen kanssa. Salasanoja ei pidä kirjoittaa muistiin tekstiasiakirjaan eikä tallentaa salaamattomana kovalevylle.

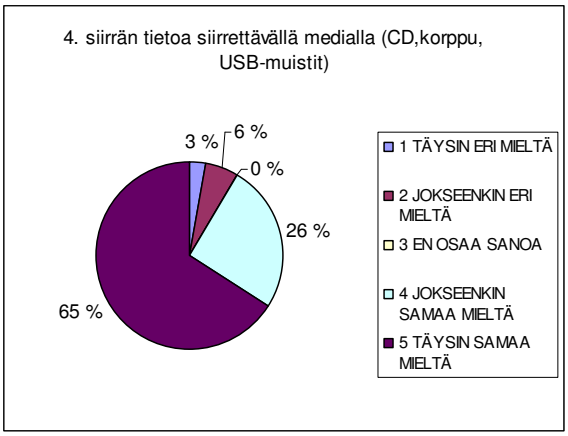
Lähes puolet vastaajista sanoo, ettei heidän kotitietokoneensa ole suojattu salasanalla ja neljäsosa sanoi lasten käyttävän tietokonetta samoilla käyttäjätunnuksilla kuin he. Lähes kaikilla vastaajilla oli käytössään Windows XP- käyttöjärjestelmä, joka mahdollistaa käyttäjätilien luomisen ja salasanojen käytön. Windows XP:n perustietoturvaa internetkäytössä parantaa se, että selainta käytetään jollakin alemmalla käyt-

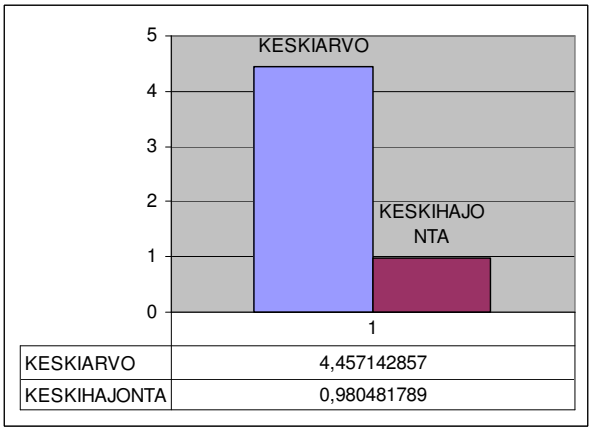
täjätasolla kuin järjestelmänvalvoja-tasolla. Tämä käytäntö estää monien haittaohjelmien asentumisen järjestelmän ytimeen.

Puolet vastaajista sanoo, että vain heillä on järjestelmänvalvojan oikeudet kotitietokoneelle. Sekä kotitietokoneella että työpaikan koneella on oleellista, että järjestelmää hallinnoi vain yksi tai korkeintaan muutama henkilö. Lapsia ei ole hyvä päästää muuttamaan tietokoneen asetuksia, koska he voivat epähuomiossa avata ulkopuolisille mahdollisuuksia tunkeutua tietokoneeseen. Esimerkiksi palomuurin tai virusturvan poiskytkeytyminen tietokoneen ollessa laajakaistayhteydessä on vaarallista. Myös monet lasten internetistä lataamat pelit ja muut ohjelmat saattavat sisältää tietoturvariskejä, jotka oikein asetettu palomuuri pystyy torjumaan. On tärkeää, että lapset eivät pääse säätämään palomuurin asetuksia ja avaamaan takaportteja tunkeutujille. On siis tärkeää, että myös kotikäytössä käyttöjärjestelmän järjestelmänvalvojan salasana ei ole lasten tiedossa eikä järjestelmänvalvojan käyttäjätiliä käytetä jokapäiväiseen internetkäyttöön. Vastauksista ei löytynyt merkittäviä korrelaatioita, mutta niiden perusteella voidaan tehdä johtopäätös, että Windows XP- käyttöjärjestelmästä on tarpeellista järjestää koulutusta ilmavoimien teknillisessä koulussa

Kysymyksiä riskialttiista toimintatavoista

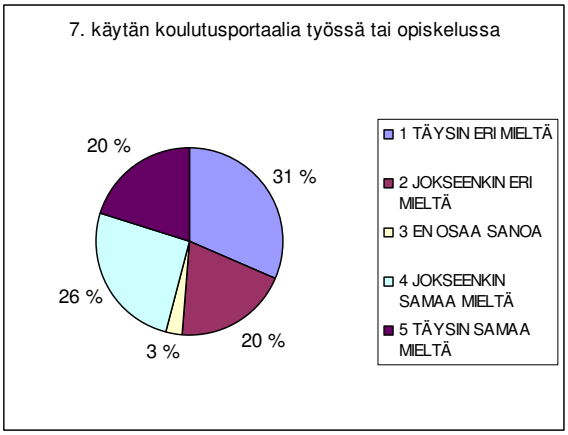
Siirrän tietoa siirrettävällä medialla (CD, korppu, USB-muistit)

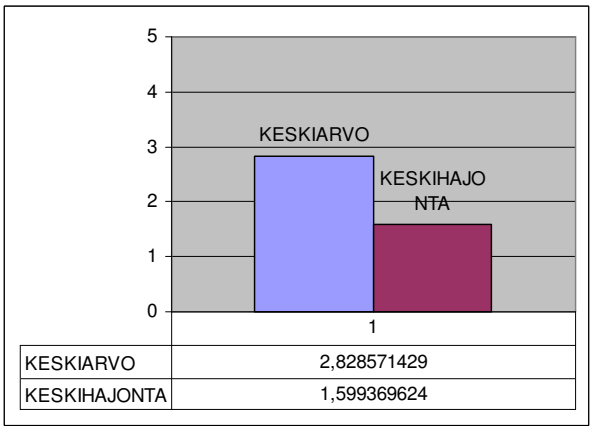




Kysymys on hieman suurpiirteinen, mutta sitä tulkitsemalla voidaan ehkä jakaa vastaajia aktiivisiin ja passiivisiin käyttäjiin. Enemmistö eli 23 siirtää tietoa siirrettävällä medialla (65%). Yhdeksän on jokseenkin samaa mieltä kysymyksen väitteen kanssa (26%). Kaksi jokseenkin ja yksi täysin eri mieltä (6% ja 3%).

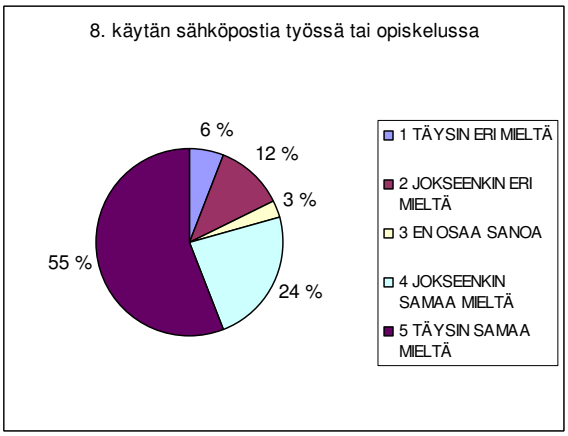
Käytän koulutusportaalia työssä tai opiskelussa

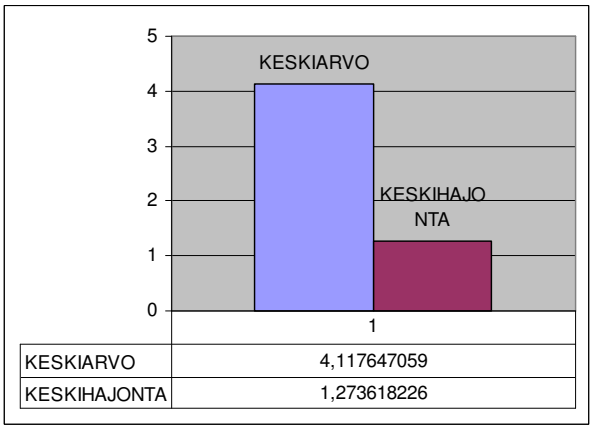




11 vastaajaa ei käytä koulutusportaalia opiskelussa tai työssään (31%), Seitsemän on ilmeisesti tutustunut portaaliin, mutta eivät aktiivisesti käytä sitä (20%). Yhdeksän vastaajaa käyttänee portaalia jonkin verran (26%) ja seitsemän aktiivisesti (20%). Yksi ei osaa vastata tai ei tunne asiaa (3%).

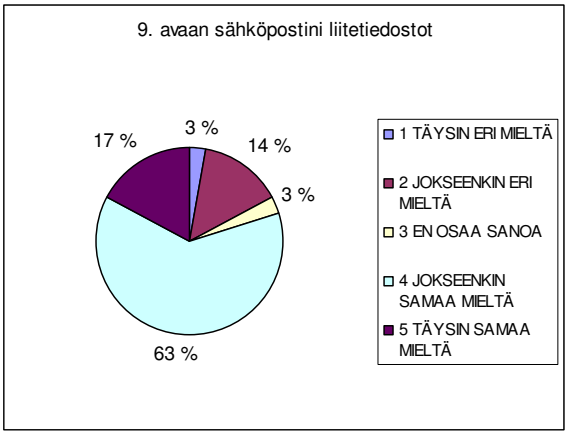
Käytän sähköpostia työssä tai opiskelussa

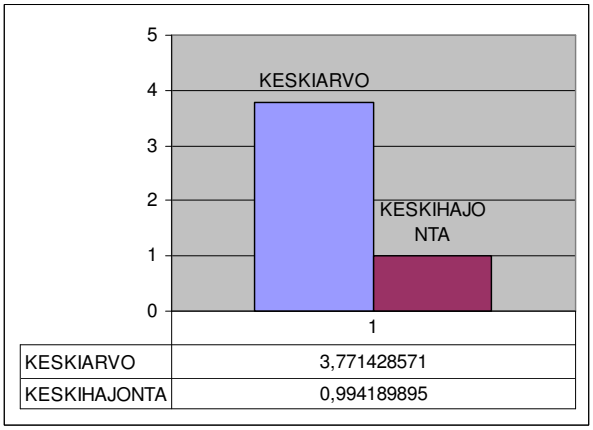




Kaksi vastaajista on täysin eri mieltä (6%) ja neljä jokseenkin eri mieltä. Yksi ei osaa vastata. Kahdeksan vastaajista on jokseenkin samaa mieltä (24%) ja yli puolet (55%) eli 19 vastaajaa on täysin samaa mieltä.

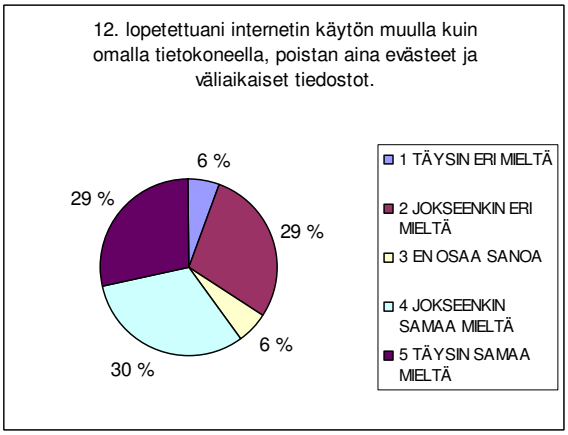
Avaan sähköpostini liitetiedostot

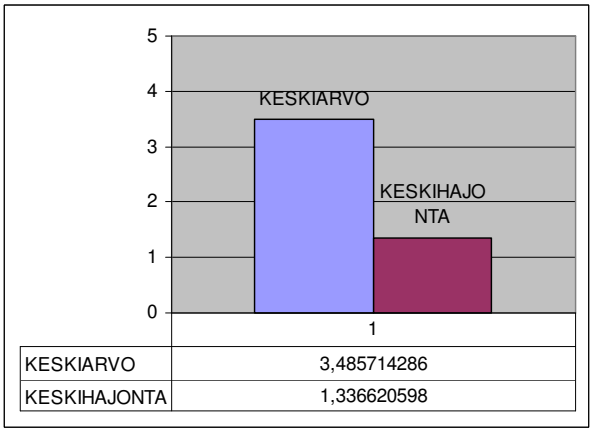




Jopa 22 vastaajaa oli jokseenkin samaa mieltä (63%) ja kuusi täysin samaa mieltä (17%). Yhdellä ei ollut mielipidettä. Viisi jokseenkin eri mieltä (14%) ja yksi täysin eri mieltä (3%).

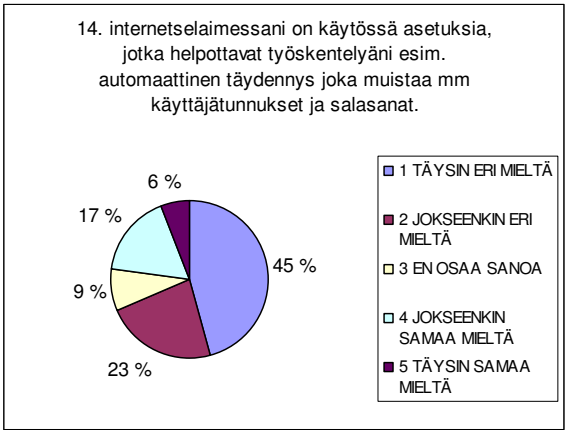
Lopetettuani internetin käytön muulla kuin omalla tietokoneella, poistan aina evästeet ja väliaikaiset tiedostot

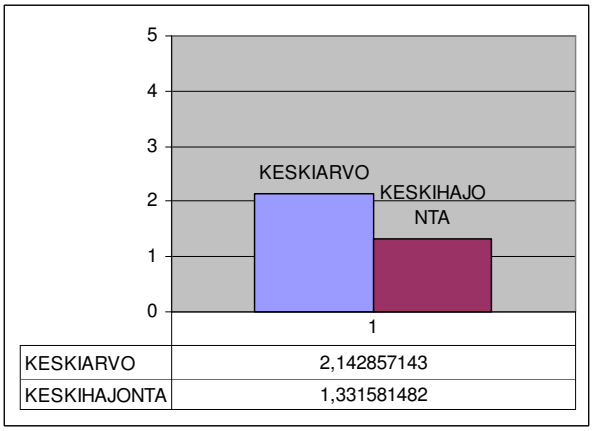




Kaksi vastaajaa on täysin erimieltä (6%) ja peräti 10 jokseenkin eri mieltä (29%). Kaksi ei osaa sanoa (6%). Jokseenkin samaa mieltä on 11 vastaajaa (30%) ja täysin samaa mieltä 10 vastaajaa (29%)

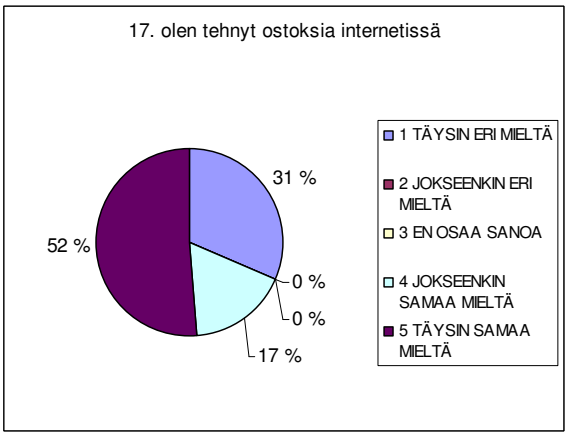
Internetselaimessani on käytössä asetuksia, jotka helpottavat työskentelyäni esim. automaattinen täydennys, joka muistaa mm käyttäjätunnukset ja salasana

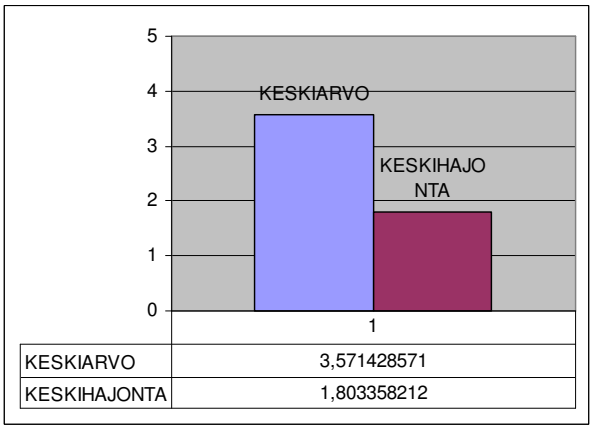




Täysin eri mieltä on peräti 45% vastaajista eli 16 henkeä. Jokseenkin eri mieltä sanoo olevansa kahdeksan vastaajaa (23%). Kolme ei osaa sanoa (9%). Jokseenkin samaa mieltä on kuusi (17%) ja täysin samaa mieltä kaksi vastaajaa (6%)

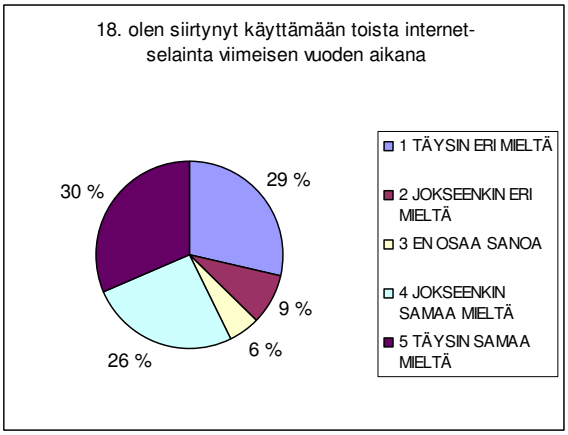
Olen tehnyt ostoksia internetissä

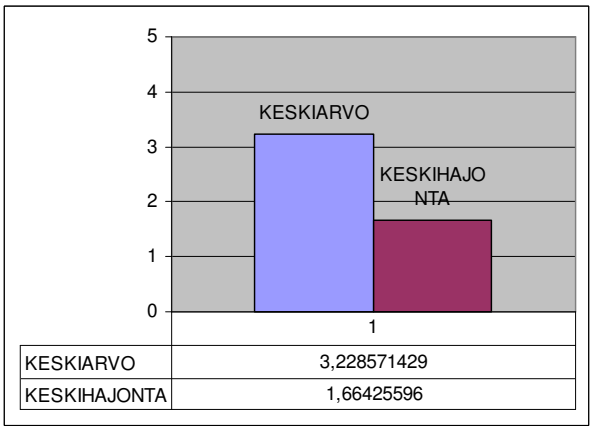




Kysymys jakaa vastaajat kolmeen osaan. 52% vastaajista (18) on varauksetta tehnyt ostoksia internetissä. 31% ei ole tehnyt (11). 17% Vastaajista on jokseenkin sitä mieltä, että he ovat tehneet ostoksia internetissä (6). On tarve tarkentaville kysymyksille, jotta voidaan selvittää mitä nämä kuusi vastaajaa tarkoittavat.

Olen siirtynyt käyttämään toista internet-selainta viimeisen vuoden aikana

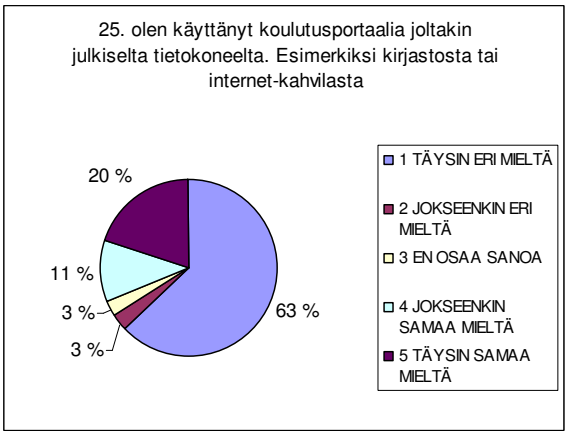


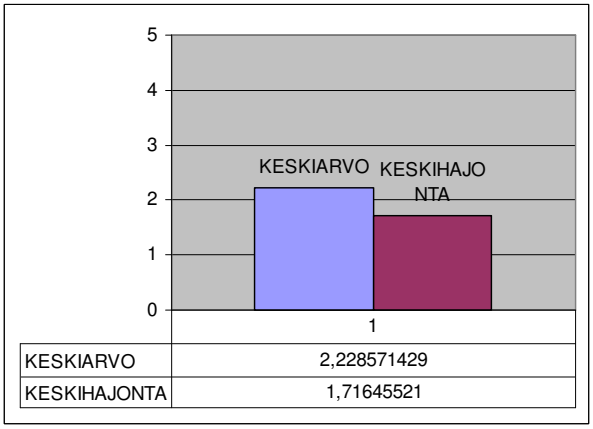


KESKIARVO	3,228571429
KESKIHAJONTA	1,66425596

11 vastaajaa on siirtynyt käyttämään toista internetselainta viimeisen vuoden aikana (30%). Yhdeksän (26%) on väitteen kanssa jokseenkin samaa mieltä eli voidaan olettaa, että he käyttävät selaimia rinnakkain tai käyttävät toista selainta esimerkiksi kotona ja toista työssä. Kaksi ei osaa sanoa (6%). Kolme on jokseenkin eri mieltä (9%) ja 10 vastaajista (29%) ei ole siirtynyt käyttämään toista selainta viimeisen vuoden aikana.

Olen käyttänyt koulutusportaalia joltakin julkiselta tietokoneelta. Esimerkiksi kirjastosta tai internet-kahvilasta





KESKIARVO	2,228571429
KESKIHAJONTA	1,71645521

Suurin osa eli 22 vastaajaa (63%) ei ole käyttänyt koulutusportaalia julkiselta tietokoneelta. Yksi vastaaja on jokseenkin eri mieltä ja yksi ei osaa sanoa (3%). Neljä on jokseenkin samaa mieltä (11%) ja seitsemän sanoo varauksetta käyttäneensä koulutusportaalia joltakin julkiselta tietokoneelta (20%).

90% vastaajista on aktiivisia tietokoneen käyttäjiä, jotka liikuttavat tietoa siirrettävillä medioilla. Erityisesti USB- massamuistien pieni koko, suuri kapasiteetti, helppo käyttö ja edullinen hintataso on lisännyt niiden käyttöä samalla lisäten tietoturvariskejä. On ehdottoman oleellista, että massamuistien käytön ohjeistus on yksinkertainen, selkeä ja ennen kaikkea noudatettavissa. Ohjeistus ei saa olla pelkkiä kieltoja, virustarkastus on tehtävä helpoksi ja siitä on tultava normaali toimintatapa, eikä hankala ja epämieluisa pakkotoimi.

46% vastaajista käyttää koulutusportaalia työssään tai opiskelussaan, joko aktiivisesti tai jonkin verran. 31% vastaajista ei käytä kolutusportaalia. Käyttäjien määrää voidaan pitää melko suurena kun otetaan huomioon, että varsinaisia opiskelijoita vastaajista on 19%. Sähköpostin käyttö työssä ja opiskelussa on vastaajien keskuudessa yleistä. Luottamus sähköpostin oikeellisuuteen on vahvaa, sillä 80% vastaajista avaa sähköpostin liitetiedostot aina tai jokseenkin aina. Tietoturvakoulutukseen on tarpeellista sisällyttää sähköpostin käyttöön liittyvää opetusta. Internet selaimen käyttö vaatii vastausten perusteella kolutusta. 35% vastanneista ei poista väliaikaisia selaintiedostoja lopetettuaan internetin käytön muulla kuin omalla tietokoneellaan. Evästeiden ja väliaikaisten tiedostojen poistaminen pienentää huomattavasti riskiä mm. salasanojen joutumisesta ei toivottuihin käsiin. Myös sähköpostin, pankkipalvelujen ja muiden kirjautumista vaativien palveluiden turvallisuus paranee käytön jälkeisen evästeiden poistamisen myötä.

Vastaajista 68% ei käytä selaimen automaattitäydennys-ominaisuutta, mutta 23% käyttää ainakin jonkin verran. Tutkijan jyrkkä mielipide on, että selaimen automaattitäydennys tulisi kytkeä pois käytöstä kokonaan, koska käyttäjätunnukset ja pahimmassa tapauksessa myös salasanat ovat muiden käyttäjien saatavissa. Tutkijalla on henkilökohtainen kokemus, jossa yhteiskäytössä olevassa tietokoneessa oli käytössä sekä automaattitäydennys että salasanojen tallentuminen. Käyttäjäoikeudet olivat rajattu niin, että väliaikaisia tiedostoja ei peruskäyttäjän profiilissa voinut poistaa. Kun tutkija kirjautui sähköpostiinsa ja epähuomiossa antoi järjestelmälle luvan muistaa salasana, hän ei tämän jälkeen pystynyt toimintaa peruuttamaan, sähköposti jäi kaikille käyttäjille luettavaksi kunnes järjestelmänvalvoja poisti selaimen väliaikaiset tiedostot.
Edellisistä vastauksista ei ollut löydettävissä merkittävää korrelaatiota.

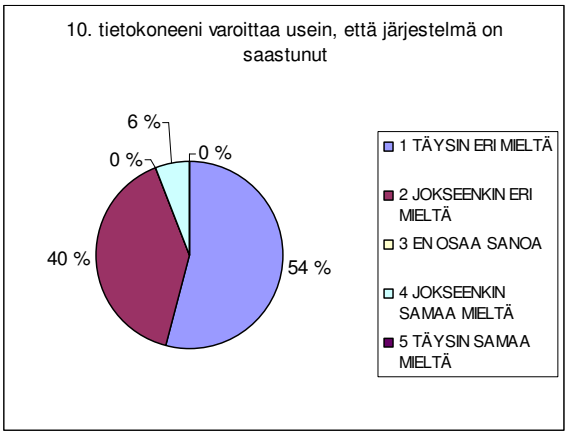
Merkittävä huomio on, että 56% vastaajista on viimeisen vuoden aikana ainakin osittain siirtynyt käyttämään toista internet-selainta. Taustalla saattaa olla puolustusvoimien tietoturva-ohjeistus vuodelta 2004, joka kehotti käyttäjiä siirtymään Explorer-selaimesta Firefox- selaimeen. Taustalla oli tuolloin havaitut Explorer- selaimen vakavat tietoturva-aukot, jotka on myöhemmin korjattu. Käyttäjille on tarpeellista tiedottaa, ettei mikään selain ole täysin turvallinen ja, että rikollisten intressit kasvavat yhdessä käyttäjämäärän kanssa.

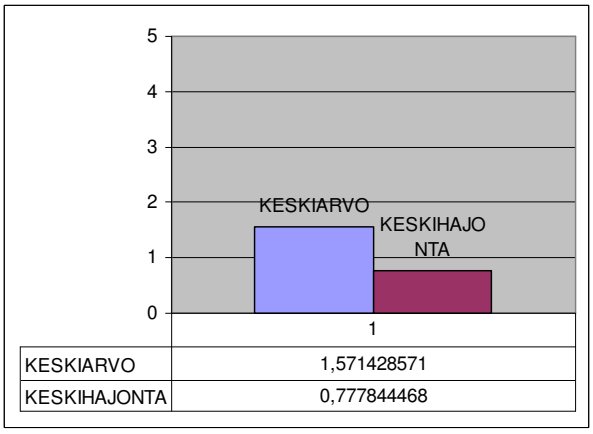
31% vastaajista on käyttänyt koulutusportaalia joltakin julkiselta tietokoneelta. Kun suhteutetaan luku niihin vastaajiin, jotka käyttävät koulutusportaalia työssään tai opiskelussaan (46%) saadaan vastaukseksi 67%. Toisin sanoen 67% aktiivisista koulutusportaalin käyttäjistä on käyttänyt sitä julkisilta tietokoneilta. AVOT-ohjelman perusperiaatteisiin kuuluu ajasta ja paikasta riippumaton oppiminen ja työskentely. On selvää että julkisen tietokoneen käyttö koulutusportaalin alustana on riskialttiimpaa kuin oman tai työpaikan tietokoneen käyttö, mutta koulutuksen kautta saavutetuilla oikeilla toimintatavoilla riskit saadaan hallittavalle tasolle.

On ilmeistä, että mikäli koulutusportaalissa tullaan sallimaan viranomaiskäyttöön luokitellun tietovarannon käsitteleminen, on julkisten tietokoneiden käyttöä rajoitettava. Pääesikunnan turvallisuusosaston eritysluvassa (R3897/12/E/III) rajattiin luokitellun materiaalin käsitteleminen sallittavaksi vain työnantajan hallinnoimilla tietokoneilla. Tutkija kyseenalaistaa tämän ohjeistuksen lisäarvon. Hän mahdollistaisi materiaalin käsittelyn opiskelijan omalla tietokoneella, jossa on puolustusvoimien ohjeistama tietoturva- ja salaamisohjelmisto. Lisäksi tulisi edellyttää, että opiskelijat käyvät läpi yhtenäisen tietoturvakoulutuksen ja siihen liittyvän näyttökokeen.

Virustorjuntaan ja riskinhallintaan liittyviä kysymyksiä

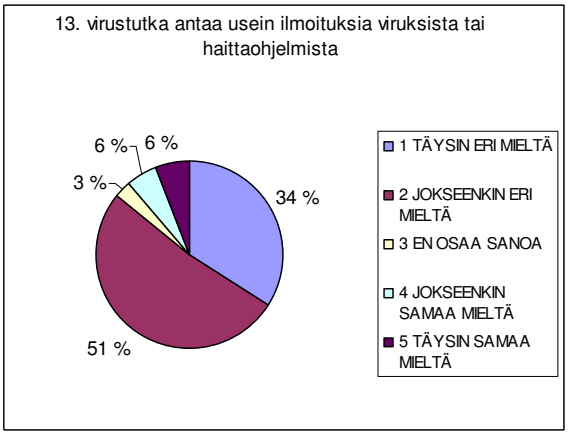
Tietokoneeni varoittaa usein, että järjestelmä on saastunut

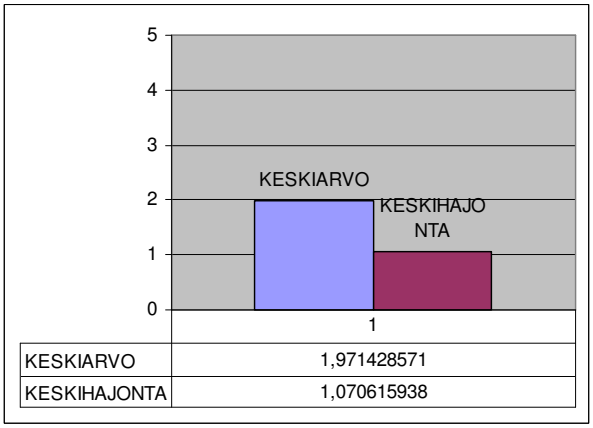




19 vastaajaa on täysin (54%) ja 14 jokseenkin eri mieltä (40). Kolme ei osaa sanoa (6%).

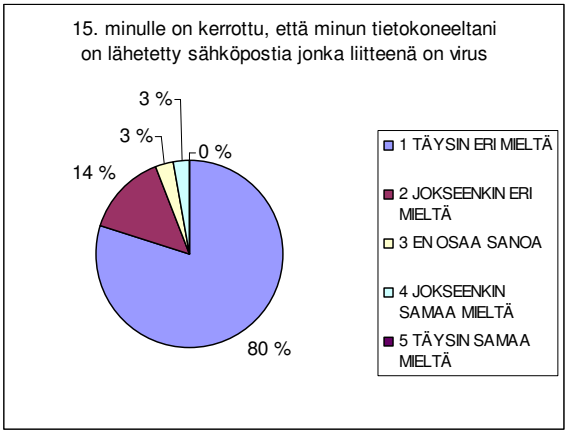
Virustutka antaa usein ilmoituksia viruksista tai haittaohjelmista

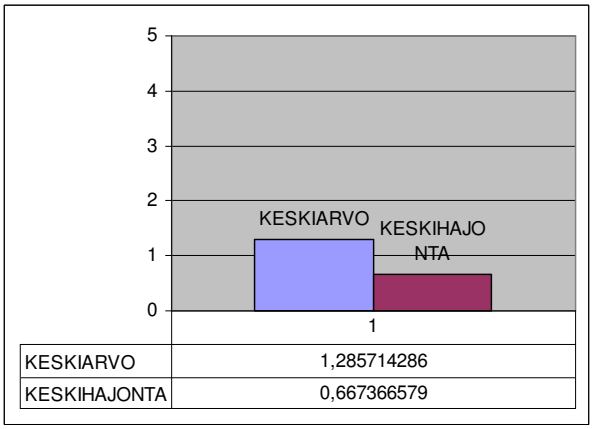




12 vastaajaa on täysi eri mieltä (34%) ja 18 jokseenkin eri mieltä (51%). Yksi ei osaa vastata. Jokseenkin samaa mieltä on kaksi vastaajaa kuten myös täysin samaa mieltä (2%)

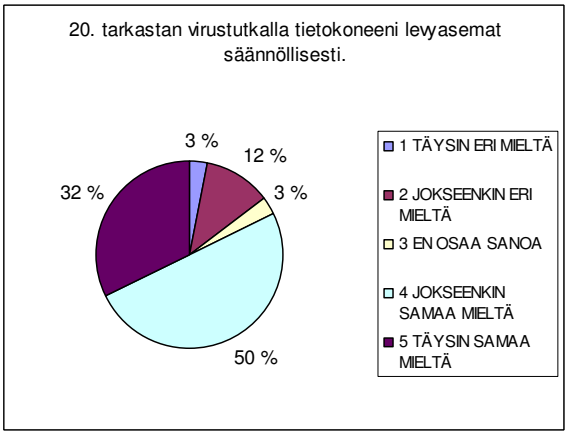
Minulle on kerrottu, että minun tietokoneeltani on lähetetty sähköpostia jonka liitteenä on virus

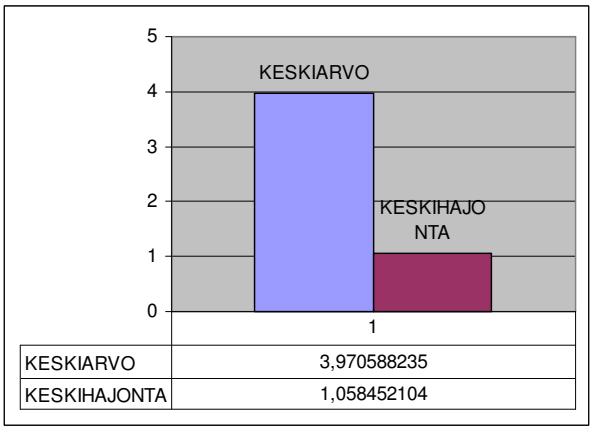




Valtaosa, 28 vastaajista on täysin eri mieltä (80%). Viisi on jokseenkin eri mieltä (14%). EI osaa sanoa ja jokseenkin samaa mieltä vastasi yksi (3%). Kukaan ei ollut täysin samaa mieltä.

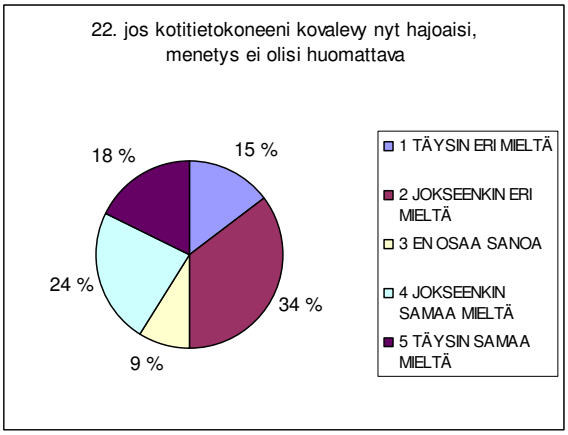
Tarkastan virustutkalla tietokoneeni levyasemat säännöllisesti

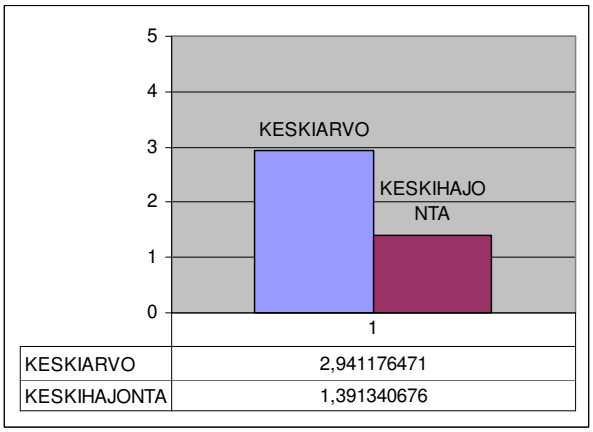




Puolet vastaajista eli 17 on jokseenkin samaa mieltä ja 11 täysin samaa mieltä (32%). Yksi ei osaa sanoa (3%). Neljä jokseenkin eri mieltä (12%) ja Yksi täysin eri mieltä (3%)

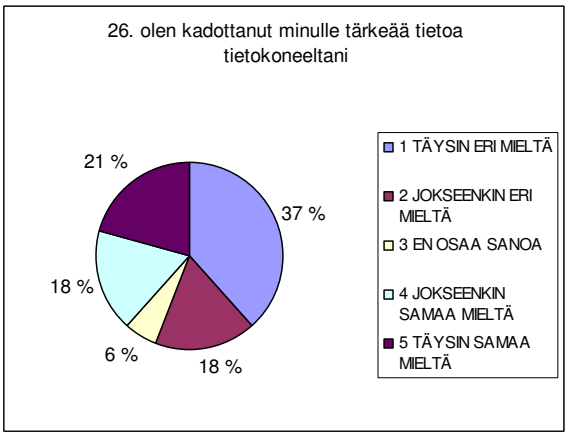
Jos kotitietokoneeni kovalevy nyt hajoaisi, menetys ei olisi huomattava

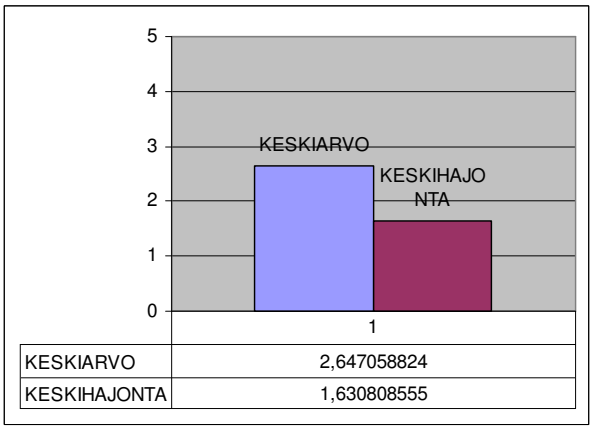




Kuusi vastaajaa on täysin samaa mieltä (18%) ja kahdeksan jokseenkin samaa mieltä (24%). Kolmella ei ole asiasta mielipidettä (9%). 12 on jokseenkin eri mieltä (34%) ja viisi täysin eri mieltä (15%)

Olen kadottanut minulle tärkeää tietoa tietokoneeltani





13 vastaajaa on täysin eri mieltä (37%) ja kuusi jokseenkin eri mieltä (18%). Kaksi ei osaa vastata (6%). Kuusi vastaajaa on jokseenkin samaa mieltä (18%) ja seitsemän täysin samaa mieltä (21%)

Johtopäätökset

Esitiedoissa suurin osa vastaajista ilmoitti käyttävänsä kaupallista tietoturvaohjelmistoa. Tämä näkyy vastauksissa siten, että tietokoneiden saastumisesta ei juurikaan saada indikaatiota. Vastaajat ovat saaneet jonkin verran virustutkan ilmoituksia viruksista ja haittaohjelmista ja se merkki tietoturvaohjelmiston normaalista toiminnasta.

Puolustusvoimat tarjoaa henkilöstölleen maksutta käyttöön F-secure tietoturvaohjelmiston lisenssin. Tämä etu on laajasti käytetty, mutta tiedottamisella on varmistettava, että myös ne vastaajat, joilla nyt on käytössään heikompi tietoturva hyödyntäisivät sen.

Vain yksi vastaaja sanoi olevansa jokseenkin samaa mieltä väitteen kanssa, että hänen sähköpostiaan olisi käytetty viruksen lähettämiseen. Tästä voidaan tehdä johtopäätös, että vastaajien sähköpostiosoitteet eivät ole päässeet vääriin käsiin ja niitä ei ole käytetty roskapostin ja virusten levittämiseen. Tutkija on saanut sähköpostiinsa viruksen sisältäviä viestejä tutulta henkilöltä, joka ei niitä ole lähettänyt. Henkilön sähköpostiosoite ja osoitekirja on varastettu joltakin saastuneelta tietokoneelta ja alistettu rikolliseen tarkoitukseen.

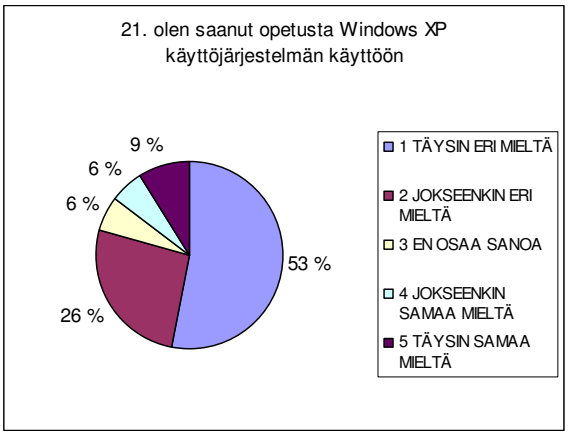
Pääosa vastaajista ilmoitti säännöllisesti tarkastavansa tietokoneensa levyasemat virusten varalta. Tämä toimenpide voidaan tehdä manuaalisesti, mutta suositeltavampi tapa on antaa virusturvaohjelman tarkastaa kone määräajoin. Hyvä aikaväli on esimerkiksi kaksi kertaa viikossa. Vaikka virustorjuntaohjelmisto valvoo aktiivisesti järjestelmää voi viruksia tai muita haittaohjelmia päästä järjestelmään esimerkiksi pakatuissa tiedostoissa tai asennustiedostoissa.

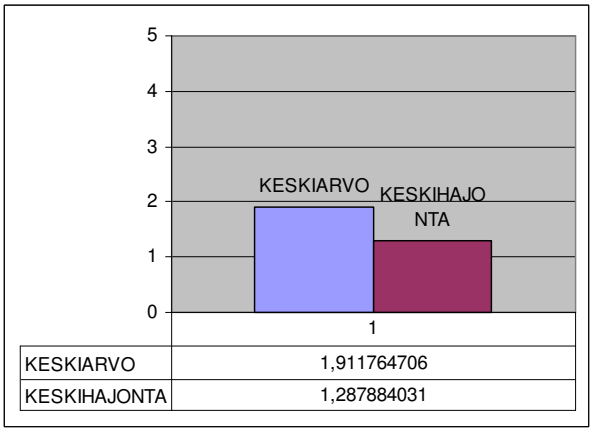
Jopa 42% vastaajista ilmoitti, että kovalevyn hajoaminen aiheuttaisi huomattavan tai jokseenkin huomattavan menetyksen ja 39% sanoi kadottaneensa tärkeää tietoa tietokoneeltaan. Kovalevyn keskimääräinen elinikä on 4 v, jolloin. siihen kohdistuu 25% vuotuinen hajoamisriski. [9] Käyttäjän on syytä kehittää itselleen sopiva, vakiintunut varmennusmenettely, jotta tärkeiden tietojen menettämiseltä vältyttäisiin. Tallentavat DVD- asemat ovat edullisia ja DVD- aihioiden 4.7 gigatavun kapasiteetti on useimmille riittävä, jotta kovalevylle tallennetuista tärkeistä tiedostoista voidaan ottaa vaivattomasti ja pienin kustannuksin varmuuskopioita esimerkiksi viikoittain. Tiedon palauttaminen rikkoutuneelta kovalevyltä on mahdollista vain siihen erikoistuneissa yrityksissä, jotka ovat hinnoitellet itsensä tavallisen kotikäyttäjän ulottumattomiin. Joillekin tietokoneen omistajille on tullut yllätyksenä, että tietokoneen takuu koskee vain laitteistoa, ei sinne tallennettua tietoa.

Tietojen varmistamisesta on tarpeellista järjestää koulutusta. Ongelma on lähinnä asenteellinen.

Koulutukseen liittyviä kysymyksiä

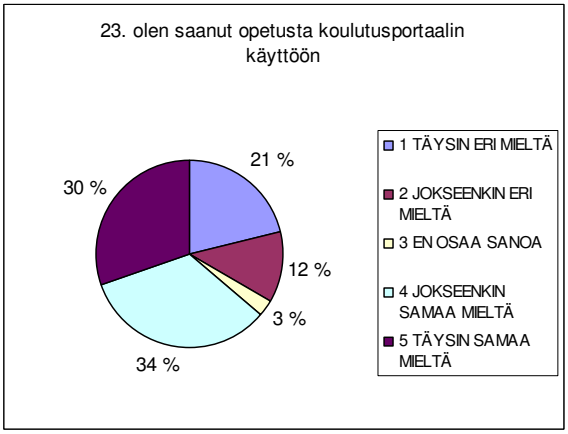
Olen saanut opetusta Windows XP käyttöjärjestelmän käyttöön

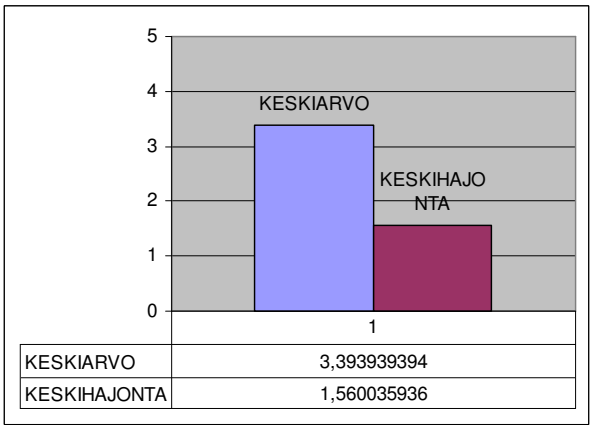




53 % eli 18 vastaajaa on täysin eri mieltä ja yhdeksän jokseenkin eri mieltä (26%). Kaksi ei osaa vastata (6%). Kaksi on jokseenkin samaa mieltä (6%) ja kolme täysin samaa mieltä (9%).

Olen saanut opetusta koulutusportaalin käyttöön





Seitsemän vastaajaa on täysin eri mieltä (21%) ja neljä jokseenkin eri mieltä (12%). Yksi ei osaa vastata (3%). 11 on jokseenkin samaa mieltä (34%) ja kymmenen täysin samaa mieltä (30%).

Koulutukseen liittyvillä kahdella kysymyksellä oli lievä positiivinen korrelaatio (0.3). Tämän perusteella voidaan tehdä varovainen johtopäätös, että koulutusta saavat tai siihen hakeutuvat tietyt henkilöt. Kun kyseessä on koko puolustusvoimissa käytössä olevat järjestelmät, kuten koulutusportaali ja Windows XP, koulutuksen tulee olla kaikille suunnattua. 53% vastaajista ei ollut saanut ja 26% vastaajista oli jokseenkin sitä mieltä, ettei ollut saanut koulutusta Windows XP käyttöjärjestelmälle.

Windows on ollut kotitietokoneiden hallitseva käyttöjärjestelmä lähes 20 vuotta, eikä sen peruslogiikka ole vuosien myötä juurikaan muuttunut. Suurin ero vastaajillakin pääsääntöisesti käytössä olevan Windows XP:n ja aikaisempien Windows 98 ja 95 versioiden välillä on se, että Windows XP on suunniteltu käytettäväksi verkkoympäristössä. Vanhaan työasemakäyttöön suunniteltuihin Windows versioihin tottuneille käyttäjille monet Windows XP:n työkalut ja ominaisuudet jäävät hyödyntämättä. Järjestelmään integroidut varmistusominaisuudet, joilla tietojen varmistaminen voidaan ajastaa tapahtuvaksi halutuin aikavälein, sekä järjestelmän palautuspisteet (restore point) esimerkkeinä mainittakoon. Tutkijan näkemys on, että käyttöjärjestelmäkoulutusta on tarpeellista järjestää sekä Ilmavoimien teknillisen koulun henkilökunnalle että opiskelijoille.

5 YHTEENVETO

Tietotekniikka kehittyy huimaavaa vauhtia. Ensimmäiset kotitietokoneet tulivat markkinoille parikymmentä vuotta sitten ja vielä kymmenen vuotta sitten vain pieni osa kotitalouksista oli kytkeytyneenä internetiin. Nykyisellä kehitysvauhdilla tietokoneiden prosessoriteho kaksinkertaistuu noin 1 - 1,5 vuoden välein ja laajakaistayhteyksien nopeudet näyttävät noudattavan saman suuntaista vakiota. Tässä kehityksessä mukana pysyminen vaatii meiltä kuluttajilta paneutumista, mielenkiintoa, aikaa, vaivaa ja taloudellista panostusta. Saattaa olla kärjistettyä sanoa, että tietotekniikka synnyttää luokkajakoa, mutta niin on helppo ajatella. Analogiset televisiolähetykset loppuvat ja videot korvataan kovalevytallentimilla. Matkapuhelimilla kuvataan videota ja surffataan internetissä. Koomista, mutta totta, että puhelimessa pitää olla virusturvaohjelmisto. Arkipäivää ovat sähköpostit, nettikauppa, sähköiset pankkipalvelut, nettitelevisio, irc, ”mese”, nettipuhelut, nettiradio, nettipelit, vertaisverkot, verkko-opiskelu.

Kuinka helppoa olisikaan jättäytyä kaiken tämän ulkopuolelle. Käydä pankissa ja asioida kassaneidin kanssa.

Koska näyttää siltä, että tietotekniikka on tullut jäädäkseen ainakin Ilmavoimien teknilliseen kouluun, on meidän pyrittävä kehittämään järjestelmiämme ja toimintatapojamme niin, että pysymme yhteisönä kehityksen mukana. Työyhteisössämme ei saa syntyä tietoteknistä luokkajakoa. On tarpeellista kartoittaa koulun henkilöstön ja oppilaiden osaamisen ja välineiden taso, mutta tärkeimpänä tavoitteena tulee olla johdonmukainen asennekasvatus. Tietoturvalliset toimintatavat lähtevät terveestä asenteesta, sillä tietoturva on ensisijaisesti inhimillisten tekijöiden summa. Tampereen yliopistossa tehdyn tutkimuksen mukaan liiketoiminnan tietojen turvallisuus muodostuu siten, että 80% koostuu henkilöstön arkirutiineista ja 20% teknisistä apuvälineistä. Joku viisas onkin sanonut, että virustorjunta ohjelmaa voisi verrata talvirenkaisiin, jotka kyllä estävät lipsumisen, mutta eivät estä ajamasta ylinopeutta.

LÄHTEET

[1] Ali-Yrkkö, Tanja. Koulutusportaali palveluksessa. Artikkeli Sotilas aikakusilehdessä 6-7/2004 s26

[2] Digitoday Verkkojulkaisu 23/07/2003. http://www.digitoday.fi/

[3] Digitoday Verkkojulkaisu.
http://digitoday.fi/showPage.php?page_id=14&news_id=40339

[4] Finnish Software Business Cluster. Verkkosivut.
http://www.swbusiness.fi/portal/news/?id=5891&area=7

[5] Flyktman Reima. PC-käsikirja. IT Press. Toinen painos. Helsinki 2004. s382

[6] F-secure. Tietoturvayhtiön verkkosivut. http://www.f-secure.fi

[7] F-secure. Tietoturvayhtiön verkkosivut http://www.f-secure.com/weblog/archives/archive-122005.html#00000757

[8] Helopuro, Sanna; Perttula, Juha; Ristola, Juhapekka. Sähköisen viestinnän tietosuoja. Talentum. Helsinki 2004. s147

[9] Helsingin teknillinen korkeakoulu, ylläpito ja turvallisuus, luentomateriaali
http://www.tkk.fi/atk/tietoturva/koulutus/1-yllapito-ja-turva.pdf

[10] History of ARPANET, Part 1: The history of ARPA leading up to the ARPANET.
http://www.dei.isep.ipp.pt/docs/arpa--1.html

[11] Ilmavoimien Esikunta. Ilmasotaohjesääntö (ISO). 31.3.1995. s. 43

[12] ILMAVOIMIEN TEKNILLISEN KOULUN OPPIMISKESKUKSEN TOIMINTAOHJE

[13] Kirsten, Peter. Video:Internet, Web, What's Next conference, CERN, Geneve, 26.6.1998.

[14] Kivimäki Jyrki. Tehokäyttäjän opas Windows NT 4. Suomen Atk-kustannus. 1998 s585

[15] Koulutusportaali. www.milnet.fi/gene/kopo

[16] Kuva – toteutusperiaate. www.mil.fi/laitokset/pvkk/koulutusportaali.dsp

[17] Laki Yleisradio Oy:stä 3 luku §7

[18] Lehtinen Erno. Verkkopedagogiikka. Oy Edita Ab 1997 s42

[19] Liikenne- ja viestintäministeriö, Tietoturvalliseen tietoyhteiskuntaan, Kansallisen tietoturvallisuusneuvottelukunnan kertomus valtioneuvostolle 14.12.2004

[20] Majander Olli. Näin tieto kulkee internetissä. Artikkeli Mikrobitti lehdessä 10/2004 s60

[21] Microsoft, Widows XP Professional –sertifikaatti. Edita Publishing oy. Helsinki 2003. s496

[22] Microsoft. Bulletins. Verkkosivut. http://www.microsoft.com/technet/security/bulletin/ms06-001.mspx.

[23] Microsoft Security Response Center. Verkkosivut. http://blogs.technet.com/msrc/archive/2005/12/30/416694.aspx

[24] Mikrobitti 11/05. Artikkeli: Langattomat tiedonsiirtotekniikat.

[25] Mikrobitti 1/06. Artikkeli: Tietoturvaa vuonna 2006

[26] Muhonen, Petri 04.11.2003. Microsoft ja tietoturva-aukot**.** Verkkojulkaisu. www.bittivuoto.net/artikkelit.php4?kat=kolumnit&id=73 – 44

[27] Nevgt, Anne, Tirri, Kirsi. Hyvää verkko-opetusta etsimässä. Suomen Kasvatustieteellinen Seura. 2003 s35

[28] Nokia. Verkkosivut. Bluetooth- tekniikka. http://www.nokia.fi/puhelimet/teknologiat/bluetooth/

[29] Opetushallitus. Verkkosivut. Etäopetus http://www.edu.fi/page.asp?path=498;3293;6986;6987;15760

[30] PÄÄESIKUNTA, koulutusosasto, Budjetointiohje oppimiskeskusten perustamiseksi, 24.01.2001 (R323/5.1/D/II)

[31] PÄÄESIKUNTA, turvallisuusosasto. Asiakirja R3897/12/E/III

[32] PÄÄESIKUNTA, turvallisuusosasto. PAK 4:15 Käyttäjän tietoturvaohje

[33] PÄÄESIKUNTA, turvallisuusosasto. PAK 1:2

[34] Saarinen Jorma, Varis Tapio, Vainio Leena, Rintala Mika, Piipari Martti, Nokelainen Petri. Kouluttajana verkossa – menetelmät ja tekniikat. Hämeen ammattikorkeakoulu. 2002 s47

[35] Sallila, Pekka, Kalli, Pekka. Verkot ja teknologoa aikuisopiskelun tukena. Kansanvalistusseura ja Aikuiskasvatuksen Tutkimusseura 2001 s180

[36] Salminen Maija. Ilmavoimien teknillisen koulun kirjastonhoitaja. Haastattelu

[37] Suvantola Jaakko, Maantieteen laitos, Joensuun yliopisto, Korrelaatio http://www.joensuu.fi/geo/geostat/Korrel.pdf

[38] Telegraph .Verkkolehti. Iso-Britannia http://news.telegraph.co.uk/news/main.jhtml?xml=/news/2005/07/28/nhack28.xml

[38] Tieteen tietotekniikan keskus. Internetin historiaa. Verkkosivusto, http://www.funet.fi/index/FUNET/history/heureka/etusivu.html

[40] Tilastokeskus. Verkkosivusto. http://www.stat.fi/tk/tp/verkkokoulu/vk/tt/oppitunnit/tt02/tt02_10/view.html

[41] Tieturi vision oy. Verkkojulkaisu. wwww.r5vision.com Arkisto-> Reservin upseeriksi verkko-opiskelulla

[42] Toiskallio Jorma, Tura Tomi, Rouvinen Miika. Kohti puolustusvoimien verkottuvaa oppimista. Maanpuolustuskorkeakoulu. Koulutustaidon laitos. Helsinki 2003.

[43] Tomsnetworking. Verkkosivusto. http://www.tomsnetworking.com/Sections-article106-page9.php

[44] Viestintävirasto. Verkkosivut. Tietoturvallisuuden perusteet. http://www.ficora.fi/suomi/tietoturva/ttkasitteet.htm

[45] Viestintävirasto. Verkkosivut. Salausmenetelmät. http://www.ficora.fi/suomi/tietoturva/salausmenetelmat.htm

[46] Viestintävirasto. Verkkosivut. Tietoturvaloukkausten havainnointi ja ratkaisu. http://www.ficora.fi/suomi/tietoturva/cert.htm#2006-01-05_2345

[47] Viestintävirasto. Verkkosivut. Tietoturvaloukkausten havainnointi ja ratkaisu. http://www.ficora.fi/suomi/tietoturva/varoitukset/varoitus-2005-51.htm

[48] Viestintävirasto. Verkkosivut. Virustorjunta. http://www.ficora.fi/suomi/tietoturva/virustorjunta.htm

[49] Virustorjunta.net. Verkkosivusto. http://www.virustorjunta.net/modules.php?name=News&file=article&sid=572

[50] Väestörekisterikeskus. Verkkosivut. http://www.sahkoinenhenkilokortti.fi/

[51] Windows XP- käyttöjärjestelmän ohje-toiminto.

LIITTEET

Liite 1 Tietoturvakysely Ilmavoimien teknillisen koulun opettajille ja kadeteille

Liite 1

Tietoturvakysely Ilmavoimien Teknillisen Koulun opettajille ja kadeteille.

Hei. Lähestyn sinua kyselyn merkeissä. Kyselyni liittyy Pro Gradu- työhöni maanpuolustuskorkeakoulussa. Aiheeni on VERKKOTUETUN MONIMUOTO-OPETUKSEN TIETOTURVARISKIT ESIMERKKINÄ ILMAVOIMIEN TEKNILLINEN KOULU.

Toivon, että sinulla on hetki aikaa vastata kysymyksiin. Aikaa vastaamiseen kuluu noin 10 minuuttia. Vastauksellasi on merkitystä.

Kyselyn tarkoituksena on kartoittaa käyttäjän toimien ja välineiden vaikutusta koulutusportaalin tietoturvallisuudelle. Vastaajajoukon koko on noin 35 henkeä ja se koostuu IlmavTK:n opettajista ja lentoteknillisen linjan kadeteista. Kyselyyn vastataan nimettömänä.

Pyri vastaamaan rehellisesti asioita kaunistelematta.

Kiitos paljon

Tatu Köykkä

Palautus kirjekuoreen Tatu Köykän lokeroon to 15.9.2005 klo 16.00 mennessä

YMPYRÖI OIKEA VAIHTOEHTO

Olen	Kadetti	Siviiliopettaja	Sotilasopettaja	Muu
Ikäni	20-27	28-35	35-42	43->
Kotitieto-koneessani on	Ei ole kotitietokonetta	Windows XP käyttöjärjestelmä	Internetyhteys	Kaupallinen tietoturva-ohjelmisto
	Ilmainen tietoturva-ohjelmisto	Linux käyttöjärjestelmä		

RASTITA OIKEA VAIHTOEHTO

	1 TÄYSIN ERI MIELTÄ	**2 JOKSEENKIN ERI MIELTÄ**	**3 EN OSAA SANOA**	**4 JOKSEENKIN SAMAA MIELTÄ**	**5 TÄYSIN SAMAA MIELTÄ**
1. tunnen puolustusvoimien tietoturvallisuusohjeiston sisällön					
2. käytän yhtä salasanaa tai sen muunnoksia kaikissa sovelluksissa					
3. puolustusvoimien tieto-turvaohjeistus on liian tiukka					
4. siirrän tietoa siirrettävällä medialla (CD,korppu, USB-muistit)					
5. kirjoitan salasanani muis-tiin					
6. puolustusvoimien tieto-turvaohjeistus hidastaa tai vaikeuttaa työtä-ni/opiskeluani					
7. käytän koulutusportaalia työssä tai opiskelussa					
8. käytän sähköpostia työs-sä tai opiskelussa					
9. avaan sähköpostini liite-tiedostot					

	1 täysin eri mieltä	2 jokseenkin eri mieltä	3 en osaa sanoa	4 jokseenkin samaa mieltä	5 täysin samaa mieltä
10. tietokoneeni varoittaa usein, että järjestelmä on saastunut					
11. kotitietokoneeni on suojattu salasanalla					
12. lopetettuani internetin käytön muulla kuin omalla tietokoneella, poistan aina evästeet ja väliaikaiset tiedostot.					
13. virustutka antaa usein ilmoituksia viruksista tai haittaohjelmista.					
14. internetselaimessani on käytössä asetuksia, jotka helpottavat työskentelyäni esim. automaattinen täydennys joka muistaa mm käyttäjätunnukset ja salasanat.					
15. minulle on kerrottu, että minun tietokoneeltani on lähetetty sähköpostia jonka liitteenä on virus					
16. lapset menevät usein tietokoneeltani internetiin samoilla käyttäjätunnuksilla kuin minä					
17. olen tehnyt ostoksia internetissä					

	1 täysin eri mieltä	**2 jokseenkin eri mieltä**	**3 en osaa sanoa**	**4 jokseenkin samaa mieltä**	**5 täysin samaa mieltä**
18. olen siirtynyt käyttämään toista internet-selainta viimeisen vuoden aikana					
19. vain minulla on järjestelmänvalvojan oikeudet tietokoneellani					
20. tarkastan virustutkalla tietokoneeni levyasemat säännöllisesti.					
21. olen saanut opetusta Windows XP käyttöjärjestelmän käyttöön					
22. jos kotitietokoneeni kovalevy nyt hajoaisi, menetys ei olisi huomattava					
23. olen saanut opetusta koulutusportaalin käyttöön					
24. olen osallistunut puolustusvoimissa tietoturvallisuusluennolle					
25. olen käyttänyt koulutusportaalia joltakin julkiselta tietokoneelta. Esimerkiksi kirjastosta tai internet-kahvilasta					
26. olen kadottanut minulle tärkeää tietoa tietokoneeltani					